

AOS Report No. AOS-17-0609

September 2017

Virtue Test and evaluation Handbook

Version 1.1

Prepared for: Intelligence Advanced Research Projects Activity (IARPA)

Prepared by: VirtUE Team

|  |  |
| --- | --- |
| Task No.: | VJY26 |
| Contract No.: | 2017-16110100002S |
| **Distribution Statement** **X:** | |
| **Export Control Notice**: If applicable. | |
| **Destruction Notice**: For unclassified, limited distribution information, destroy by any method that will prevent disclosure of contents or reconstruction of the document. | |

**CONTENTS**

Page

1. Introduction 1

1.1 Program Background 1

1.2 Purpose 2

1.3 References 2

2. Roles and responsibilities 2

2.1 VirtUE Test & Evaluation Team 2

2.2 VirtUE Performer Team(s) 2

3. Communication Plan 3

3.1 Technical Status Meetings 3

3.2 Email Communications 3

3.3 Site Visit 4

3.4 Pre-Test Coordination 4

4. Dry Run Test Exercise 4

5. System Delivery 4

5.1 Documentation 4

5.1.1 System Architecture and Design 5

5.1.2 System Interface Details 5

5.1.3 Deployment Information 5

5.1.4 User Information 5

5.1.5 Administrator Information 5

5.1.6 Test Readiness Plan 6

5.2 Virtue Deployment Package 6

6. Test Event 6

6.1 Test Schedule 6

7. Rules of engagement 8

7.1 Assumptions and Limitations 8

7.2 Test and Evaluation 8

8. JHU/APL Visitor control 10

8.1 Non-U.S. Citizens 10

8.2 Network Access 10

9. Summary 11

Table 1: Referenced Documents 2

# Introduction

JHU/APL is providing support to the Virtuous User Environment (VirtUE) program sponsored by the Intelligence Advanced Research Projects Activity (IARPA).  JHU/APL’s main efforts are focused along three technical areas: systems engineering, software engineering, and testing and evaluation (T&E). As part of JHU/APL’s T&E support, JHU/APL is responsible for developing a testbed to support test and evaluation of performer solutions.

In months 9 and 18, performers shall travel to the Government-selected T&E facilities at JHU/APL in Laurel, MD to undergo a midterm and end-of-phase assessment of their solution’s performance. For planning purposes, proposers should allow three days for interactive testing and test readiness review at JHU/APL for each assessment. Performers will be expected to deliver all software and documentation required for JHU/APL to adequately assess their offering to T&E team members prior to assessments. T&E team members will be responsible for instrumenting and creating a testing environment within Amazon Web Services (AWS) to assess offerors’ solutions against the requirements of the program[[1]](#footnote-1).

## Program Background

VirtUE seeks to leverage the federal government’s migration to commercial cloud-based Information Technology (IT) infrastructure and the current explosion of new virtualization and operating system (OS) concepts to create and demonstrate a more secure interactive user compute environment (UCE) than is currently available for government use or is expected to be available in the near future1.

* In Phase 1, the program 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.
* 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.

In support of Phase 1 of the VirtUE program, JHU/APL is serving as the T&E partner for IARPA, responsible for conducting rigorous testing of solutions developed by Phase 1 performers. JHU/APL will conduct tests at the midpoint of Phase 1 of the program (month 9) and at the completion of Phase 1 of the program (month 18). Information presented in this document is specific to Phase 1 of the VirtUE program.

## Purpose

This document serves as a T&E Handbook for performers providing guidance on performer interactions with the T&E team, expectations concerning system delivery, expectations of pre-test events and test events, T&E rules of engagement, and requirements and procedures for visiting the APL campus.

## References

Documents referenced in the process of developing the Virtue Test and Evaluation Handbook are listed in Table 1.

|  |  |
| --- | --- |
| Document | URL |
| FedRamp Security Assessment Plan (Template) Version 1.0 | https://www.gsa.gov/graphics/staffoffices/SAP\_Template\_051712\_508.doc |
| NIST Technical Guide to Information Security Testing and Assessment SP 800-115 2008 | http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf |

Table : Referenced Documents

# Roles and responsibilities

## VirtUE Test & Evaluation Team

The VirtUE T&E Team (VTE) consists of staff from JHU/APL supporting the VirtUE program with all T&E activities. The VTE serves as independent evaluators of VirtUE performer solutions and is responsible for developing the T&E methodology, constructing the VirtUE testbed, hosting performers during test readiness review, and executing all tests against VirtUE performer solutions.

