IARPA

BROAD AGENCY ANNOUNCEMENT

IARPA-BAA-16-12

Virtuous User Environment (VirtUE) Phase 1

IARPA-BAA-16-12

Release Date: 18 October 2016

IARPA

BROAD AGENCY ANNOUNCEMENT: IARPA-BAA-16-12

Virtuous User Environment (VirtUE) Phase 1

TABLE OF CONTENTS

GENERAL INFORMATION

This publication constitutes a Broad Agency Announcement (BAA) and sets forth research of interest in the area of creatively defining and developing new, inherently secure, virtual user environments. Awards based on responses to this BAA are considered to be the result of full and open competition.

- **Federal Agency Name** – Intelligence Advanced Research Projects Activity (IARPA)
- **Funding Opportunity Title –** Virtuous User Environment (VirtUE) Phase 1
- **Announcement Type –** Initial
- **Funding Opportunity Number –** IARPA-BAA-16-12
- **Catalog of Federal Domestic Assistance Numbers (CFDA)** – Not applicable
- **Dates**
  - Posting Date: 18 October 2016
  - Proposal Due Date for Initial Round of Selections: **5:00 pm Eastern Time 12 December 2016**
  - BAA Closing Date: 5:00 PM Eastern Time - 10 January 2017
- **Anticipated individual awards** – Multiple awards anticipated
- **Types of instruments that may be awarded** – Procurement contracts, grants, cooperative agreements and other transactions
- **Agency Points of contact**
  ATTN: IARPA-BAA-16-12
  Office of the Director of National Intelligence
  Intelligence Advanced Research Projects Activity
  Washington, DC 20511
  Electronic mail: dni-iarpa-BAA-16-12@iarpa.gov
  Unclassified Fax: 301-851-7440
- **Program Manager** – Kerry Long, IARPA
- **Program website** – http://www.iarpa.gov/index.php/research-programs/virtue
- **BAA Summary** – The VirtUE program seeks to creatively define and develop new, inherently secure, virtual user environments.
- **Questions** – Submit questions on administrative, technical, or contractual issues by email to dni-iarpa-BAA-16-12@iarpa.gov. All requests shall include the full name and affiliation of a point of contact. Do not send questions with proprietary content. A consolidated Question and Answer response shall be posted on the Federal Business Opportunities website (http://www.fbo.gov) and linked from the IARPA website (http://www.iarpa.gov/index.php/research-programs/Virtue/questions.html). No answers shall go directly to the submitter. IARPA shall accept questions until **10 November 2016**.

OVERVIEW

SECTION 1: FUNDING OPPORTUNITY DESCRIPTION

The Intelligence Advanced Research Projects Activity (IARPA) often selects its research efforts through the Broad Agency Announcement (BAA) process. The use of a BAA solicitation allows a wide range of innovative ideas and concepts. The BAA shall appear first on the FedBizOpps website, http://www.fedbizopps.gov/, and then linked to the IARPA website at http://www.iarpa.gov/. The following information is for those wishing to respond to this Program BAA.

This BAA (IARPA-BAA-16-12) is for the Virtuous User Environment (VirtUE) program Phase 1. IARPA is seeking innovative solutions for VirtUE Phase 1 in this BAA. VirtUE Phase 1 is envisioned to begin June 2017 and end by December 2018. This solicitation covers the first of three potential phases that will build upon each other to achieve overall VirtUE program objectives. VirtUE Phase 2 with a Phase 3 option will be a separate solicitation projected to occur in August of 2018. Participation in VirtUE Phase 2 will be open to all interested parties regardless of their participation in this VirtUE Phase 1 proposal.

1.A. Program Overview

1.A.1 Program Definitions

The VirtUE program uses a standardized nomenclature to ensure clarity. Key terms used throughout the program and their meaning are provided in Table 1 below.

Table 1. VirtUE Program Definitions

VirtUE Term	Definition
Applications	Executables and their associated libraries. Examples include Microsoft Word or SSH
Attack Surface	Subset of system resources (see resource definition below) potentially used in the attack of a system
Analytics/Control Layer	A trusted execution environment running on separate physical hardware than Virtues that communicates with, monitors, protects, and controls Virtues through dynamic control logic and analytics
Dynamic Analytics/Control Logic	A series of heuristics and logic that leverages the dynamic capabilities of Virtues to better detect and protect computing users in the cloud
Exploitable Processes	Processes resident in a Virtue that could be exploited by either a privileged internal user of the Virtue or external logic executed by the Virtue

Exposed Portion	Any part of a Virtue's environment that is directly exposed to either users or external processes/entities (excluding the Analytics/Control Layer)
Logging Option	Set of informational elements in a log that contain similar content and specificity that can be independently tasked for collection (possible examples include login attempts, login failures, file accesses, file contents, list of altered files, and directory contents.
Logs	Any security relevant information collected from or about a Virtue used as potential inputs to dynamic analytics in the Analytics/Control Layer.
Infrastructure-Based Attacks	For this program, an attack that leverages the functionality of the cloud provider's hypervisor to read or write to a hosted guest's memory.
Peer	Virtual machine or Virtue residing on the same hypervisor
Permissions on a Resource	The actions that a role is permitted to take on a particular resource (resources are defined below)
Presentation Interface	A means to enable users with direct access to a thin client the ability to interact with numerous remote Virtues and to authenticate to the Analytics/Control Layer
Protection	An action/configuration that a Virtue can implement that increases its security posture
Protection Option	A protection that can be individually invoked or configured that provides additional security value
Role	An enterprise defined set of one or more computational tasks that involve similar risks and require similar applications, resources, and protection
Resource	An informational technology asset such as services, applications, accessible files, accessible network locations, printers etc.
T&E Team	Test and Evaluation team, JHU-APL , tasked with assessing performers' deliverables against program requirements through the use of a highly structured testing methodology
UCE	User Computing Environment. An environment for computation that a user interacts with to launch needed applications and access required informational resources. Comprised of one or more Virtues and a presentation interface
User Action	An event, initiated by a user, that effects a change in state of some resource
Virtue	A virtualized construct capable of running (mostly*) independently on an Amazon Web Services (AWS) hypervisor that incorporates all the functionality and protections required to securely accomplish a defined user role.
Virtue Image	Virtue distribution unit that completely encompasses and defines the characteristics of a particular Virtue, used to invoke a running Virtue instance on AWS

*(The Virtue shall depend minimally on certain services provided by the Analytics/Control Layer and at the performer's discretion may rely on external application servers for access to certain needed applications).

1.A.2 Introduction and Concept of Operations

VirtUE seeks to leverage the federal government's impending migration to commercial cloud-based information Technology (IT) infrastructures and the current explosion of new virtualization and operating system (OS) concepts to create and demonstrate a more secure interactive user computing environment (UCE) than the government has had in the past or likely to have in the near future. Currently the government UCE is represented by a general purpose Windows desktop OS running multiple installed applications hosted on either a dedicated physical computer or on a shared virtualized platform. When a desktop OS is hosted on a shared virtualized platform, it is called a virtualized desktop interface or VDI.

In Phase 1, VirtUE seeks to deliver an interactive UCE designed from the outset to be a more secure, capable sensor and defender in the cloud environment than the current government UCE solution. To be acceptable to potential government consumers, the new UCE must still offer functionality and performance characteristics comparable to the current government UCE. Phase 1 performers shall create a UCE that mitigates the exploitation of legacy and cloud-based vulnerabilities and/or provides numerous logging and protection options for future external security logic to do so.

In Phase 2, performers shall take the technologies and/or concepts developed in Phase 1 and create novel external analytics and security controls that leverage them. The purpose of this analytics/control effort is to create dynamic detection and protection capabilities that make the VirtUE user environment more resistant to attacks expected in the commercial cloud while minimizing the costs associated with these capabilities.

1.A.3 Current Situation and Motivation

1.A.3.1. Cloud UCEs as a Target

UCEs in the cloud are likely to be highly targeted. In its current instantiation, UCEs in the cloud, often referred to as virtual desktops, are little more than virtualized replicas of physical workstations running on general purpose operating systems on a standard virtual machine (VM) instance. The methods and technologies external adversaries are comfortable using to exploit and control physical workstations are still largely effective with virtualized UCEs. As with traditional physical workstations, users can be tricked by adversaries to compromise security through running untrusted code in emails and from web sites. Current virtual UCEs are susceptible to the same credential stealing techniques that allow adversaries to move laterally within an organization. Virtualized UCEs are also susceptible to the same OS vulnerabilities that enable privilege escalation. Cloud encryption technologies that are being promulgated as a means of protecting user data in the cloud can be circumvented by exploiting virtualized user workstations that can view such data in its unencrypted state.

Virtualizing UCEs may make monitoring and countering illicit internal user activities more difficult and hence more exploitable by malicious users. Freed from the constraints of physical machines, IT architects are likely to increase the number of both workstation and server endpoints running security relevant workloads. Security analysts will now have even more data to comb through looking for processes or users behaving incorrectly. The ephemeral nature of most virtual UCEs will make it much harder for investigators to gather forensic evidence when a user is suspected of bad behavior.

1.A.3.2. State of Practice

Security researchers who have been studying and proposing security mitigations for cloud-based workloads have largely constrained their efforts to lower user interaction platforms such as web/database servers or compute nodes. This may be due in part to the difficulties introduced by the interactive and dynamic nature of the user computing environment. For example: users in a UCE may deliberately or unintentionally interfere with efforts or technologies that provide security; user behavior is nondeterministic and difficult to design for; and finally, users are less tolerant than server processes to delays and intermittent operations that new security mitigations may entail. The VirtUE program hopes to focus future virtualization security researchers on the important security challenges of the UCE cloud-based workload. To facilitate this, IARPA shall endeavor to make findings available to the public for organizations to incorporate into future work.

Current security mitigations for virtualized UCEs are largely the same technologies and methods that have been used with mixed success for years on physical desktop workstations. UCEs run resident security agents that occupy the same OS memory space as the processes and/or people they seek to monitor. This enables crafty processes or users to disable these local security programs or interfere with their operation. Security logs from these now-suspect agents are forwarded *en masse* to centralized databases and Security Event and Incident Management Systems (SEIMS) where analytics and/or analysts try to detect rare events with incomplete data, hours to days after the actions have occurred.

The expense associated with collecting, transporting and processing existing security logs can be substantial. In an environment that sees attacks rarely, much of this logging expense is wasted. Yet currently, there are few good alternatives to collecting and processing as much data as possible "just in case". Similarly, the processing cost user environments already expend with "always on" security protections is starting to adversely impact the user computing experience in government organizations. Continuing to use the existing government UCE model will make this situation even worse in the future. To deal with new threat vectors found in future commercial clouds, government security professionals will have little choice but to collect and process greater amounts of logging data by default and employ more default security protections in an attempt to provide similar amounts of assurance. The VirtUE program aims to improve this situation by providing methods that will incur collection and protection costs in a more considered fashion.

When illicit activity is discovered, current virtualized UCEs offer few alternatives to respond to hostile activity beyond the "power down" and rebuild option of legacy physical workstations. The VirtUE program aims to improve this situation by demonstrating a more secure paradigm where

the UCE is designed from the outset to respond to malicious actions with more nuanced protection options.

Workloads in the cloud are largely run within one of two virtualization constructs. The choices are either a traditional VM running a full-featured general purpose OS or a minimized application container that shares the kernel functions of an OS with other containers on the same hardware platform. As implemented, both of these constructs have troubling security weaknesses. Current government virtual desktop offerings utilize a traditional VM construct. In theory this affords the UCE more protection from other peer workloads than popular container technologies, but relies exclusively on the cloud provider's (untrusted?) hypervisor for protection from peer and cloud infrastructure based attacks. The VirtUE programs seeks to create alternative virtualization constructs for secure user computing environments to occupy in the cloud.

1.A.3.3. Current UCE Security Shortcomings

The VirtUE program asserts that the familiar UCE consisting of a general purpose, multi-function Windows-like desktop running in a traditional VM is not sufficient to protect sensitive government users or workloads of the future in the cloud. Key security shortcomings of the current UCE model are:

1. An inability to collect security relevant information without potential interference from malicious processes or users
2. A lack of dynamic log collection or defensive capabilities that can adjust rapidly to changing possibilities
3. The inability to adjust security processing loads/costs based on the current threat
4. A large code-base and resource pool introducing numerous potential vulnerabilities
5. The inclusion of resources/applications not needed or not authorized for users
6. An inherently problematic trust model that enables a user to employ different credentials for different unrelated tasks in the same operating environment
7. A complex user behavioral model that has proven difficult to analyze or predict
8. An inability to mitigate or detect threats to a guest from peer virtual machines (VM) or provider managed hypervisors
9. An inability to effectively mitigate or detect threats from privileged users or malicious processes
10. A cumbersome method of creating, capturing, and distributing successful UCE configurations throughout the government and the commercial cloud

1.A.4 Phase 1 Approach

In Phase 1, VirtUE intends to create a secure, modular virtualized construct called a "Virtue" (see Figure 1 for concept) that directly addresses the shortcomings of the current UCE model above. This construct may be thought of as a type of virtual appliance built specifically for the purpose of safe, user-interactive computing tasks in a commercial cloud. A Virtue will need to run on a typical cloud provider's virtualized infrastructure. However, it is not conceptually restricted to the

common construct of a VDI instance – a general purpose OS running within a virtualized machine (VM) image.

