Questions & Answers – VirtUE IARPA-BAA-16-12

Responses to Questions # 1 to 19

Q1: Is building a secure Virtue-based application development platform the primary goal of this BAA?

A1: No. The primary purpose is to build a Virtue—a new user computer environment that will replace the current conception of the workstation or desktop—and the infrastructure for admins to create and distribute this environment in the cloud. If we define applications as we did in the BAA, the applications are no different than what are running in a user desktop, except that now they are in an environment that protects and monitors them better and of course there aren't nearly so many of them installed in any given instance of a Virtue. Applications as they are defined in this BAA really should not require additional development. What will require development and creativity is the new operating environment and the development infrastructure that can create these environments.

Q2: What is the relative importance of supporting legacy applications vs. supporting the new development of secure Virtue-based applications?

A2: There should be minimal development of special secure Virtue-based applications in general. It is permissible for performers to create new applications for security or logging purposes or some other Virtue management function, but in general most applications that run in Virtues will be legacy.

Q3: What type of applications are envisioned to be created as Virtue-based applications?

A3: There will be multiple roles a Virtue will have to support—each running different applications, resources, protections and logging. The underlying Virtue technologies will be the same, just the configuration will change. Performers will be required to build Virtues to demonstrate that they can support several different roles, but ultimately their design's extensibility to support roles no one has thought of yet will be paramount.

Q3a: Simple (single developer, single user, and single node): A small web browser application is alluded to should this be the type of application expected?

A3a: Whatever an average user can run in his standard Windows and/or Linux desktop is in scope. A small web browser might be expected to be one of the applications present in a theoretical web browsing Virtue role, but an admin might also include an Adobe Reader and a Microsoft PowerPoint viewer when building this role's Virtue.

Q3b: Complex (multi-developer. multi-user, multi-node): Would supporting the development of a large highly distributed multi-user application be in scope?

A3b: Yes, but the intent is to initially support the types of workloads that the average IC user performs on their desktops. Except, instead of having one desktop to run all these applications in, the user will have several Virtues.

Q4: Is it expected that performers build some sample secure Virtue-based applications?

A4: No, if applications are defined in the traditional sense (e.g., MS Word). However, if referring to the application of a Virtue to address a role, then yes. The BAA requires performers to demonstrate creation of Virtues serving different user roles and all the code and infrastructure to enable admins to create, provision and distribute these Virtues.

Q4a: If so, will there be certain ones expected or is up to the performer?

A4a: Performers will be given some roles to demonstrate and can add others at their discretion.

Q5a: The BAA States: "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." How does this effect use of other open source technologies with different licenses as part of the solution?

A5a: The intent of this project is to publish as much of the effort to the world as possible. GPL 3.0 is the licensing scheme proposed for original work that performers do on behalf of Virtue. Different open source licensing options for a performer's Virtue solution might be permissible if it makes more sense based on the inclusion of other open source works.

Q5b: What about use of other GOTS technologies with different licenses as part of the solution?

A5b: The use of GOTS technologies as part of the Virtue solution might be acceptable if assurances can be provided that its sharing with the open source community is permissible.

Q5c: What if modifications / extensions are required to the open source and/or GOTS technology being used as part of VirtUE. Can the modifications be done under the original license?

Performers should comply with the applicable open source license in making modifications or extensions to any open source software during performance. The Government strongly prefers that offerors use open source software whose licenses permit users to make modifications and extensions to the code and make these modifications and extensions available as open source software to the community. Note that technology developed during this program which cannot be shared with the open source community is out of the scope of the program as stated in BAA section 1.A.7.

Q6: Does the required "legacy" support for Windows imply that Windows-based Virtues will be subjected to all of the prescribed metrics? If not, which ones?

A6: Depending on how you define and build a Virtue, there may be only one Virtue type that runs both Linux and Windows applications. But assuming your Virtue solution had two or more variants, one of which supported Windows applications and was called a Windows-based Virtue, then yes it would be subject to the same metrics.

Q7: Requirement (2a) requires <= 200 system calls. Does this take into consideration "extensible" system call interfaces, e.g. netlink, ioctls, or proc interfaces?