## VirtUE Performer Team(s)

VirtUE performers consist of organizational teams selected by the VirtUE program to develop fully functioning solutions that satisfy VirtUE program requirements. Performer teams are responsible for design, implementation, integration, and preliminary testing of their respective solutions. In support of VirtUE T&E activities, each performer is expected to provide documentation including system architectures, software designs, interface specifications, and deployment guides. Performers are also expected to provide a deployable package consisting of their Virtue environment and/or any dependent executables and configuration utilities required to deploy and operate their system in AWS. In addition, performers are expected to deliver all source code developed in support of the program to the T&E team. In order to mitigate potential complications with performer solution integration with the T&E testbed, performers are encouraged to follow T&E guidance on supporting specific interfaces to the T&E environment as described in section 7.

# Communication Plan

Establishing frequent and open communications between VirtUE performers and the T&E team is critical in order to facilitate the exchange of technical knowledge pertaining to performers’ solutions. This should include the solution’s configuration, deployment, operation, and integration with the T&E testbed. Interactions between performer teams and the T&E team will provide opportunities for the discussion of unique Virtue capabilities and configurations, T&E integration points, known limitations, and potential issues that may present challenges when conducting T&E.

Open dialogue and free exchange of information will assist in preparing all parties for successful T&E events. The following sections introduce the VirtUE T&E Communications Strategy, consisting of technical status meetings, email communications, site visits, and pre-test event coordination.

## Technical Status Meetings

Technical status meetings will be held every other week with each performer and the JHU/APL T&E team. The purpose of the technical status meeting is for performers to provide updates on development efforts that include discussions on recent progress, architecture and design considerations, deployment considerations, and testing strategy. Virtue interfaces, in particular T&E integration points, will be an area of special interest to cover during status meetings. The biweekly status meeting will allow the T&E team to develop a deep understanding of a performer’s solution to ensure alignment with T&E infrastructure and overall testing strategy. JHU/APL will also present discussions covering the testbed infrastructure including configuration and operation of testbed assets, metrics to be evaluated during testing, and the T&E scoring methodology. JHU/APL will be responsible for setting up the conference bridge. The duration of the biweekly meeting is expected to be one hour.

## Email Communications

The JHU/APL T&E team can be contacted at any time via the team’s email alias – [virtue@jhuapl.edu](mailto:virtue@jhuapl.edu). JHU/APL may provide answers to questions and comments submitted by performers to all performer teams if all performers would benefit from the information. If a question or comment submitted by a performer team is sensitive in nature, i.e. the question or comment reveals technical information pertinent to a performer’s solution that the performer prefers not to be disclosed to others, the subject of the email should contain [PERFORMER SENSITIVE].

## Site Visit

The JHU/APL T&E team will participate in a performer site visit currently scheduled for the November 2017 timeframe. The site visit will allow the JHU/APL team to interact with performer teams, observe demonstrations of performer solutions, and engage in technical deep dives to develop a comprehensive understanding of the capabilities of performer solutions and the solution’s integration with the JHU/APL testbed.

## Pre-Test Coordination

Pre-Test coordination meetings will be held between the JHU/APL T&E team and performer teams to discuss plans and strategy for sharing performer solutions with the T&E team and integrating performer solutions with the JHU/APL testbed. Pre-Test coordination meetings will provide JHU/APL with an opportunity to review and resolve testbed deployment and integration issues with performers. It is expected that pre-test coordination meetings will be held in advance of dry run test exercises and in advance of mid-term and final test events.

# Dry Run Test Exercise

Performers are encouraged to conduct dry run testing exercises well in advance of official testing events. A dry run testing exercise is an opportunity to deploy a performer’s solution, which may support limited capabilities or stubbed out interfaces, to the T&E testbed. A dry run exercise allows the T&E team to examine testbed-to-solution interactions and verify correct operation of testbed infrastructure. Dry run testing exercises are viewed as a critical risk reduction strategy that will allow both performers and the T&E team to uncover potential integration and deployment challenges. Failure to conduct dry run testing exercises may prevent integration and deployment complications from being discovered early enough to allow sufficient time and resources for issues to be resolved. Identification of testbed integration and deployment issues just prior to an official T&E event may severely limit or disrupt testing. The T&E testbed will be available for dry run testing exercises beginning in January of 2018.