The performer's key creative task for this proposal is to devise what a Virtue should consist of to meet the requirements of Phase 1 detailed below. For example, a Virtue might be a simple VM image running some specially designed OS. A Virtue could be one or more containers sharing a secure OS kernel running within a VM. The Virtue might be 3 small VM's linked together in a virtualized private network each performing specialized tasks. It could be a micro hypervisor running its own services guest with a complimentary inspection guest (see Figure 2). Note that these are only possible examples and are not exhaustive.

The VirtUE program will be supported by an independent test and evaluation (T&E) team to assess the efficacy of performers' solutions throughout Phase 1.

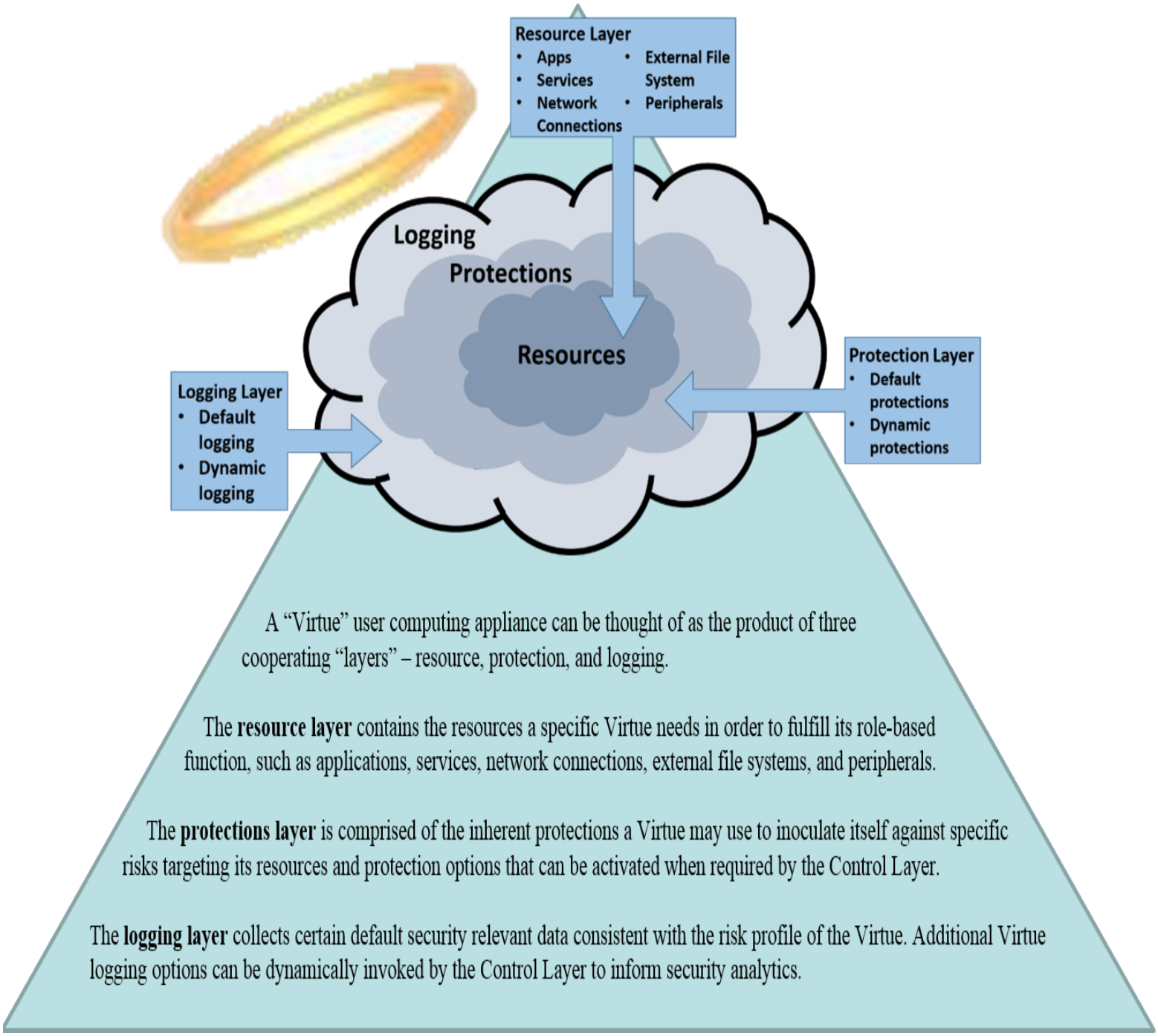


Figure 1. The Virtue Concept

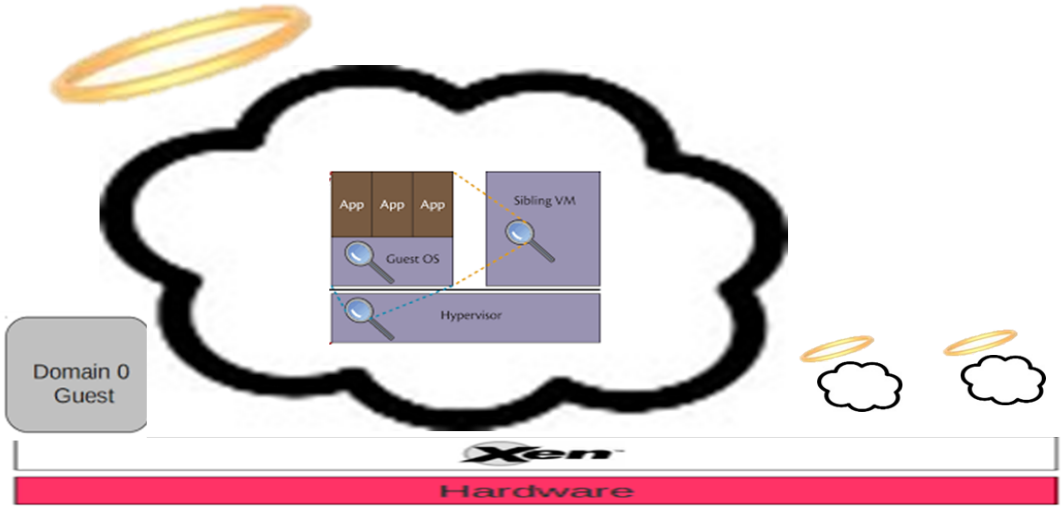
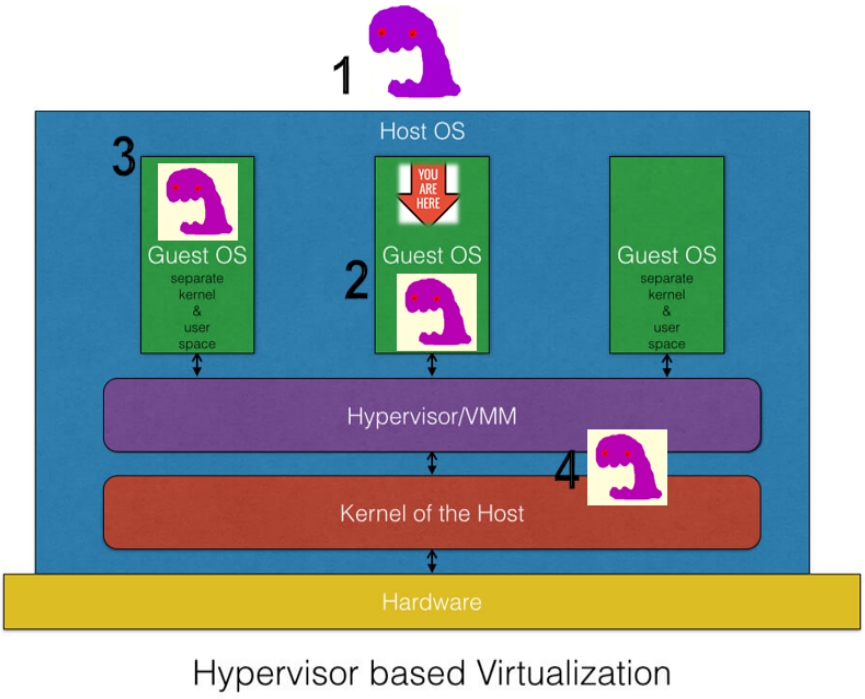


Figure 2. A Potential Virtual Construct for a Virtue



1. External (traditional)
2. Internal/Insider
3. Peer
4. Infrastructure Based

Figure 3. Cloud Threat Vectors

1.A.5 Phase 1 Virtue Requirements

1.A.5.1 Requirements Explained

For Phase 1, these requirements have been designed to specify desired performance characteristics, not technology approaches. While some specific technology approaches may be discussed in this solicitation as reference exemplars, this in no way indicates a bias towards these particular technologies or approaches. It is IARPA's objective to develop novel methods of provisioning, protecting and monitoring cloud-based user environments. Accomplishing this objective shall require innovation, not modest improvements to existing approaches or commercial technologies.

Although Phase 1 solutions should not focus on improvements to existing commercial technologies, pre-existing, publicly available commercial technologies can be used as components in a Phase 1 solution. The key distinction is that Phase 1 performers may use existing commercial technologies as components in a Phase 1 solution provided that no IARPA funds are used in the alteration of the commercial product and that the product or products comprise only a portion of the total Phase 1 solution.

Performers that incorporate commercial components into their solution must provide fully licensed versions of these technologies with the solution package that they deliver to the T&E team for assessments.

The order of stated requirements are not intended to convey relative importance. Each requirement is important to the success of Phase 1 and proposers should attempt to satisfy each of them. Inevitably there will be tradeoffs required between performance, security, and functionality considerations in a performer's solution when addressing these requirements. It is key for the proposer to develop a solution that effectively balances these equally important qualities in such a way to provide significantly more security than the current government UCE without requiring significantly more resources or significantly impacting functionality. Because of the novelty of this effort, proposer's work over the Phase 1 period will help to define what the state of the possible is. However, where appropriate, initial numeric goals derived from current government UCE characteristics are provided to aid proposers in scoping their efforts and measuring their progress.

VirtUE program solutions shall run on hardware and hypervisor technologies currently available or on the Amazon Web Services (AWS) EC2 cloud or reasonably projected to be on the AWS cloud by January 2018. AWS has been chosen as the reference cloud infrastructure for this effort because of its current and future use within the intelligence community (including in the IC ITE project), its use of popular, open source hypervisor technology, and its well-defined measurement model. VirtUE proposers are free to leverage any AWS technologies available to Amazon customers, but should not assume that any special considerations or accesses will be provided to VirtUE performers by Amazon. Proposers relying on innovations in AWS beyond what is available at the time proposals are due shall need to make a case why

they believe the technology or innovation their proposal depends upon shall likely be available by January 2018 within AWS.

Proposers shall also offer feasible methods in the proposal for the T&E team to simulate any required future capabilities that the proposer's Virtue solution depends upon during scheduled midterm and final examinations. (Note: Dedicating an entire AWS physical server for each individual user's virtualized workload, though an obvious way to eliminate peer workload threats, shall not be considered a realistic option for this proposal.)

The formal requirements for Phase 1 follow:

1.A.5.1.1 Requirement 1 Proposers shall devise a repeatable, automated secure means of storing, launching, and interacting with their Virtues within the AWS infrastructure.

Discussion:

Proposers should provide methods for consumers of Virtues to conveniently and securely access a Virtue image (refer to Table 1 for definition of Virtue image) from a secure repository location within the AWS cloud; use the image to automatically create and launch a fully functional, running instance of the Virtue appliance within AWS; and provide secure convenient interfaces for both Virtue users and the future Analytics/Control Layer to interact with Virtues over the AWS network.

T&E team members will use performer-provided methods to launch several Virtues from Virtue images within AWS to assess the ease and effectiveness of the performer's methodology. T&E team members will leverage available Virtue interfaces to test both their security and performance characteristics.

Network connections between the end device, the Analytics/Control Layer, and Virtues should be encrypted using existing encryption algorithms when possible to prevent eavesdropping. If a proposer's solution requires the remote presentation and control of cloud user environments, proposers are encouraged to utilize existing open source or commercial remote access protocol solutions where appropriate. The focus of the VirtUE effort is not to build a better remote access protocol or engineer a new encryption protocol. Some popular examples of remote access protocols are PCoIP, Spice, RDP, and VNC.

The T&E team will not assess the security and performance of remote access protocols directly during this effort, however the team may assess protocols indirectly when they impact the overall usability of Virtues.

1.A.5.1.2 Requirement 2 Virtues shall present themselves as atomic, largely immutable entities to other Virtues and external processes. They shall be simpler and more modular than current VDI solutions with a minimized attack surface.

Discussion:

A Virtue instance when running may be comprised of multiple components and technologies but these components must not be directly addressable/visible from other virtual workloads external to the Virtue instance. Virtues shall present themselves as a virtual appliance that communicates with other external entities, including other Virtues only through its network stack.

Virtues should accrue intrinsic security advantages by breaking down the traditional general purpose desktop VM paradigm into simpler, specially-crafted environments. The objective is for an individual Virtue to exhibit less complex, better defined behavior than a general VM hosting a typical desktop operating system. One possible method to measure potential behavioral complexity is based on the number of resources a user environment has access to. A "simple" Virtue would not have access to resources it does not need.