A7: The intent of this requirement is to try and reduce the complexity of the user and external exposed portions of an operating environment compared to what is normally expected in the traditional desktop user environment of a Linux or Windows workstation. One measure of this

complexity is the number of system calls that are possible between the user space and the kernel space. This assumes that the proposer's Virtue solution provides a processing environment where user level code and or external sourced code requires interaction with a kernel like layer. Assuming this, netlink handlers and ioctls that are used or could be used should be considered for this metric. 200 is a target for performers, not a hard requirement. The intent is to see how few system calls a performer can expose while still enabling functionality.

Q8: Requirement (2d) requires <= 3 communication paths. Is IP networking "one path"?

A8: IP Networking for one interface between the Virtue boundary and the external world with its associated protections and logging would be considered one path. Using your example, one could imagine one external IP Networking path for the thin client to interact with the Virtue delivering audio, video, input; another IP Networking path to enable the Virtue to interact with the Control Plane; and perhaps a third IP networking path to interact with other Virtues. This is only one possible example of course, but a reasonable one.

Q9a: Requirement 8 suggests that virtues are required to securely save, pass, and retrieve basic state information and calls out "individual files". Does this file transfer need to be for seamless operations? E.g. Opening a Word docx downloaded from Browser Role / Virtue should open a document editor virtue?

A9a: No. It is up to the performer to balance the need for security with the need for usability. This would be a very user friendly feature for a Virtue to provide. You would have to be creative to ensure its security from both insider and external threats that might be aware of this capability.

Q9b: Or is transfer via home directory / network storage sufficient (although more manual)?

A9b: See A9a.

Q9c: What about other types of hyperlinks?

A9c: See A9a.

Q10: Is smart card authentication required for phase 1 or is Password authentication sufficient?

A10: Either is permissible.

Q11: Requirement 5 states "A log repository accessible by SFTP will be provided by the T&E team for performers to deposit all logs." Is SFTP logging supposed to be live? Or some snapshot of logs upload to T&E? As in, do we need to support logging via SFTP?

A11: Yes. Performers will deliver the output of their Virtue sensing to a repository as actions are occurring or "live" just like they would deliver it to the Control Plane in phase 2. The T&E team will make their repository accessible via SFTP and Syslog. They may also accommodate requests for other transfer methods to the repository if this does not require much additional effort on their part.

Q12: The presentation slides stated "VirtUE must support windows authentication tokens without incurring vulnerabilities of traditional Windows workstations". What tokens are being referred to here? Access tokens? Smart cards?

A12: Access tokens are being referred to.

Q13: Should we assume the windows application running in the context of Active Directory domains for Phase 1?

A13: Yes

Q14: What is the expected TRL of the Phase I system?

A14: The expected TRL of the Phase 1 system is TRL 5.

Q15: [Section 4.B.2.b F.] requires a table of all labor categories and their associated direct labor rates. Should this table be inclusive of Prime and Subcontactor labor categories? If so, is it acceptable for the rates of the subcontractors to be fully burdened as they may consider their direct labor rates to be proprietary?

A15: The Prime must include subcontractor total costs at a summary level under the Appendix E template, and use Appendix F to provide a breakdown of individual subcontractor cost elements to include labor categories at fully burdened or loaded rates. If selected for negotiations, the government will contact subcontractors directly regarding their proprietary rate information.

Q17: [Section 4.B.2.c Direct Labor] requires listing of all key personnel by name, category and rate. If any of the offeror's subcontractor personnel are considered key should they be listed in this section or in the Subcontracts section?

A16: Subcontractor personnel considered to be key personnel should be identified in the subcontractor section, and **all** key personnel should be listed in a Key Personnel Table per section 4.B.1.c.I of the BAA. See also Appendix F (Subcontractor Cost Element Sheet).

Q18: Regarding Section 4.B Proposal Format and Content, Offeror requests foldout pages or larger than 8 ½ x 11 be allowed for the cost excel files as the excel file may be large.

A18: Cost excel files may be larger than 8 ½ x 11.

Q19: Regarding Section 4.B Proposal Format and Content, Is the font requirement for the cost excel files 10 pt or 12 pt?

A19: The font size for figure, tables, and charts shall not be smaller than 10 pt. That includes excel spreadsheets.