# System Delivery

Virtue system delivery shall include the deployment ready Virtue environment, preferably a collection of Amazon Web Services (AWS) Amazon Machine Images (AMIs) and associated deployment configurations, as well as a documentation package. While the T&E team expects to collaborate openly and frequently with each performer team, final system delivery is expected on [*TBD*] or [*TBD*] days before mid-term and final testing.

## Documentation

The Virtue documentation package shall consist of the following artifacts: system architecture and design, systems interface specification, deployment guide, user guide, administrator guide, and a test readiness plan. This collection of documentation is considered a minimum set of artifacts. Performers are encouraged to provide any additional documentation that will assist the T&E team with developing a comprehensive understanding of their unique solutions. Delivery of Virtue documentation, including updates as system development progresses, is necessary in order to allow the T&E team to plan for and implement adjustments required to the testbed or test execution plan in order to accommodate unique capabilities offered by a performer solution.

### System Architecture and Design

A Virtue system architecture and design document shall describe the systems level view of a Virtue, including major sub-systems and their interactions, to include interactions with external systems. This document shall also identify system-level components and describe data flows between components.

### System Interface Details

A systems interface specification shall describe all Virtue interfaces necessary for the operation, management, and administration of the Virtue system and supporting environment. Special emphasis shall be given to interfaces that support client end-point connections (i.e., thin client) to a Virtue, and command and control channels to Virtues and supporting infrastructure. A well-defined systems interface specification is essential to assist the T&E team with preparing for integration of the Virtue system with the testbed. The interface specification is expected to provide software application programming interface (API) details that describe support for programmatic invocation of Virtue operations.

### Deployment Information

Virtue deployment information shall include instructions describing steps required to install and launch Virtue infrastructure and Virtue instances. Deployment information shall include AWS expected configurations including CPU, memory, storage, and network capacity. Deployment information shall also cover network configuration details which may include network interfaces, routing tables, internet gateways, DHCP options, use of DNS, IP address assignments, use of network address translation, and any other networking information that would assist the T&E team with Virtue deployment and testing.

### User Information

Virtue user information shall include instructions describing how standard Virtue users interact with and use the Virtue system. User information shall include items such as: using the Virtue client interface, launching a Virtue, authenticating to a Virtue, accessing Virtue applications, using Virtue applications, suspending a Virtue, and shutting down a Virtue.

### Administrator Information

Virtue administrator information shall include instructions describing how Virtue administrators interact with and manage the Virtue system. Administrator interactions covered shall include items such as: defining a Virtue role, managing Virtue users, managing Virtues, managing Virtue security settings, and managing Virtue logging settings.

### Test Readiness Plan

A test readiness plan shall contain procedures and checklists to be performed and reviewed to verify that a performer system is deployed correctly and operating as expected in the JHU/APL testbed. The test readiness plan shall include performance benchmarks to compare the solution’s performance while operating in the JHU/APL testbed against the performer’s development/test environment. Execution of the test readiness plan and acceptance of test readiness results represents official handover of the system under test to the T&E team.

## Virtue Deployment Package

Performer teams are responsible for providing all materials (i.e., a Virtue deployment package) required for the T&E team to replicate the performer’s AWS environment(s) in order to conduct T&E in a separate, JHU/APL-managed AWS environment. The Virtue deployment package should include the following essential items:

* Deployment Scripts – All scripts developed to interface with AWS SDK/API to support deployment and initialization of a performer’s Virtue environment
* Virtue AMI – AWS AMIs used by performers to establish a Virtue environment
* Source Code – All source code developed in support of the Virtue effort

Resource sharing between AWS accounts is the preferred approach to providing a Virtue deployment package to JHU/APL. This will allow JHU/APL to access performer-created AMIs as well as other required materials (e.g., deployment scripts, source code). Resource sharing will be disabled prior to an official testing event. Close and continued interaction between performer teams and JHU/APL is required to determine optimal strategies for sharing materials and replicating a performer’s AWS environment, especially given the potential for unique configurations and/or complex AWS service orchestration.

# Test Event

The VirtUE mid-term and final test event will be conducted at JHU/APL’s main campus in Laurel, Maryland. Performer teams are welcome to be on-site at JHU/APL for a total of three days in advance of mid-term and final testing. This pre-test period will allow performers to engage with the JHU/APL test team to confirm deployment and operation of their respective solutions. Test readiness procedures will be conducted to allow all parties to verify that the system-under-test is operating according to its deployment specification and properly integrated with the JHU/APL testbed. Known limitations and/or system failures discovered during solution deployment and standup will be documented and adjustments to T&E execution plans will be considered.