Ideally T&E team members should find a performer's Virtue has far fewer available services, applications, credentials and files exposed than a typical VDI VM, thus reducing its attack surface as well as its memory, processing and storage requirements.

1.A.5.1.3 Requirement 3 Virtues shall be role-based.

Discussion:

A convenient, discernable method for modularizing the current general purpose user environment is through the application of computational roles – providing only the particular resources and credentials a user needs for one or more closely related computational tasks (see table 2). Specifically:

- A user has one or more enterprise-defined roles, and a separate Virtue environment corresponds to each and every one of these roles
- It is easier for cyber security personnel/developers to understand, log, detect and defend computer environments that exhibit well-understood user behaviors
- Users of Virtues should only be permitted to assume roles for which they have been explicitly authorized and authenticated
- Process and Application isolation exists between the instantiation of every role and hence every Virtue
- Every user will invoke and interact with several role-based environments (Virtues) simultaneously through a presentation interface. This provides the opportunity to define and limit user behaviors for each individual environment without limiting overall user capabilities
- A role may require multiple cooperating applications. Thus, a Virtue must support multiple cooperating applications.

Roles and their resultant Virtues shall ultimately be defined and created by an enclave's personnel and shall not be predetermined by performers. However, performers shall be

required to demonstrate the capabilities of certain predefined roles generated by the T&E team for the purpose of assessments.

Table 2. Sample User Role-Based Virtues

Document Editor/Creator/Printer Virtue
Internal SharePoint browser/reader Virtue
Active Directory Admin Virtue
SharePoint Admin Virtue
Router Admin Virtue
Internal Internet Consumer Virtue
External Internet Consumer (General) Virtue
Corporate Email user Virtue

1.A.5.1.4 Requirement 4 Virtues shall be built on a more defensible virtualized construct than the current general purpose VDI VM to address threats expected on a public cloud (see figure 3).

Discussion:

Proposers shall improve the following characteristics of the existing general purpose VDI VM construct:

- Existing VMs encourage the use of various user privilege levels and group memberships to access resources of different sensitivities within the same operating space. This increases the risk of privilege escalation and credential stealing.
- Existing VMs have few options to monitor internal behaviors reliably. Logging processes designed for this task reside in the same memory space as the untrusted users and processes they seek to monitor.
- Existing VMs currently have no ability to detect or deter attacks from peer workloads or from the underlying hypervisors that control them.
- Existing VDI offers no better resistance to external and internal attacks than legacy physical workstations that historically have been very prone to compromise
- Defenses against potential compromise that might be employed by VMs reside in the same processing space that may be compromised.

T&E team members will simulate the common threats expected from the commercial cloud and attempt to compromise performer's Virtues through a series of attacks that involve conventional external attacks, malicious insider attacks, peer guest attacks, and cloud provider memory snooping/alterations (see figure 3). Performers' Virtues should demonstrate resistance to these

attacks. At a minimum, Virtues should demonstrate the capability to log relevant events that could conceivably expose such attacks.

1. A.5.1.5 Requirement 5 Virtues shall offer numerous logging capabilities and be capable of dynamically adjusting their sensoring when commanded by the Analytics/Control Layer to address newly suspected threats.

Discussion:

Existing government UCE's running general purpose operating systems largely rely on resident software processes and agents to collect a preset type and amount of information about the user environment often without regard for the immediate needs of the upstream analytics ingesting them. This can result in the needless expense of computational resources with little security gain. To alleviate processing costs and improve security posture, Virtues should have a trust-worthy, well-defined means of capturing numerous types and amounts of user environment data dynamically (logging options). Ultimately the Virtue is being created for the use of future unspecified dynamic security analytics to detect and counter specific risks associated with the Virtue's role. Performers shall provide a well-defined programmatic capability (API) for the Analytics/Control Layer to both ascertain and request different amounts and types of user environment information available from a given Virtue. Performers should consider and counter the possibility of compromised exploitable processes or users within the Virtue attempting to interfere with logging efforts.

During examinations, The T&E team will create a simulated Analytics/Control Layer that will use the performer-provided API to request various logging options and access their accuracy. A log repository accessible by SFTP will be provided by the T&E team for performers to deposit all logs. The T&E team will expect all performers to demonstrate the capability of their Virtue to capture some basic prescribed Virtue logging options. However, performers will differentiate themselves through the extensibility of their Virtue to offer many logging options – To collect many types and categories of security relevant user environment data.

1.A.5.1.6 Requirement 6 Virtues shall offer numerous protection options tailored to the expected risks of the environment. They shall demonstrate the capability to respond dynamically by invoking various protections once security analytics determine the possibility of suspicious behavior.

Discussion:

Existing VMs have very little flexibility to adjust behavior to deal with possible attacks. Taking the VM offline or quarantining it from outside networks are actions that should be available in the case of a confirmed compromise. However in many cases, VMs may exhibit suspicious but non-conclusive behaviors. Currently security practitioners are confronted with the unenviable choice of either allowing the VM to continue serving the user or countering the threat by significantly impeding user processing. In numerous cases, user VMs are allowed to perform all permitted/possible tasks until compelling suspicious behavior warrants its suspension. Virtues

should offer numerous creative protection options to mitigate threats as the probabilities of a Virtue's compromise vary with additional data collected. Users should only be inconvenienced as much as required to address the likelihood and nature of the threat.

The T&E team will assess the quantity and effectiveness of Virtue protection options available to address varying degrees of suspicion or compromise. Performers should consider and counter the possibility of compromised exploitable processes or malicious users within the Virtue attempting to interfere with defensive actions.

1.A.5.1.7 Requirement 7 Virtues shall be capable of invoking and interacting with several legacy applications (including several Windows apps).

Discussion:

Certain user tasks can be assumed to require the use of legacy applications currently available in traditional VDI instantiations. For example, Adobe Acrobat could be required for an email user Virtue or Microsoft Publisher might be required for use in a document creator Virtue. To demonstrate the flexibility and practicality of a Virtue, performers shall be given a list of representative Windows and Linux applications that shall need to be able to be invoked and accessible in different Virtue instantiations. Initially it can be assumed that at a minimum all Office 2013 applications and common Windows administrative tools will be included in this list. Application invocation and interaction from within a Virtue does not necessarily imply execution within a Virtue. There is no innate requirement in this program for a required application to execute within a Virtue's own processing space. However vulnerabilities to the Virtue or its accessible resources that are introduced by executing an application within an external machine's processing space shall still need to be considered and mitigated by performers.

Support for intensive graphic applications like CAD/CAM or other 3D manipulation applications shall not be directly assessed as part of this effort. However, support for legacy applications presenting extensive 2D graphics, video and audio information shall be assessed. Users of Virtues may be assumed to have acquired the proper application software licensing to make a proposer's solution work.

1.A.5.1.8 Requirement 8 Virtues shall be capable of securely saving, passing, and retrieving basic state information (hyperlinks, file locations, individual files, default printers, etc.) with each other (Virtue-to-Virtue) and also with a secure Analytics/Control Layer (Virtue-to-Control Layer).

Discussion:

Certain Virtue roles may work more effectively if they are able to exchange limited data between each other in a secure manner. One example might be an email user Virtue that displays an email message with a hyperlink that the user wishes to explore. The email user Virtue might not have the applications or access to browse the site itself. Rather a user would require a specially created web-browsing Virtue for this task. Allowing the user to pass the hyperlink of interest

between the two Virtues would minimize the disruption the user would otherwise experience using these Virtues.

Proposers shall provide a method for users to create persistent settings from the presentation interface that do not undermine the immutable nature of Virtue images or the security of running Virtues. The user shall be able to use these persistent settings like default printers, home directories, and authorization tokens within their running Virtue once a user is properly authenticated.

Performers can demonstrate this persistence capability to the T&E team by providing an external storage capability within AWS for a Virtue to store and fetch this state information from.

1.A.5.1.9 Requirement 9 Proposers shall provide an intuitive presentation interface allowing access to numerous authorized Virtues to provide all the functionality required by a user delivered securely to an end device.

Discussion:

Users of Virtues shall require multiple different Virtues to accomplish their required roles. It is assumed that users shall access Virtues through some sort of minimal end device at their work locations, comparable to a generic thin client. It can be assumed the thin client is capable of basic compute and network tasks, but shall be unable to perform significant graphics and compute tasks locally. The network that exists between the thin client and the cloud provider is adequate to accommodate all remote desktop users of Citrix's current HDX remote viewing/access protocol.

The user of a Virtue should be presented with an interface on the thin client that enables him to interact with at least 6 different Virtues in an effective manner. Users should be able to select the Virtues they wish to invoke from a list of Virtues they are authorized to access. Presentation interface users should also be able to start up and stop individual Virtues on demand. Performers will need to create a basic methodology to accomplish this.

The T&E team will assess the capability of a performer's presentation interface to interact with a basic authentication/authorization service and to invoke and stop appropriate Virtues from the presentation interface. The T&E team will utilize a performer-provided basic authentication/authorization service when testing this.

1.A.5.1.10 Requirement 10 Virtues shall be capable of interacting with their environment in a performant manner.

Discussion:

Proposers shall need to devise a way for Virtues to authenticate and interact with existing network resources such as external file shares and printers in a way that is intuitive and convenient for users but that is also as secure as possible. In an ephemeral environment such as the cloud, permanent network resources such as printers and file servers are prized assets for an

adversary. Proposers should assume such assets shall be either the target or source of clever adversary attacks.

Virtues should attempt to minimize the amount of resources consumed to prevent greatly exceeding projected government cloud processing budgets. Measuring a solution's consumed resources in a large, shared cloud environment is notoriously tricky. Thankfully large cloud providers such as AWS have done much of the work by building measurement instrumentation and a rich set of related APIs to enable proposers to inspect the performance of their workloads (e.g. AWS CloudWatch). Additionally, cloud providers such as AWS have created a convenient method to assess the utilization of cloud resources consumed by a workload as a single cost per unit time.

These costs are publicly available for all consumers to view from the Amazon web site. As such, they can serve as a well-considered metric for the amount of resources a proposer's Virtue solution is expected to consume. Proposers can assume an average IC user shall use 6 Virtues for a total of 8 hours per day on the Amazon EC2 Infrastructure. A current IC-enhanced VDI can be assumed to require the resources of an on-demand Linux AWS m4.xlarge, US East region instance type which currently has an on-demand cost of .239 dollars per hour per instance.[1] This equates to a resource usage metric of $1.91 per user per day. Proposer solutions should attempt to minimize the overall cost per user per day metric accounting for the competing requirements of security, functionality, and performance.

For the purposes of this proposal, proposers are asked to discuss in as much detail as possible the types of AWS technologies such as the instance type, AMI, EBS, etc. that they will leverage and the reasons for these choices. For midterm and final examinations, proposers will be assessed on the AWS technologies they have chosen for their solutions. To ensure software licensing costs are not part of this resource utilization metric, instances/AMIs can be assumed to be using generic Linux pricing regardless of the actual operating systems used. For example:

> *Our Virtue solution requires the use of 1 Linux "g2.2xlarge" instance type to support a user computing environment consisting of 1 to 8 Virtues. We require this instance type because we need at least 6 vCPUs, 10GB of memory, a capable graphics processor to support lively streaming between the UCE interface and the thin client, SSD storage to support high random I/O rates and a platform providing VT-x capabilities, especially EPT support.*

During examinations, the T&E team will calculate two AWS cost-based performance metrics: the cost per user per day and cost per Virtue per day. These performance metrics will be based on the "on demand" service rate published by Amazon for all utilized resources proposed by a solution at the time of each examination. For our Virtue solution above, the Linux g2.2xlarge instance type in the US Eastern region with on demand pricing currently costs $.65 per hour for a daily Virtue user performance metric of $5.20.

[1] https://aws.amazon.com/ec2/pricing. Linux instances were chosen to remove the impact of licensing costs on the unit cost of solutions.

1.A.5.1.11 Requirement 11 Proposers shall provide methodology and utilities to define, construct, assure, and transport Virtue images.

Discussion:

Key to Virtues being an acceptable technology for virtualization designers, engineers and operators is a well thought out methodology for defining, constructing, and exchanging Virtue images. The proposer shall provide a method to define the credentials, resources, applications, default logging and default protections a Virtue shall possess and capture it in a Virtue image – a convenient package that enables a Virtue's use by multiple users at multiple locations. Virtue images should be immutable. Once a Virtue image is created, approved and deployed, patching an extant Virtue image is discouraged. Desired modifications to a Virtue image should result in a new version of a Virtue image replete with a new version number and associated hash value. User-created content that needs to persist—including preferences—should be stored separately from any Virtue-intrinsic file system. Virtue images should also be generic with respect to the individuals using them. Customizations to a Virtue to accommodate particular users (not roles) should be provided separately from the Virtue image (see Requirement 8).

As with docker images, Virtue images defined and tested by one trusted entity should be easily shared and extended by another entity without having to follow cumbersome recipes or copying multiple disparate files. Unlike docker images, Virtues should provide convenient, assured methods to ascertain both Virtue image software components and Virtue image creators. This enables security auditors to determine if Virtues possess software vulnerabilities that need to be mitigated or if an unauthorized Virtue is being offered for use. Additionally Virtue images should enable easy inspection of Virtue configuration settings to aid security auditors and IT professionals in assessing their capabilities and vulnerabilities.