## Test Schedule

A three-day test readiness review will be conducted preceding the official start of each test event. Following the test readiness review stage, a four-week T&E effort will commence. At the conclusion of the T&E stage, test results will be analyzed and a test results report, per performer, will be developed and delivered to the VirtUE program manager.

Test readiness review activities may use the following schedule:

**Day 1:**

* 8:00AM – 8:30AM – Arrival and check-in
* 8:30AM – 9:00AM – Welcome and Opening Remarks
* 9:00AM – 12:00PM – Virtue Deployment Discussion (breakout sessions with performers and JHU/APL team members)
* 12:00PM – 1:00PM – Lunch
* 1:00PM – 4:00PM – AWS Configuration & Resource Verification (breakout sessions with performers and JHU/APL team members)
* 4:00PM – 4:30PM – Compile end of day summary (status, findings, and issues)
* 4:30PM – 5:00PM – End of day recap (performers dismissed)
* 5:00PM – 5:30PM – Gov’t and JHU/APL meeting

**Day 2:**

* 8:00AM – 8:15AM – Arrival and check-in
* 8:15AM – 8:30AM – Opening Remarks
* 8:30AM – 12:00PM – Virtue Functionality Walk-Through (breakout sessions with performers and JHU/APL team members to exercise Virtue capabilities)
* 12:00PM – 1:00PM – Lunch
* 1:00PM – 4:00PM – Virtue Performance Verification (breakout sessions with performers and JHU/APL team members to compare performance against performer benchmarks)
* 4:00PM – 4:30PM – Compile end of day summary (status, findings, and issues)
* 4:30PM – 5:00PM – End of day recap (performers dismissed)
* 5:00PM – 5:30PM – Gov’t and JHU/APL meeting

**Day 3:**

* 8:00AM – 8:15AM – Arrival and check-in
* 8:15AM – 8:30AM – Opening Remarks
* 8:30AM – 12:00PM – Virtue Security Walk-Through (breakout sessions with performers and JHU/APL team members to exercise Virtue security capabilities)
* 12:00PM – 1:00PM – Lunch
* 1:00PM – 4:00PM – Final Readiness Assessment (breakout sessions with performers and JHU/APL team members to examine and review open items and finalize readiness assessment)
* 4:00PM – 4:30PM – Complete readiness checklist
* 4:30PM – 5:00PM – Gov’t and JHU/APL meeting
* 5:00PM – 5:30PM – Readiness review closeout

Following the three-day test readiness event, JHU/APL will conduct T&E of performer solutions. JHU/APL expects to conduct T&E of performer solutions in parallel using separate and isolated systems, networks, and AWS instances. Functionality, performance, and security testing will be performed against performer solutions over a four-week testing period.

# Rules of engagement

This section describes rules of engagement that define assumptions and known limitations of the T&E environment and testing process; communications with the T&E team; access to the VirtUE testbed for dry run test exercises; and expectations for system delivery, test events, and test execution.

## Assumptions and Limitations

Assumptions and known limitations of the T&E environment and testing process are identified below.

* Performer solutions will be deployed to AWS.
* Performer solutions will be deployed to a JHU/APL AWS managed instance(s).
* Performer solutions may be deployed to in-house JHU/APL testing infrastructure.
* JHU/APL is responsible for paying for AWS charges incurred in APL’s AWS account during T&E.
* Performer is responsible for paying for AWS charges incurred in Performer’s AWS account during T&E.
* Performer solution will provide a means of establishing new user accounts (Virtue users).
* Performer solution will provide a means of establishing new administrator accounts (Virtue administrators).
* Performer solution will provide a means of establishing new Virtue roles.
* Performer solution delivery will not include hardware (e.g., servers, network switches, client access points).
* T&E will be conducted within AWS.
* T&E network connections to AWS will originate from JHU/APL networks.
* T&E team will provide the following enterprise services: Network Time Protocol (NTP), Simple Mail Transfer Protocol (SMTP), Network File Storage, and Active Directory.
* T&E team will obtain security authorizations from AWS before conducting security tests.

## Test and Evaluation

This section defines specific rules and sets clear boundaries to be followed during T&E. T&E rules of engagement are intended to establish a common understanding of testing expectations, acceptable test methods, test conditions, and potential test targets.