1.A.6 Team Expertise

IARPA anticipates offeror teams may include, but are not limited to, experts in the following technical areas:

Operating Systems
Virtualization
Computer Security/Computer exploitation
Application Development and Optimization
Data analytics (to enable phase 1 performers to better understand the needs of Phase 2 analytic developers)
Secure Networking
Computer Security
Human Factors

1.A.7 Out of Scope

The following are examples of topics considered out of scope for this program:

- Changes to the underlying AWS infrastructure
- Recreating remote desktop access protocols such as PCoIP, HDX, Spice, VNC, RDP
- Hardware-dependent solutions – based on hardware not already planned for implementation by AWS on cloud production servers by January 2018.
- SEIM or data aggregation solutions
- Technology developed during this program which cannot be shared with the open source community (proposers may supplement their solution with existing, publicly available commercial technologies)
- Protections designed and suited specifically for server, HPC, or other low interaction computing workloads
- Approaches that propose or are likely to result in only modest improvements over the current state of the art (such as improving existing commercial technologies)

1.A.8 Threat Considerations

1. User-induced attacks (intentional or otherwise: insider threat, spearfishing, web exploits)
2. Peer-based attacks
3. Hypervisor-based attacks
4. External-based attacks
5. Consequences of a compromised Virtue

Not current focus:

1. Denial of Service attacks (DOS)
2. hardware alterations
3. Attacks directed against Phase 2 Analysis/Control Layer(except from Virtues)
4. Guest and hypervisor collusion attacks

1.B. Program Measurement and Schedule Waypoints

The Government shall use the Program Metrics listed below to evaluate the effectiveness of proposed solutions in achieving the stated program objectives, and to determine whether satisfactory progress is being made to warrant continued funding of the program. The metrics are intended to aid in the scoping of the effort, while affording maximum flexibility, creativity, and innovation in proposing solutions to the stated problem. The offeror is free to propose additional milestones and metrics to provide evidence that the technical and programmatic risks associated with their proposed approach are being addressed. Any such milestones and metrics shall be clear and well-defined, with a logical connection to offeror and/or Government decisions.

The VirtUE program is envisioned as a four-year effort that is intended to begin around June 2017. Phase 1 of the program (covered by this solicitation) shall last 18 months, and shall be structured as a technical development initiative addressing the eleven requirements listed previously. Phase 2 of the program is anticipated to be solicited in a separate BAA and is expected to last

approximately 21 months, with a one to three month overlap with the Phase 1 period of performance (see Figure 4). For Phase 1, each offeror team is expected to produce and publish a body of work that may be incorporated by future Phase 2 performers as part of one or more Phase 2 solutions. Successful Phase 2 performers may be offered the option of participating in Phase 3 at the government's discretion. Phase 3 shall create a fully functioning prototype using technologies developed in Phase 2 that runs within an IC enclave.

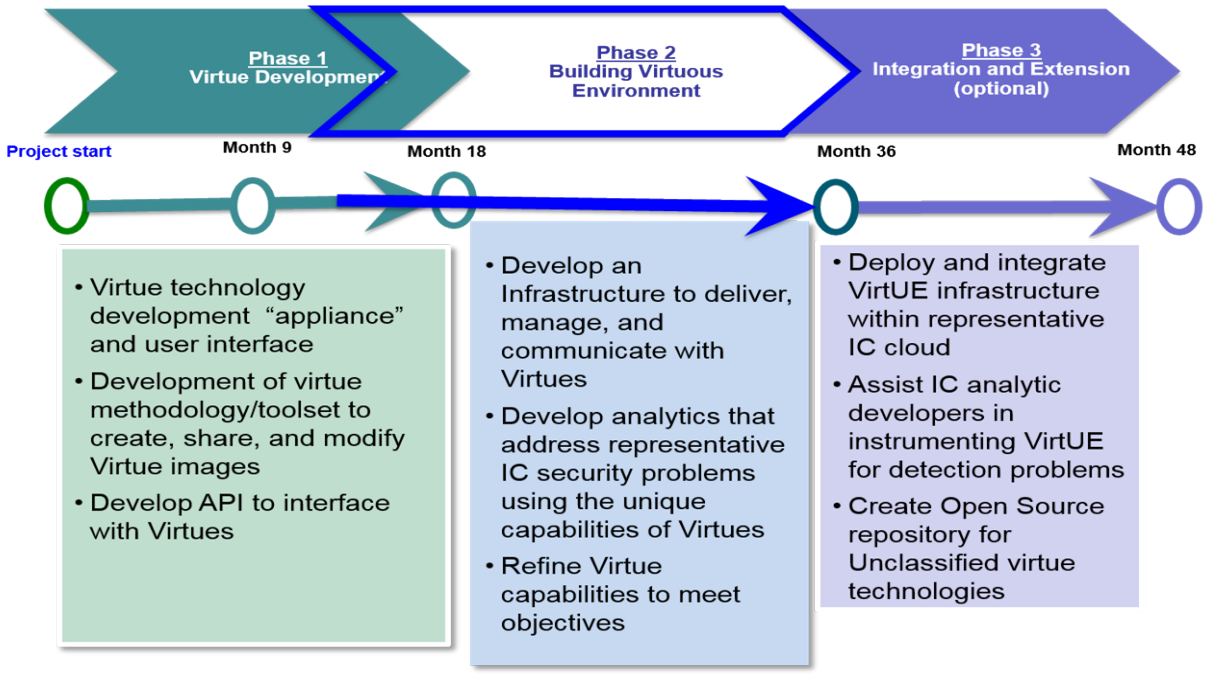


Figure 4. Tentative VirtUE Timeline

1.B.1 Program Metrics and Milestones

Phase 1 of the VirtUE program shall have two formal milestones: a mid-term and end-of-phase examination that shall assess performers' offerings against a detailed set of metrics to assess the effectiveness of their efforts in meeting program objectives.

1.B.1.1 Purpose:

Ultimately the purpose of Phase 1 metrics and milestones is to produce technologies that can be used by Phase 2 performers to build the virtuous user environment. Phase 2 performers shall be responsible for the performance and security of any Phase 1 technologies they incorporate into their solutions. The intent is for Phase 1 midterm and final examination results to enable Phase 2 performers to better assess the potential of Phase 1 offerings to meet their needs.

1.B.1.2 Test and Evaluation (T&E) Examinations

In months 9 and 18 performers shall travel to the Government-selected test and evaluation (T&E) facilities at the Johns Hopkins University Applied Physics Lab (APL) outside Baltimore, MD to undergo examinations that shall provide a midterm and end-of-phase assessment of their solution's performance. For planning purposes, proposers should allow three days for interactive testing at JHU APL for each examination. Performers will be expected to deliver all software and documentation required for APL to adequately assess their offering to T&E team members one week prior to examinations. T&E team members will be responsible for instrumenting and creating a testing environment within AWS to assess offerors' solutions against the requirements of the program.

1.B.1.3 Proposed Measurement Criteria for VirtUE Phase 1:

Performers' solutions shall be measured using the following general criteria when addressing program requirements:

Security Test Criteria – A Virtue is better able to deter, detect, and/or mitigate representative attacks that target user computing environments.

Detection and mitigation capabilities will be evaluated during Phase 2. In Phase 1, performers shall demonstrate a Virtue's ability to deter attacks through inherent security properties such as attack surface, logging capabilities, and available protection options. Additionally, two simulated Red Team exercises will be conducted against a performer's submission to test the overall deterrence capabilities of performer's solutions. The first test will assess deterrence based on a Virtue with generic default logging & protection options present. The second test will assess deterrence based on performer customized logging & protection options. For the second test, performers will be able to submit configurations for each threat category the Red Team will simulate (see Figure 3).

Functionality Test Criteria – A Virtue shall meet all program requirements while providing users an experience that compares favorably with existing government VDI environment.

A solution's functionality will mainly be measured through simple checklists of required attributes. The usability portion of functionality may be assessed through measuring the time it takes users to accomplish certain tasks with Virtues and/or through user surveys assessing effectiveness.

Performance Test Criteria – A Virtue shall be able to satisfy criteria under processing loads expected within the government cloud using available computational resources

Extensive instrumentation within the T&E team's test environment will assess the resources expended and time taken by a Performer's Virtues in undertaking numerous tasks.

1.B.1.4 Phase 1 Preliminary Metrics and Goals:

In Table 2A, Phase 1 preliminary performance metrics/goals are provided and mapped to corresponding Phase 1 program requirements to enable proposers to better design and assess potential solutions. These metrics and goals may be altered based on further research by the T&E team.

Table 2A. Preliminary Metrics

RID	Requirement Synopsis	Metric ID	Metric Statement	Measurement Type	Functional	Security	Performance
2	Virtues shall present themselves as atomic, largely immutable entities to other Virtues and external processes. They shall be simpler and more modular than current VDI solutions with a minimized attack surface	2.a	The number of exposed system calls in the exposed portion of a Virtue	count <= 200		X	X
		2.b	The number of running processes in the exposed portion of a Virtue	count <= 20		X	X
		2.c	The number of active/available services in the exposed portion of a Virtue	count <= 45		X	X
		2.d	The number of communication paths that traverse a Virtue trust boundary	count <= 3		X	
		2.e	The number of credentials in the exposed portion of a Virtue	count = 1		X	
4	Virtues shall be built on a more defensible virtualized construct than the current general	4.a	The success rate and performance cost of a Virtue with default protections in deterring attacks to each of the four vectors (success rate = foiled attacks/total attacks per category; Performance cost = Cost of memory and processing for protections): • external	cost TBD ratios 50%		X	

	purpose VDI VM to address threats expected on a public cloud		**• internal/insider • peer • hypervisor/management layer**	**50% 25% 25%**			
5	**Virtues shall offer numerous logging capabilities and be capable of dynamically adjusting their sensoring when commanded by the Analytics/Control Layer to address newly suspected threats**	**5.a**	**The number of unique hypervisor & network logging options that Virtue logging can capture**	**number >= 30**		**X**	
		5.b	**The number of unique internal logging options that Virtue logging can capture**	**number >= 100**		**X**	
6	**Virtues shall offer numerous protections tailored to the expected risks of the environment. They shall demonstrate the capability to respond dynamically once security analytics determine the**	**6.a**	**The number of unique protections against network and hypervisor based attacks provided by a Virtue**	**number >= 30**		**X**	
		6.b	**The number of unique insider threat protections provided by a Virtue**	**number >= 10**		**X**	

	possibility of suspicious behavior	6.c	The success rate and performance cost of a Virtue with all pertinent protections deployed in deterring attacks to each of the four vectors (success rate = foiled attacks/total attacks per category; Performance cost = Cost of memory and processing for protections): • external • internal/insider • peer • hypervisor/management layer	cost TBD ratios 75% 75% 50% 50%		X	
7	Shall be capable of invoking and interacting with several legacy applications (including several Windows apps)	7.a	The proportion of Windows applications from a supplied list that are able to be successfully invoked from within a Virtue	ratio 70%	X		
		7.b	The proportion of Linux applications from a Government-supplied list that are able to be successfully invoked from within a Virtue	ratio 90%	X		
9	A presentation interface combining numerous authorized Virtues to provide all the functionality required by a user are delivered securely to an end device	9.a	The Virtue's thin client interface shall enable a user to access and interact with 6 different unique Virtues within x seconds	time <= 30 sec	X		X
		9.b	An user shall successfully complete a functional use case that involves starting, accessing, and terminating a Virtue within x minutes	time <= 1 min			X
10	Capable of interacting with its environment in a performant manner	10.a	A performer shall minimize the amount of AWS resources (compute, memory, storage, and network) consumed by representative Virtues as measured by: • cost per Virtue / per Day • cost per User / per Day	cost <$1.00 < $4.00			X

		10.b	**Average processing and memory usage for prescribed logging and protection processes over total amount of Virtue processing and memory usage for several use cases**	**ratio < 30%**			**X**
11	**Methodology and utilities to define, construct, assure and transport Virtue images**	**11.a**	**An end-to-end execution of the methodology to define and construct Virtue images shall be completed within x**	**time <= 15 min**	**X**		
		11.b	**The completeness and accuracy of the Virtue image self-reported contents as compared to inspection results**	**ratio > 95%**	**X**		

1.B.2 Government Furnished Information (GFI)

After program award, selected teams shall be provided the following information:

- An updated set of metrics participants will be assessed against during midterm and final milestone examinations
- Monthly technical, financial and final report template
- A list of specific user role-based Virtues performers will need to demonstrate for tests
- A list of basic logging and protection options for a Virtue to demonstrate
- A list of specific legacy applications that a Virtue will need to support
- A detailed description of the network resources Virtues will need to interface with
- A description of the type of attacks that testers will employ against performers' offerings
- Requirements for interacting with the testing rig

1.C. Program Timeline and Deliverables

Performers shall be responsible at the end of Phase 1 for delivering technologies, code, and explanatory documentation to the government that would enable a consumer with moderate computer knowledge the ability to successfully deploy and interact with a provider's Virtue solution within the AWS environment. Additionally providers shall make all technologies and documentation developed using IARPA funds, publically available to the open source community via GitHub under the terms of the GNU General Public License (GPL) 3.0.

At the end of Phase 1, performers shall also be responsible for creating an academic quality publication based on their VirtUE program work that they will submit both to the government

and to a tier one conference and/or journal recognized by the field. Additional required deliverables are detailed in Table 3.

If performers' solutions incorporate pre-existing, publicly available commercial technology components, these components will not be delivered to the government nor published online. Rather performers shall publish instructions on how to obtain the necessary commercial technology along with the methods required to integrate these commercial technologies with the performer's technical solution.

The Government shall use the following review and deliverables chart with programmatic gates to help the program maintain its 18-month program schedule:

Table 3. Program Review and Deliverables

Deliverable	Month
Kickoff meeting. Presentation package detailing updated technical approach and research work plan	1
On-site visit. Reports on technical progress, details of successes and issues, contributions to the Program objectives, and technology demonstrations shall be expected	4,(12-if necessary)
Testing and assessment at Government T&E Facility.	9,18
Washington metro area performer briefings at Phase 2 Proposers' Day	11
Submit a paper describing research to a tier one conference or journal recognized by the field, and publicly post source code of all deliverables	18
Software and documentation published and available for Phase 2 performers	18
Final report describing traceability to Phase 1 objectives. Format provided upon contract award.	18
Monthly technical and financial reports per 6.B.8.	Monthly, by 10th day of following month.
Monthly teleconferences	Monthly, in conjunction with technical report

Table 3 also includes a schedule for the key deliverables the performer shall provide. The offeror may add other deliverables in addition to the minimum set listed in the table.

1.D. Meeting and Travel Requirements

Performers are expected to assume responsibility for administration of their projects and to comply with contractual and Program requirements for reporting, attendance at Program workshops, and availability for site visits.

Table 4. Meetings and Locations Anticipated

Meeting Title	Location	Duration	Month

Kickoff Workshop	Washington, DC	1-2 business days	Month 1
Site Visit	Contractor Site	1-2 business days	Month 4
Midterm Waypoint Exam	Baltimore, MD	3 business days	Month 9
Phase 2 Proposers' Day Workshop	Washington, DC	1 business day	Month 11
Optional Site Visit	Contractor Site	1 business day	Month 12-18
Final Waypoint Exam	Baltimore, MD	3 business days	Month 18

1.D.1 Workshops

The VirtUE Phase 1 Program intends to hold a Kick-Off meeting for all chosen offerors during the first month of the Program. Additionally all offerors shall be expected to present their current results at the Phase 2 Proposers' Day, which is anticipated to occur during month 11 of the Program.

1.D.2. Site Visits

Site visits by the Contracting Officer Representative and the VirtUE Program Manager shall generally take place up to twice during the life of the Program. The first site visit shall occur by month 4 and the second shall occur between month 10 and 18 if needed. These visits shall occur at the Contractor's facility. Reports on technical progress, details of successes and issues, contributions to the Program objectives, and technology demonstrations shall be expected at such visits.

1.E. Place of Performance

Performance shall be conducted at the contractor site(s) specified by the offeror.

1.F. Period of Performance

The VirtUE Program (Phase 1) is envisioned as an 18-month effort that is intended to begin June 2017.

For situational awareness, Phase 2 of the program is anticipated to be solicited in a separate BAA and is expected to last approximately 21 months, with a one-to-three month overlap with the Phase 1 period of performance.

SECTION 2: AWARD INFORMATION

The BAA shall result in awards for Phase 1. Subsequent phases shall be covered by separate solicitation(s). Multiple awards are anticipated. The amount of resources made available under this BAA shall depend on the quality of the proposals received and the availability of funds.

The Government reserves the right to select for negotiation all, some, one, or none of the proposals received in response to this solicitation and to make awards without discussions with

offerors. The Government also reserves the right to conduct discussions if the Source Selection Authority determines them to be necessary. Additionally, IARPA reserves the right to accept proposals in their entirety or to select only portions of proposals for negotiations for award. In the event that IARPA desires to award only portions of a proposal, negotiations may be opened with that offeror.

Awards under this BAA shall be made to offerors on the basis of the Evaluation Criteria listed in Section 5, program balance, and availability of funds. Proposals selected for negotiation may result in a procurement contract. However, the Government reserves the right to negotiate the type of award instrument it determines appropriate under the circumstances.

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

SECTION 3: ELIGIBILITY INFORMATION

3.A. Eligible Applicants

All responsible sources capable of satisfying the Government's needs may submit a proposal. Historically Black Colleges and Universities (HBCUs), Small Businesses, Small Disadvantaged Businesses and Minority Institutions (MIs) are encouraged to submit proposals and join others in submitting proposals; however, no portion of this announcement shall be set aside for these organizations' participation due to the impracticality of reserving discrete or severable areas for exclusive competition among these entities. Other Government Agencies, Federally Funded Research and Development Centers (FFRDCs), University Affiliated Research Centers (UARCs), Government-Owned, Contractor-Operated (GOCO) facilities, Government Military Academies, and any other similar type of organization that has a special relationship with the Government, that gives them access to privileged and/or proprietary information or access to Government equipment or real property, are not eligible to submit proposals under this BAA or participate as team members under proposals submitted by eligible entities. An entity of which only a portion has been designated as a UARC may be eligible to submit a proposal or participate as a team member subject to an organizational conflict of interest review described in section 3.A.1.

Foreign entities and/or individuals may participate to the extent that such participants comply with any necessary Non-Disclosure Agreements, Security Regulations, Export Control Laws and other governing statutes applicable under the circumstances. Proposers are expected to ensure that the efforts of foreign participants do not either directly or indirectly compromise the laws of the United States, nor its security interests. As such, offerors should carefully consider the roles and responsibilities of foreign participants as they pursue teaming arrangements.

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

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

If a prospective offeror, or any of its proposed subcontractor teammates, believes that a potential conflict of interest exists or may exist (whether organizational or otherwise), the offeror should promptly raise the issue with IARPA and submit a notification by e-mail to the mailbox address for this BAA at dni-iarpa-baa-16-12@iarpa.gov. All notifications shall be submitted through the prime offeror, regardless of whether the notification addresses a potential OCI for the offeror or one of its subcontractor teammates. A potential conflict of interest includes, but is not limited to, any instance where an offeror, or any of its proposed subcontractor teammates, is providing either scientific, engineering and technical assistance (SETA) or technical consultation to IARPA. In all cases, the offeror shall identify the contract under which the SETA or consultant support is being provided. Without a waiver from the IARPA Director, neither an offeror, nor its proposed subcontractor teammates, can simultaneously provide SETA support or technical consultation to IARPA and compete or perform as a Performer under this solicitation.

All facts relevant to the existence of the potential conflict of interest, real or perceived, should be disclosed in the notification. The request should also include a proposed plan to avoid, neutralize or mitigate such conflict. The offeror, or subcontractor teammate as appropriate, shall certify that all information provided is accurate and complete, and that all potential conflicts, real or perceived, have been disclosed. Offerors may submit this notification after release of the BAA, however, the Government may not respond prior to the proposal due date. Submission of a proposal is not dependent on a Government response. If, in the sole opinion of the Government, after full consideration of the circumstances, the conflict situation cannot be resolved or waived, any proposal submitted by the offeror that includes the conflicted entity shall be excluded from consideration for award.

As part of their proposal, offerors who have identified any potential conflicts of interest shall include either an approved waiver signed by the IARPA Director, an IARPA Determination letter stating that no conflict of interest exists, or a copy of their notification. Otherwise, offerors shall include in their proposal a written certification that neither they nor their subcontractor teammates have any potential conflicts of interest, real or perceived. A sample certification is provided in APPENDIX D.

If, at any time during the solicitation or award process, IARPA discovers that an offeror has a potential conflict of interest and no notification has been submitted by the offeror, IARPA reserves the right to immediately withdraw the proposal from further consideration for award.

Offerors are strongly encouraged to read "Intelligence Advanced Research Projects Activity's (IARPA) Approach to Managing Organizational Conflicts of Interest (OCI)", found on IARPA's website at: http://www.iarpa.gov/index.php/working-with-iarpa/iarpas-approach-to-oci.

3.A.2 Multiple Submissions to the BAA

Organizations may participate in more than one submission to the BAA, IARPA-BAA-16-12. However, if multiple submissions to the BAA which include a common team member are selected, IARPA shall, at contract negotiation, ensure that there is no duplicative funding, i.e. no one entity can be paid twice to perform the exact same task.

3.B. US Academic Organizations

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

It is ***highly*** recommended that offerors submit with their proposal a completed and signed Academic Institution Acknowledgement Letter for each U.S. academic institution that is a part of their team, whether the academic institution is serving in the role of prime, or a subcontractor or consultant at any tier of their team. A template of the Academic Institution Acknowledgement Letter is enclosed in APPENDIX A of this BAA. It should be noted that an appropriate senior official from the institution, i.e., typically the President, Chancellor, Provost, or other appropriately designated official, shall sign the completed form. Note that this paperwork **shall** be received before IARPA can enter into any negotiations with any offeror when a U.S. academic organization is a part of its team.

3.C. Other Eligibility Criteria

3.C.1. Collaboration Efforts

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

SECTION 4: PROPOSAL AND SUBMISSION INFORMATION

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

4.A. Proposal Information

Interested offerors are required to submit full proposals in order to receive consideration for award. All proposals submitted under the terms and conditions cited in this BAA shall be reviewed. Proposals shall be received by the time and date specified in section 4.C.1 in order to be assured of consideration during the initial round of selections. IARPA may evaluate

proposals received after this date but prior to BAA closing. Selection remains contingent on the evaluation criteria, program balance and availability of funds. The typical proposal should express a consolidated effort in support of one or more related technical concepts or ideas. Disjointed efforts should not be included in a single proposal.

The Government intends to use employees of Booz Allen Hamilton, SCITOR Corporation, TASC, Vencore, Welkin Associates, BRTC Federal Solutions, Comtech Telecommunications Corporation, and Ops Consulting LLC to provide expert advice regarding portions of the proposals submitted to the Government and to provide logistical support in carrying out the evaluation process. These personnel shall have signed and be subject to the terms and conditions of non-disclosure agreements. By submission of its proposal, an offeror agrees that its proposal information may be disclosed to employees of these organizations for the limited purpose stated above. Offerors who object to this arrangement shall provide clear notice of their objection as part of their transmittal letter. If offerors do not send notice of objection to this arrangement in their transmittal letter, the Government shall assume consent to the use of contractor support personnel in assisting the review of submittal(s) under this BAA.

Only Government personnel shall make evaluation and award determinations under this BAA.

All administrative correspondence and questions regarding this solicitation should be directed by email to dni-iarpa-baa-16-12@iarpa.gov. Proposals shall be submitted in accordance with the procedures provided in Section 4.C.2.

4.B. Proposal Format and Content

All proposals shall be in the format given below. Non-compliant proposals may be rejected without review. Proposals shall consist of two volumes: "Volume 1 - Technical and Management Proposal" and "Volume 2 - Cost Proposal." All pages shall be printed on 8-1/2 by 11 inch paper and IARPA desires that the font size not be smaller than 12 point. IARPA desires that the font size for figures, tables and charts not be smaller than 10 point. All contents shall be clearly legible with the unaided eye. Excessive use of small font, for other than figures, tables, and charts or unnecessary use of figures, tables, and charts to present information may render the proposal non-compliant. Foldout pages shall not be used. The page limitation for full proposals includes all figures, tables, and charts. All pages should be numbered. Unnecessarily elaborate brochures or presentations beyond what is sufficient to present a complete and effective proposal are not acceptable and shall be discarded without review

The Government anticipates proposals submitted under this BAA shall be UNCLASSIFIED.

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

Volume 1 – Technical & Management Proposal (Limit to 35 Pages)
Section 1 - Cover Sheet & Transmittal Letter
Section 2 – Summary of Proposal (Estimated not to exceed 10 pages)
Section 3 – Detailed Proposal

Section 4 – Attachments (Not included in page count, but number appropriately for elements included)

1 – Academic Institution Acknowledgment Letter Template, if required
2 – Restrictions on Intellectual Property Rights
3 – OCI Waiver, Determination, Notification or Certification
4 – Bibliography
5 – Relevant Papers (up to three)
6 – Consultant Letters of Commitment
7 – A Three Chart Summary of the Proposal (see APPENDIX H)

Volume 2 – Cost Proposal
Section 1 – Cover Sheet
Section 2 – Estimated Cost Breakdown
Section 3 – Supporting Information

4.B.1. Volume 1, Technical and Management Proposal {Limit of 35 pages}

Volume 1, Technical and Management Proposal, may include an attached bibliography of relevant technical papers or research notes (published and unpublished) which document the technical ideas and approach on which the proposal is based. Copies of not more than three relevant papers can be included with the submission. The submission of other supporting materials along with the proposal is strongly discouraged and shall not be considered for review. Except for the cover sheet, transmittal letter, table of contents (optional), and the attachments included in Volume 1, Section 4. Volume 1 shall not exceed 35 pages. Any pages exceeding this limit shall be removed and not considered during the evaluation process. Full proposals should be accompanied by an official transmittal letter, using contractor format. All full proposals shall be written in English.