* An upper bound limit on test execution time will be defined for applicable test cases to prevent indefinite wait for test completion.
* Virtue client-endpoints shall support either Remote Desktop Protocol (RDP) or Virtual Network Computing (VNC) in order to integrate with JHU/APL’s testbed.
* Virtue client-endpoints shall support SSH connections in order to integrate with JHU/APL’s testbed.
* Virtue client-endpoints shall provide a Virtue command line interface to enable JHU/APL testbed components to invoke Virtue operations.
* Virtue logging apparatus shall provide an interface to enable retrieval of collected log data.
* Virtue logging apparatus shall provide an interface to enable configuration of logging.
* Virtue security apparatus shall provide an interface to enable configuration of security settings.
* Reset mechanism needs to exist to allow T&E team to reset Virtue environment (e.g., remove registered users, registered Virtues).
* T&E test assets may be placed inside a Virtue or Virtue supporting infrastructure in order to monitor and/or instrument test execution and gather data required for analysis.
* T&E team may have access to commercial cloud infrastructure components (e.g., AWS hypervisor) to support test execution and monitoring.
* T&E team will perform regular T&E infrastructure calibration to verify data collection, time synchronization, and access to performer system.
* T&E will be conducted against images and binaries provided by performers, however JHU/APL reserves the right to build from source to create fresh binaries.
* The following Windows applications are expected to be supported: MS Office, MS Outlook, MS Communicator, Internet Explorer, Windows Media Player, and File Explorer.
* The following Linux applications are expected to be supported: Open Office, Thunderbird, Firefox, Skype, GIMP, and VLC Media Player.
* Security testing may include port scans and other network service interactions and queries.
* Security testing may include attempted logins or other use of systems, with any account name/password.
* Security testing may include use of exploit code.
* Security testing may include “hands-on” red teaming activities.
* Security testing may include spoofing or deceiving servers regarding network traffic.
* Security testing will not include denial of service attacks (smurf, land, SYN flood, etc.).
* Security testing will not include exploits that will introduce new weaknesses to the system.
* Infrastructure attacks are attacks originating from the AWS hypervisor.
* Insider attacks may originate from an authorized user within a Virtue.
* Peer-to-peer attacks may originate from within a Virtue (to include a virtual machine, container, or other Virtue construct as defined by a performer’s solution) and launched against another running Virtue.
* Human subject testing may be performed to assess the usability of performer solutions in order to evaluate a Virtue’s impact on a user’s work effectiveness.

# JHU/APL Visitor control

JHU/APL is a secure facility, operating under Department of Defense regulations for restricted entry. All visits to the Laboratory must be pre-approved via written request and notification by responsible staff members. All performer visits and visit requests shall be coordinated with the JHU/APL VirtUE project manager:

Name: Chris James

Email: [christopher.james@jhuapl.edu](mailto:christopher.james@jhuapl.edu)

Phone: 443-778-2858

Visitors must present photo identification to the lobby receptionists, sign the visitor register, receive the appropriate badge, and remain under escort unless otherwise authorized by Visitor Control. Visitors should be aware of APL rules for bringing [restricted and controlled items](http://jhuapl.edu/privacy/controlled.asp), such as electronic devices, on site. All computer equipment must be checked in with the guard at the point of entry. At that time, a property tag (valid for 1 day) will be issued and affixed to the equipment. Additional details on JHU/APL’s rules for bringing restricted and controlled items can be found on JHU/APL’s public website - <http://jhuapl.edu/privacy/controlled.asp>.

Additional visitor information, including a campus map can be found on JHU/APL’s public website - <http://jhuapl.edu/aboutapl/visitor/default.asp>.

## Non-U.S. Citizens

Advance notice (a minimum of 30 – 45 days) is required to process visit requests for non-U.S. Citizens. Non-U.S. Citizen visit requests shall be coordinated with the JHU/APL VirtUE project manager.

## Network Access

Guest network access will be provided to visitors and may be accessed from computer equipment owned and operated by a visitor. Network access may include wireless or wired network connectivity. Visitors requiring network access shall coordinate with the JHU/APL project manager so guest accounts and access permissions can be established in advance of a visit to JHU/APL.

# Summary

The Virtue Test and Evaluation Handbook provides guidance and sets expectations on items pertaining to Virtue test and evaluation activities. This includes outlining performer interactions with the T&E team, expectations concerning system delivery, expectations of pre-test events and test events, T&E rules of engagement, and requirements and procedures for visiting the APL campus. In the event that program developments necessitate modifications to guidance provided in this document, an updated version of this document will be released.

1. VirtUE Broad Area Announcement: https://www.iarpa.gov/index.php/research-programs/virtue/virtue-baa [↑](#footnote-ref-1)