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

A. Cover sheet: (*See APPENDIX B for Cover Sheet Template*)
B. Official Transmittal Letter.

4.B.1.b. Section 2: Summary of Proposal (Estimated not to exceed 10 pages)

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

A. A technical overview of the proposed research and plan. This section is the centerpiece of the proposal and shall succinctly describe the proposed approach and research. The overview shall provide an intuitive understanding of the approach and design, technical rationale, and constructive plan for accomplishment of technical objectives and deliverable production. The approach shall be supported by basic, clear calculations. Additionally,

proposals shall clearly explain the innovative claims and technical approaches that shall be employed to meet or exceed each program metric and provide ample justification as to why approaches are feasible. The use of non-standard terms and acronyms should be avoided. This section shall be supplemented with a more detailed plan in Volume 1, Section 3 of the proposal.

B. Summary of the products, transferable technology and deliverables associated with the proposed research results. Define measurable deliverables that show progress toward achieving the stated Program Milestones. All proprietary claims to the results, prototypes, intellectual property, or systems supporting and/or necessary for the use of the research, results, and/or prototype shall be detailed in Attachment 2. If there are no proprietary claims, this should be stated. Should no proprietary claims be made, Government rights shall be unlimited.

C. Schedule and milestones for the proposed research. Summarize, in table form and clearly legible for all activity, the schedule and milestones for the proposed research. Do not include proprietary information with the milestones.

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

E. Project contributors. Include a clearly defined and clearly legible organizational chart of all anticipated project participants, organized under functional roles for the effort, and also indicating associated task number responsibilities with individuals.

F. Technical Resource Summary:
- Summarize total level of effort by labor category and technical discipline (i.e. research scientist/chemist/physicist/engineer/administrative, etc.) and affiliation (prime/ subcontractor/consultant). Key Personnel shall be identified by name. Provide a brief description of the qualifications for each labor category (i.e. education, certifications, years of experience, etc.)
- Summarize level of effort by labor category and technical discipline for each major task, by affiliation
- Identify software and intellectual property required to perform, by affiliation (List each item separately)
- Identify materials and equipment (such as IT) required to perform, by affiliation (List each item separately)
- Identify any other resources required to perform (i.e. services, data sets, facilities, government furnished property, etc., by affiliation, list each item separately)
- Estimated travel, including purpose of travel and number of personnel per trip, by affiliation

The above information shall cross reference to the tasks set forth in the offerors statement of work, as described in BAA section 4.B.1.c, and shall be supported by the detailed cost and pricing information provided in the offeror's Volume 2 Cost Proposal.

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

This section of the proposal shall provide the detailed, in-depth discussion of the proposed research as well as supporting information about the offeror's capabilities and resources. Specific attention shall be given to addressing both the risks and payoffs of the proposed research and why the proposed research is desirable for IARPA to pursue. This part shall provide:

A. Statement of Work (SOW) - In plain English, clearly define the technical tasks and sub-tasks to be performed, their durations and the dependencies among them. For each task and sub-task, provide:
   - A general description of the objective;
   - A detailed description of the approach to be taken, developed in an orderly progression and in enough detail to establish the feasibility of accomplishing the goals of the task;
   - Identification of the primary organization responsible for task execution (prime, sub-contractor, team member, etc.) by name;
   - The exit criteria for each task/activity, i.e., a product, event or milestone that defines its completion;
   - Definition of all deliverables (e.g., data, reports, software, etc.) to be provided to the Government in support of the proposed research tasks/activities.

   Note: Do not include any proprietary information in the SOW.

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

B. A detailed description of the objectives, scientific relevance, technical approach and expected significance of the work. The key elements of the proposed work should be clearly identified and related to each other. Proposals should clearly detail the technical methods and/or approaches that shall be used to meet or exceed each program milestone, and should provide ample justification as to why the proposed methods/approaches are feasible. Any anticipated risks should be described and possible mitigations proposed. General discussion of the problem without detailed description of approaches, plausibility of implementation, and critical metrics shall result in an unacceptable rating.

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

D. Data sources. Identification and description of data sources to be utilized in pursuit of the project research goals.

Offerors proposing to use existing data sets shall provide written verification that all data were obtained in accordance with U.S. laws and, where applicable, are in compliance with End User License Agreements, Copyright Laws, Terms of Service, and laws and policies regarding privacy protection of U.S. Persons. Offerors shall identify any restrictions on the use or transfer of data sets being used, and, if there are any restrictions, the potential cost to the Government to obtain at least Government Purpose Rights in such data sets.[2]

Offerors proposing to obtain new data sets shall ensure that their plan for obtaining the data complies with U.S. Laws and where applicable, with End User License Agreement, Copyright Laws, Terms of Service, and laws and policies regarding privacy protection of U.S. Persons.

The Government reserves the right to reject a proposal if it does not appropriately address all data issues.

E. Deliverables. Deliverables are identified in Section 1.C.

The Government requires at a minimum Government Purpose Rights for all deliverables; anything less shall be considered a weakness in the proposal. However, if limited or restricted rights are asserted by the offeror in any deliverable or component of a deliverable, the proposal shall identify the potential cost associated with the Government obtaining Government Purpose Rights in such deliverables. Proposals that do not include this information shall be considered non-compliant and may not be reviewed by the Government.

In Attachment 2 of the proposal, offerors shall describe the proposed approach to intellectual property for all deliverables, together with a supporting rationale of why this approach is in the Government's best interest. This shall include all proprietary claims to the results, prototypes, intellectual property or systems supporting and/or necessary for the use of the research, results and/or prototype, and a brief explanation of how the offerors may use these materials in their program. To the greatest extent feasible, offerors should not include background proprietary technical data and computer software as the basis of their proposed technical approach.

[2] "Government Purpose Rights" (or "GPR") means the rights to use, modify, reproduce, release, perform, display, or disclose technical data and computer software within the Government without restriction; and to release or disclose technical data and computer software outside the Government and authorize persons to whom release or disclosure has been made to use, modify, reproduce, release, perform, display, or disclose that data or software for any United States Government purpose. United States Government purposes include any activity in which the United States Government is a party, including cooperative agreements with international or multi-national defense organizations, or sales or transfers by the United States Government to foreign governments or international organizations. Government purposes include competitive procurement, but do not include the rights to use, modify, reproduce, release, perform, display, or disclose technical data or computer software for commercial purposes or authorize others to do so.

If offerors (including their proposed teammates) desire to use in their proposed approach, in whole or in part, technical data or computer software or both that is proprietary to offeror, any of its teammates, or any third party, in Attachment 2 they should: (1) clearly identify such data/software and its proposed particular use(s); (2) identify and explain any and all restrictions on the Government's ability to use, modify, reproduce, release, perform, display, or disclose technical data, computer software, and deliverables incorporating such technical data and computer software; (3) identify the potential cost to the Government to acquire GPR in all deliverables that use the proprietary technical data or computer software the offeror intends to use; (4) explain how the Government shall be able to reach its program goals (including transition) within the proprietary model offered; and (5) provide possible nonproprietary alternatives in any area in which a Government entity would have insufficient rights to transfer, within the Government or to Government contractors in support of a Government purpose, deliverables incorporating proprietary technical data or computer software, or that might cause increased risk or cost to the Government under the proposed proprietary solutions.

Offerors also shall identify all commercial technical data and/or computer software that may be embedded in any noncommercial deliverables contemplated under the research effort, along with any applicable restrictions on the Government's use of such commercial technical data and/or computer software. If offerors do not identify any restrictions, the Government shall assume that there are no restrictions on the Government's use of such deliverables. Offerors shall also identify all noncommercial technical data and/or computer software that it plans to generate, develop and/or deliver under any proposed award instrument in which the Government shall acquire less than unlimited rights. If the offeror does not submit such information, the Government shall assume that it has unlimited rights to all such noncommercial technical data and/or computer software. Offerors shall provide a short summary for each item (commercial and noncommercial) asserted with less than unlimited rights that describes the nature of the restriction and the intended use of the intellectual property in the conduct of the proposed research.

Additionally, if offerors propose the use of any open source or freeware, any conditions, restrictions or other requirements imposed by that software shall also be addressed in Attachment 2. Offerors should leverage the format in APPENDIX G for their response. (See also section 6.B.2. Intellectual Property). The technical content of Attachment 2 shall include only the information necessary to address the proposed approach to intellectual property; any other technical discussion in Attachment 2 shall not be considered during the evaluation process. Attachment 2 is estimated not to exceed 4 pages.

For this solicitation, IARPA recognizes only the definitions of intellectual property rights in accordance with the terms as set forth in the Federal Acquisition Regulation (FAR) part 27, or as defined herein. If offerors propose intellectual property rights that are not defined in FAR part 27 or herein, offerors shall clearly define such rights in Attachment 2 of their proposal. Offerors are reminded of the requirement for prime contractors to acquire sufficient rights from subcontractors to accomplish the program goals.

F. Cost, schedule, milestones. Cost, schedule, and milestones for the proposed research, including estimates of cost by task, total cost, and company cost share, if any. The milestones shall not include proprietary information.

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

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

I. Detailed Management Plan. The Management Plan should identify both organizations and individuals within organizations that make up the team, and delineate the expected duties, relevant capabilities, and task responsibilities of team members and expected relationships among team members. Expected levels of effort (percentage time or fraction of an FTE) for all key personnel and significant contributors should be clearly noted. A description of the technical, administrative and business structure of the team and the internal communications plan should be included. Project/function/sub-contractor relationships (including formal teaming agreements), Government research interfaces, and planning, scheduling, and control practices should be described. The team leadership structure should be clearly defined. Provide a brief biography of the key personnel (including alternates, if desired) who shall be involved in the research along with the amount of effort to be expended by each person during the year. Participation by key personnel and significant contributors is expected to exceed **(25%)** of their time. A compelling explanation is required for any variation from this figure.

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

A table such as the following (**Table 5**) is recommended.

Table 5. Team Organization

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

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

K. The names of other federal, state or local agencies or other parties receiving the proposal and/or funding the proposed effort. If none, so state.

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

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

Attachment 1: Signed Academic Institution Acknowledgement Letter(s) (if applicable). Template provided as APPENDIX A. See paragraph 3.B, US Academic Institutions.

Attachment 2: Restrictions on Intellectual Property Rights (if applicable). Template provided as APPENDIX G. This attachment is estimated not to exceed 4 pages.

Attachment 3: OCI Waiver/Determination/Notification or Certification. Template, provided as APPENDIX D. See paragraph 3.A.1., Organizational Conflicts of Interest (OCI).

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

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

Attachment 6: Consultant Commitment Letters. If needed.

Attachment 7: A Three Chart Summary of the Proposal. A PowerPoint summary that quickly and succinctly indicates the concept overview, key innovations, expected impact, and other unique aspects of the proposal. The format for the summary slides is included in APPENDIX H to this BAA and does not count against the page limit. Slide 1 should be a self-contained, intuitive description of the technical approach and performance. These slides may be used during the evaluation process to present a summary of the proposal from the proposers view.

4.B.2. Volume 2: Cost Proposal {No Page Limit}

The Offeror's proposal shall contain sufficient factual information to establish the offeror's understanding of the project, the perception of project risks, the ability to organize and perform the work and to support the realism and reasonableness of the proposed cost.

IARPA recognizes that undue emphasis on cost may motivate offerors to offer low-risk ideas with minimum uncertainty and to staff the effort with junior personnel in order to be in a more competitive posture. IARPA discourages such cost strategies. Cost reduction approaches that shall be received favorably include innovative management concepts that maximize direct funding for technology and limit diversion of funds into overhead.

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

See APPENDIX C, Cover Sheet Template

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

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

A. Completed Cost/Price Template - Offerors shall submit a cost element breakdown for the base period, each option period and the total program summary in the format provided in APPENDIX E[3].

[3] **NOTE:** Educational institutions and non-profit organizations as defined in FAR Part 31.3 and 31.7, respectively, at the prime and subcontractor level may deviate from the cost template in APPENDIX E and APPENDIX F when

B. Subcontractor/Inter-organizational Transfers (IOTs) and Consultants summary in the format provided in APPENDIX F. (After selection, offerors may be required to submit full cost proposals, see 4.B.2.c. Subcontracts.)
C. Total cost broken down by major task (Requirements 1 thru 11 per Section 1.A.5))
D. Major program tasks by fiscal year
E. A summary of projected funding requirements by month
F. A summary table listing all labor categories used in the proposal and their associated direct labor rates, along with escalation factors used for each base and option period of the acquisition.
G. A summary table listing all indirect rates used in the proposal for each for each base and option period of the acquisition.

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

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

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

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

Subcontracts (to include consultants and IOTs) – The offeror is responsible for compiling and providing all subcontractor proposals with the Cost Volume. Subcontractor cost element sheets shall be completed for the base period, each option period and the total summary in the format provided in APPENDIX F (Excel is not required for initial submittal, see paragraph below). Consultant letter(s) of commitment shall also be attached.

If a proposal is selected for negotiations, the prime shall be prepared to present full subcontractor proposals (if applicable per subcontract type) for the base period, each

---

estimating the direct labor portion of the proposal to allow for OMB guided accounting methods (2 CFR Part 220) that are used by their institutions. The methodology shall be clear and provide sufficient detail to substantiate proposed labor costs. For example, each labor category shall be listed separately; identify key personnel, and provide hours/rates or salaries and percentage of time allocated to the project.)

option period and total cost summary including all direct and indirect costs immediately upon request by the Contracting Officer. Information shall be presented in Excel with intact formulas using the format provided in APPENDIX E and addressing the supporting cost information as outlined in 4.B.2.b. and 4.B.2.c. In addition to the full and complete subcontractor cost proposal, the offeror shall also provide its analysis of the subcontractor's proposal including justification for why the subcontractor was selected and its determination that the cost/price is fair and reasonable (Reference FAR Part 44 and FAR clause 52.244-2). If subcontractors have concerns about proprietary cost information, subcontractors can submit their detailed cost proposals directly to the Contracting Officer.

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

Other Direct Costs (ODCs) and Travel – ODCs shall be listed separately and supported by quotes, historical data or any other information including the offeror's analysis. The proposed travel supporting detail shall include destination and purpose of the trip, number of travelers per trip and price per traveler in sufficient detail to verify the BOE. Proposed travel costs shall comply with the limitations set forth in FAR Part 31.

Government Purpose Rights - If the offeror asserts limited or restricted rights in any deliverable or component of a deliverable, the cost proposal shall separately identify the estimated cost associated with the Government obtaining Government Purpose Rights in such deliverables (reference sections 4.B.1.c.D. and 4.B.1.c.E).

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

Cost sharing – Describe the source, nature and amount of cost-sharing, if any. Reference section 4.B.1.c.J.

Other Pricing Assumptions - Identify pricing assumptions which may require incorporation into the resulting award instrument (e.g., use of Government Furnished Property/ Facilities/Information, access to Government Subject Matter Experts, etc.). Reference section 4.B.1.c.J.

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

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

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

- Accounting system
- Purchasing system

Certified "cost or pricing data" may be requested after selection for procurement contract awards of $750,000 or greater, unless the Contracting Officer approves an exception from the requirement to submit cost or pricing data. (Reference FAR Part 15.403.)

4.C. Submission Details

4.C.1. Due Dates

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

4.C.2. Proposal Delivery

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

After registration has been approved, offeror's should upload proposals (Volume 1 and Volume 2), scanned certifications and permitted additional information in 'pdf' format or as otherwise directed (Excel, PowerPoint, etc). Offerors are responsible for ensuring compliant and final submission of their proposals to meet the BAA submittal deadlines. Time management to upload and submit is wholly the responsibility of the offeror.

Upon completing the proposal submission the offeror shall receive an automated confirmation email from IDEAS. Please forward that automated message to dni-iarpa-BAA-16-12@iarpa.gov**.** IARPA strongly suggests that the offeror document the submission of their proposal package by printing the electronic receipt (time and date stamped) that appears on the final screen following compliant submission of a proposal to the IDEAS website.

Proposals submitted by any means other than IDEAS (e.g., hand-carried, postal service, commercial carrier and email) shall not be considered unless the offeror attempted electronic submission but was unsuccessful. Should an offeror be unable to complete the electronic submission, the offeror shall employ the following procedure. The offeror shall send an e-mail to dni-iarpa-BAA-16-12@iarpa.gov, prior to the first round proposal due date and time specified in the BAA, and indicate that an attempt was made to submit electronically but that the submission was unsuccessful. This e-mail shall include contact information for the offeror. Following this email contact, additional guidance shall be provided.

Proposals shall be submitted by the time and date specified in the BAA in order to be assured of consideration during the first round of selections. IARPA may evaluate proposals received after this date until the closing date of the BAA. Selection remains contingent on proposal evaluation, program balance and availability of funds. Failure to comply with the submission procedures may result in the submission not being evaluated.

4.D. Funding Restrictions

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

SECTION 5: PROPOSAL REVIEW INFORMATION

5.A. Technical and Programmatic Evaluation Criteria

The criteria to be used to evaluate and select proposals for this Program BAA are described in the following paragraphs. Because there is no common statement of work, each proposal shall be evaluated on its own merits and its relevance to the Program goals rather than against other proposals responding to this BAA. The proposals shall be evaluated on the basis of the evaluation criteria listed in this section 5.A, program balance, and availability of funds. The evaluation criteria of this section 5.A, in descending order of importance, are: Overall Scientific and Technical Merit, Effectiveness of Proposed Work Plan, Contribution and Relevance to the IARPA Mission and Program Goal, Relevant Expertise and Experience, and Resource Realism. Specifics about the evaluation criteria are provided below, in descending order of importance.

Award(s) shall be made to offerors on the basis of the evaluation criteria listed below in paragraphs 5.A.1 through 5.A.5, program balance, and availability of funds and subject to successful negotiations with the Government. Award recommendations shall not be made to offeror(s) whose proposal(s) are determined not to be selectable. Offerors are cautioned that evaluation ratings may be lowered or proposals rejected if submission instructions are not followed.

5.A.1. Overall Scientific and Technical Merit

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

5.A.2. Effectiveness of Proposed Work Plan

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

The roles and relationships of prime and sub-contractors is clearly delineated with all participants fully documented. Work plans shall demonstrate the ability to provide full Government visibility into and interaction with key technical activities and personnel, and a single point of responsibility for contract performance. Work plans shall also demonstrate that key personnel have sufficient time committed to the Program to accomplish their described Program roles.

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

The offeror's proposed intellectual property and data rights are consistent with the Government's need to be able to effectively manage the program and evaluate the technical output and deliverables, communicate program information across Government organizations and support transition and further use and development of the program results to Intelligence Community users at an acceptable cost. The proposed approach to intellectual property rights is in the Government's best interest.

5.A.3. Contribution and Relevance to the IARPA Mission and Program Goal

The proposed solution meets the letter and intent of the stated program goals and all elements within the proposal exhibit a comprehensive understanding of the problem. The offeror clearly addresses how the proposed effort shall meet and progressively demonstrate the Program goals. The offeror describes how the proposed solution contributes to IARPA's mission to invest in

high-risk/high-payoff research that can provide the U.S. with an overwhelming intelligence advantage over its future adversaries.

5.A.4. Relevant Experience and Expertise

The offeror's capabilities, related experience, facilities, techniques, or unique combination of these, which are integral factors for achieving the proposal's objectives, shall be evaluated, as well as qualifications, capabilities, and experience of the proposed principal investigator, team leader, and key personnel critical in achieving the proposal objectives. Time commitments of key personnel shall be sufficient for their proposed responsibilities in the effort.

5.A.5. Resource Realism

The proposed resources are well justified and consistent with the unique technical approach and methods of performance described in the offeror's proposal. Proposed resources reflect a clear understanding of the project, a perception of the risks and the ability to organize and perform the work. The labor hours and mix are consistent with the technical and management proposal and are realistic for the work proposed. Material, equipment, software, data collection and travel, especially foreign travel, are well justified, reasonable, and required for successful execution of the proposed work.

5.B. Method of Evaluation and Selection Process

IARPA's policy is to ensure impartial, equitable, comprehensive proposal evaluations and to select the source (or sources) whose offer meets the Government's technical, policy and programmatic goals. Evaluations will be conducted using a combination of an adjectival and numerical rating methodology. In order to provide the desired evaluation, qualified Government personnel shall conduct reviews and (if necessary) convene panels of experts in the appropriate areas.

IARPA shall only review proposals against the evaluation criteria described under section 5.A above, program balance, and availability of funds, and shall not evaluate them against other proposals, since they are not submitted in accordance with a common work statement. For evaluation purposes, a proposal is the document described in Sections 4.A and 4.B. Other supporting or background materials submitted with the proposal shall not be considered. Only Government personnel shall make evaluation and award determinations under this BAA. Selections for award shall be made on the basis of the evaluation criteria listed in paragraphs 5.A.1 through 5.A.5, program balance and the availability of funds. Selections for award shall not be made to offeror(s) whose proposal(s) are determined to be not selectable.

5.C. Negotiation and Contract Award

Award of a contract is contingent on successful negotiations. After selection and before award, the contracting officer shall determine cost/price realism and reasonableness, to the extent appropriate, and negotiate the terms of the contract.

The contracting officer shall review anticipated costs, including those of associate, participating organizations, to ensure the offeror has fully analyzed the budget requirements, provided sufficient supporting cost/price information, and that cost data are traceable and reconcilable. Additional information and supporting data may be requested.

If the parties cannot reach mutually agreeable terms, a contract shall not be awarded.

5.D. Proposal Retention

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

SECTION 6: AWARD ADMINISTRATION INFORMATION

6.A. Award Notices

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

6.B. Administrative and National Policy Requirements

6.B.1. Proprietary Data

It is the policy of IARPA to treat all proposals as competitive information, and to disclose their contents only for the purpose of evaluation. All proposals containing proprietary data should have the cover page and each page containing proprietary data clearly marked as containing proprietary data. It is the offeror's responsibility to clearly define to the Government what the offeror considers proprietary data.

6.B.2. Intellectual Property

6.B.2.a. Noncommercial Items (Technical Data and Computer Software)

Offerors responding to this BAA requesting a procurement contract shall identify in Volume 1, Attachment 2 of the proposal all noncommercial technical data and noncommercial computer software that it plans to generate, develop and/or deliver under any proposed award instrument in which the Government shall acquire less than unlimited rights and to assert specific restrictions on those deliverables, the basis for such restrictions, the potential cost to the Government to acquire GPR in all deliverables incorporating such noncommercial technical data and computer software, and the intended use of the technical data and noncommercial computer software in the conduct of the proposed research and development of applicable deliverables. If offerors intend to incorporate noncommercial, proprietary technical data or computer software into any deliverable,

offerors should provide in Volume 1, Attachment 2 of their proposals all of the information regarding such proprietary technical data or computer software as described in sections 4.B.1.c.D and 4.B.1.c.E of this BAA.

In the event that offerors do not submit such information, the Government shall assume that it automatically has unlimited rights to all noncommercial technical data and noncommercial computer software generated, developed, and/or delivered under any award instrument, unless it is substantiated that development of the noncommercial technical data and noncommercial computer software occurred with mixed funding. If mixed funding is anticipated in the development of noncommercial technical data and noncommercial computer software generated, developed and/or delivered under any award instrument, then offerors should identify the data and software in question and that the Government shall receive GPR in such data and software. The Government shall automatically assume that any such GPR restriction is limited to a period of five years, at which time the Government shall acquire unlimited rights unless the parties agree otherwise. A sample format for complying with this request is shown in APPENDIX G. If no restrictions are intended, then the offeror should state "NONE."

Offerors are advised that the Government shall use this information during the source selection evaluation process to evaluate the impact of any identified restrictions and may request additional information from the offeror, as may be necessary, to evaluate the offeror's assertions.

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

The Government reserves the right to reject a proposal if it does not appropriately address all data issues.

6.B.2.b. Commercial Items (Technical Data and Computer Software)

Offerors shall identify in Section 4 (Attachment 2, template provided as APPENDIX G) of its proposal all commercial technical data and commercial computer software that may be incorporated in any noncommercial deliverables contemplated under the research effort, along with any applicable restrictions on the Government's use of such commercial technical data and/or commercial computer software. In the event that offerors do not submit the list, the Government shall assume that there are no restrictions on the Government's use of such commercial items. The Government may use the list during the source selection evaluation process to evaluate the impact of any identified restrictions and may request additional information from the offeror, as may be necessary, to evaluate the offeror's assertions. A sample

format for complying with this request is shown in APPENDIX G. If no restrictions are intended, then the offeror should state "NONE."

6.B.2.c. All Offerors – Patents

Include documentation using the format provided in APPENDIX G, proving ownership of or possession of appropriate licensing rights to all patented inventions (or inventions for which a patent application has been filed) that shall be utilized under the proposal for the IARPA program. If a patent application has been filed for an invention that the proposal utilizes, but the application has not yet been made publicly available and contains proprietary information, the offeror may provide only the patent number, inventor name(s), assignee names (if any), filing date, filing date of any related provisional application, and a summary of the patent title, together with either: (1) a representation that the offeror owns the invention, or (2) proof of possession of appropriate licensing rights in the invention.

If offerors intend to incorporate patented technology into any deliverable, i.e., if offerors intend for any deliverable to embody any invention covered by any patent or patent application the offerors list in APPENDIX G, offerors should also provide in Volume 1, Attachment 2 of their proposals all of the information described in section 4.B.1.c.E of this BAA.

6.B.2.d. All Offerors – Intellectual Property Representations

The offeror shall provide a good faith representation that they either own or possess appropriate licensing rights to all other intellectual property that shall be utilized under their proposal for the program.

6.B.3 Human Use

No research proposals involving human subjects shall be accepted under this BAA.

6.B.4. Animal Use

No research proposals involving animal subjects shall be accepted under this BAA.

6.B.5. Publication Approval

It is anticipated that research funded under this Program shall be unclassified research that shall not require a pre-publication review. However, performers should note that pre-publication approval of certain information may be required if it is determined that its release may result in the disclosure of sensitive intelligence information. A courtesy soft copy of any work submitted for publication shall be provided to the IARPA Program Manager and the Contracting Officer Representative (COR) a minimum of 5 days prior to release in any forum.

6.B.6. Export Control

(1) The offeror shall comply with all U.S. export control laws and regulations, including the International Traffic in Arms Regulations (ITAR), 22 C.F.R. Parts 120 through 130, and the Export Administration Regulations (EAR), 15 C.F.R. Parts 730 through 799, in the performance of this contract. In the absence of available license exemptions/exceptions, the offeror shall be responsible for obtaining the appropriate licenses or other approvals, if required, for exports of (including deemed exports) hardware, technical data, and software, or for the provision of technical assistance.

(2) The offeror shall be responsible for obtaining export licenses, if required, before utilizing non-U.S. persons (as defined in the ITAR and EAR, as applicable) in the performance of this contract, including instances where the work is to be performed on-site at any Government installation (whether in or outside the United States), where the foreign person shall have access to export-controlled technologies, including technical data or software.

(3) The offeror shall be responsible for all regulatory record keeping requirements associated with the use of licenses and license exemptions/exceptions.

(4) The offeror shall appropriately mark all contract deliverables controlled by ITAR and/or EAR.

(5) The offeror shall be responsible for ensuring that the provisions of this section apply to its sub-contractors**.**

(6) The offeror may be required to certify knowledge of and intended adherence to these requirements in the representations and certifications of the contract.

6.B.7. Subcontracting

It is the policy of the Government to enable small business and small disadvantaged business concerns to be considered fairly as sub-contractors to contractors performing work or rendering services as prime contractors or sub-contractors under Government contracts and to assure that prime contractors and sub-contractors carry out this policy. Each offeror that is selected for negotiation for award and is expected to be awarded a contract which exceeds the simplified acquisition threshold may be asked to submit a sub-contracting plan before award in accordance with FAR 19.702(a) (1). The plan format is outlined in FAR 19.704.

Offerors shall declare teaming relationships in their proposals and shall specify the type of teaming arrangement in place, including any exclusive teaming arrangements. IARPA neither promotes nor discourages the establishment of exclusive teaming agreements within offeror teams. Individuals or organizations associated with multiple teams shall take care not to over-commit those resources being applied.

6.B.8. Reporting

Fiscal and management responsibility are important to the Program. Although the number and types of reports shall be specified in the award document, all performers shall, at a minimum, provide the Contracting Office, Contracting Officer Representative and the Program Manager

with monthly technical reports and monthly financial reports. The reports shall be prepared and submitted in accordance with the procedures contained in the award document and mutually agreed upon before award. Technical reports shall describe technical highlights and accomplishments, priorities and plans, issues and concerns, evaluation results, and future plans. Financial reports shall present an on-going financial profile of the project, including total project funding, funds invoiced, funds received, funds expended during the preceding month, and planned expenditures over the remaining period. Additional reports and briefing material may also be required, as appropriate, to document progress in accomplishing program metrics.

The performer shall prepare and provide a research report of their work annually by month 12. The reports shall be delivered to the Contracting Officer, Contracting Officer Representative and the Program Manager. The reports shall include:

- Problem definition
- Findings and approach
- System design
- Possible generalization(s)
- Information on performance limitations and potential mitigation
- Anticipated path ahead
- Final identification of all commercial, third-party, or proprietary hardware, software, or technical data integrated into any deliverable and all applicable use restrictions.

6.B.9. System for Award Management (SAM)

Selected offerors not already registered in the Systems for Award Management (SAM) may be required to register in SAM prior to any award under this BAA. Information on SAM registration is available at http://www.sam.gov**.**

6.B.10. Representations and Certifications

Selected offerors may be required to complete electronic representations and certifications at http://www.sam.gov and may also be required to complete additional representations and certifications prior to award.

6.B.11. Lawful Use and Privacy Protection Measures

All data gathered by the performer shall be obtained in accordance with U.S. laws and in compliance with the End User License Agreement, Copyright Laws, Terms of Service, and laws and policies regarding privacy protection of U.S. Persons. Before using such data, the performer shall provide proof that the data was acquired in accordance with U.S. laws and regulations.

6.B.12. Public Access To Results

IARPA is committed to making the results of this research available and maximally useful to the public, industry, government, and the scientific community, in accordance with the policy set forth in the White House Office of Science and Technology Policy's memorandum "Increasing

Access to the Results of Federally Funded Scientific Research," dated February 22, 2013[4], consistent with all other applicable law and policy; agency mission; resource constraints; and U.S. national, homeland, and economic security.

Awardees shall be required to submit to IARPA the final version of peer-reviewed publication manuscripts related to research funded under awards made under this BAA. Awardees shall be required to authorize IARPA to release these manuscripts to the public no later than twelve (12) months after the manuscript's official publication date in a journal or other publication. In addition, IARPA intends to make unclassified data sets, samples, and other supporting materials developed or delivered under awards available to the public, unless IARPA stipulates otherwise or to the extent that such public release would compromise the ability to file for intellectual property protection on any invention arising from the data.

Insofar as possible, all data produced for VirtUE, reports to IARPA, and all VirtUE -based publications shall follow the suggestions of the Center for Open Science. Insofar as possible, all VirtUE publications should qualify for Open Science's[5] Open Data and Open Materials badges.

To the extent possible, all awardee reports to IARPA and all VirtUE -based publications should be consistent with the statistical and methodological requirements for publication found in the 2014 Psychological Science editorial "Not Business as Usual"[6]. For example, wherever appropriate, effect sizes and confidence intervals (or the Bayesian equivalents) should be reported, and the data and methodology shall be presented so that it is easily used for meta-analysis and independent re-analysis of the data. All offerors are encouraged to include statisticians and methodologists who are expert in these areas. All offerors shall describe the plans to ensure that the above requirements are satisfied.

6.B.13. Cloud Compatibility

Software deliverables shall be deployable to the Government-specified test rig which shall be comparable to Amazon Web Services (AWS) infrastructure.

[4] https://www.whitehouse.gov/sites/default/files/microsites/ostp/ostp_public_access_memo_2013.pdf
[5] Open Science (2013). Badges to acknowledge open practices. https://openscienceframework.org/project/TVyXZ/
[6] Psychological Science (2014) http://pss.sagepub.com/content/25/1/3

APPENDIX A

Academic Institution Acknowledgement Letter Template

IARPA Broad Agency Announcement

Virtuous User Environment (VirtUE)

(IARPA-BAA-16-12)

-- Please Place on Official Letterhead --

<Insert date>

To: Contracting Officer
ODNI/IARPA
Office of the Director of National Intelligence
Washington, D.C. 20511

Subject: Academic Institution Acknowledgement Letter

Reference: Executive Order 12333, As Amended, Para 2.7

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

The undersigned further acknowledges that he/she is aware of the Intelligence Advanced Research Projects Activity's proposed contractual relationship with <insert name of institution> through IARPA-BAA-16-XX and is hereby approved by the undersigned official, serving as the president, vice-president, chancellor, vice-chancellor, or provost of the institution.

_____

<Name> Date
<Position>

APPENDIX B

SAMPLE COVER SHEET

For

VOLUME 1: Technical/Management Details

BROAD AGENCY ANNOUNCEMENT (BAA)

Virtuous User Environment (VirtUE)

(IARPA-BAA-16-12)

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

APPENDIX C

SAMPLE COVER SHEET

For

VOLUME 2: Cost Proposal

BROAD AGENCY ANNOUNCEMENT (BAA)

Virtuous User Environment (VirtUE)

(IARPA-BAA-16-12)

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

APPENDIX D

Letter Template

For

Organizational Conflicts of Interest Certification Letter Template

IARPA Broad Agency Announcement (BAA)

Virtuous User Environment (VirtUE)

(IARPA-BAA-16-12)

(Month DD, YYYY)

Office of the Director of National Intelligence
Intelligence Advanced Research Projects Activity (IARPA)
Virtuous User Environment (VirtUE)
ATTN: Kerry Long
Washington, DC 20511

Subject: OCI Certification

Reference: VirtUE, IARPA-BAA-16-12

Dear Mr. Long,

In accordance with IARPA Broad Agency Announcement IARPA-BAA-16-12, Section 3.A.1, *Procurement Integrity, Standards of Conduct, Ethical Considerations, and Organizational Conflicts of Interest (OCI)*, and on behalf of (offeror name) I certify that neither (offeror name) nor any of our subcontractor teammates has as a potential conflict of interest, real or perceived, as it pertains to the VirtUE program.

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

Sincerely,

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

(Insert signature)

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

APPENDIX E

Sample Prime Contractor Cost Element Sheet

For

VOLUME 2: Cost Proposal

IARPA Broad Agency Announcement (BAA)

Virtuous User Environment (VirtUE)

(IARPA-BAA-16-12)

PRIME CONTRACTOR COST ELEMENT SHEET [SAMPLE]			
Complete a Cost Element Sheet for the Base Period and <u>each</u> Option Period			
COST ELEMENT	**BASE**	**RATE**	**AMT**
DIRECT LABOR (List each labor category separately. Identify Key Personnel by name.)	# of Hours	$	$
TOTAL DIRECT LABOR			$
FRINGE BENEFITS	$	%	$
TOTAL LABOR OVERHEAD	$	%	$
SUBCONTRACTORS, IOTS, CONSULTANTS (List separately. See below table.)			$
MATERIALS & EQUIPMENT (List each material and equipment item separately.)	Quantity	$ unit price	$
SOFTWARE & INTELLECTUAL Property (List separately. See table below.)	$	$	$
TOTAL MATERIALS & EQUIPMENT			$
MATERIAL OVERHEAD	$	%	$
TRAVEL (List each trip separately.)	# of travelers	$ price per traveler	$
TOTAL TRAVEL			$
OTHER DIRECT COSTS (List each item separately.)	Quantity	$ unit price	$
TOTAL ODCs			$
G&A	$	%	$
SUBTOTAL COSTS			$
COST OF MONEY	$	%	$
TOTAL COST			$
PROFIT/FEE	$	%	$
TOTAL PRICE/COST			$
GOVERNMENT SHARE, IF APPLICABLE			$
RECIPIENT SHARE, IF APPLICABLE			$

SUBCONTRACTORS/INTERORGANIZATIONAL TRANSFERS (IOT) & CONSULTANTS PRICE SUMMARY

A	B	C	D	E	F
SUB-CONTRAC-TOR IOT & CONSULTANT NAME	**SOW TASKS PERFORMED ***	**TYPE OF AWARD**	**SUB-CONTRAC-TOR, IOT & CONSULTANT QUOTED PRICE**	**COST PROPOSED BY PRIME FOR THE SUBCONTRAC-TOR, IOT & CONSULTANT**	**DIFFERENCE (Column D - Column E) IF APPLICABLE**

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

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

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

APPENDIX F

Sample Subcontractor Cost Element Sheet

For

VOLUME 2: Cost Proposal

IARPA Broad Agency Announcement (BAA)

Virtuous User Environment (VirtUE)

(IARPA-BAA-16-12)

SUBCONTRACTOR COST ELEMENT SHEET [SAMPLE]			
Complete a Cost Element Sheet for each applicable period			
COST ELEMENT	**BASE**	**BURDENED RATE**	**AMT**
DIRECT LABOR (List each labor category separately. Identify Key Personnel by name.)	# hrs	$	$
TOTAL DIRECT LABOR			$
SUBCONTRACTORS, IOTS, CONSULTANTS			$
MATERIALS & EQUIPMENT (List each material and equipment item separately.)	qty	$ unit price	$
TOTAL MATERIALS & EQUIPMENT			$
TRAVEL (list each trip separately)	# of travelers	$ price per traveler	$
TOTAL TRAVEL			$
OTHER DIRECT COSTS (List each item separately.)	qty	$ unit price	$
TOTAL OTHER DIRECT COSTS			$
TOTAL PRICE/COST			$

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

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

APPENDIX G

Restrictions on Intellectual Property Rights

For

VOLUME 1: Technical and Management Proposal

IARPA Broad Agency Announcement (BAA)

Virtuous User Environment (VirtUE)

(IARPA-BAA-16-12)

Noncommercial Items (Technical Data and Computer Software)

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

Description of restrictions on Government's ability to use, modify, reproduce, release, perform, display, or disclose technical data, computer software, and deliverables incorporating technical data and computer software listed above:

Potential cost to the Government to acquire GPR in all deliverables incorporating the technical data and computer software listed above:

Intended use of the technical data and computer software listed above in the conduct of the proposed research:

Commercial Items (Technical Data and Computer Software)

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

Patents

PATENTS			
Patent number (or application number)	**Patent name**	**Inventor name(s)**	**Patent owner(s)**
(LIST)	(LIST)	(LIST)	(LIST)

APPENDIX H

Templates for Three Chart Summary of the Proposal

For

VOLUME 1: Technical and Management Proposal; Section 2

IARPA Broad Agency Announcement (BAA)

Virtuous User Environment (VirtUE)

(IARPA-BAA-16-12)

Chart 1: Overview

- Self-contained, intuitive description of the technical approach and performance
  - Avoid acronyms! Especially those that are contractor specific.

Chart 2: Key Innovations

- Innovation 1
- Innovation 2
- Innovation 3

Graphics / Data

Chart 3: Expected Impact

- Deliverable 1; Performance and Impact
- Deliverable 2; Performance and Impact
- Unique aspects of the proposal