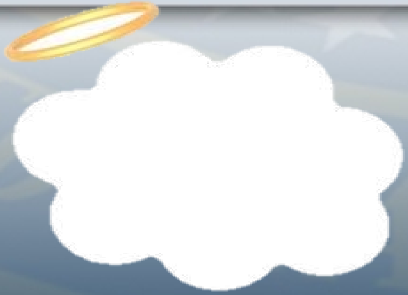
OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

VirtUE Proposers' Day



Kerry Long PM

July 19, 2016

dni-iarpa-baa-16-12@iarpa.gov

Proposers' Day Goals

- Familiarize participants with IARPA and with the VirtUE program concept:
  - Brief participants on the goals and metrics of the Phase 1 BAA
  - Provide participants information about successive program goals
- Solicit feedback and questions.
- Foster networking and discussion of synergistic opportunities and capabilities among potential program participants (A.K.A. "teaming")

Proposers' Day Goals

- Please ask questions and make suggestions: this is your chance to influence the design of the program
  - Record your questions and comments on the note cards provided and submit them to IARPA staff during the break
  - After today, questions will be answered in writing on the program website
- Once a BAA is released, questions can only be submitted to the email address provided in the BAA

Disclaimer

These presentations are provided solely for information and planning purposes.

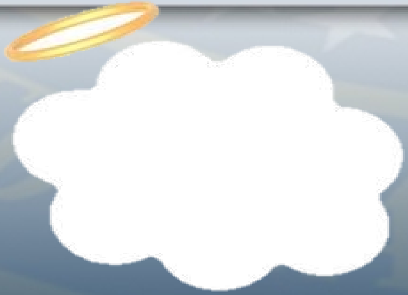
The Proposers' Day does not constitute a formal solicitation for proposals or abstracts.

Nothing said at Proposers' Day changes the requirements set forth in a BAA.

- A BAA supersedes anything presented or said by IARPA at the Proposers' Day

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

Program Overview
Virtuous User Environment (VirtUE)
Phase 1



Kerry Long PM
July 19, 2016

Presentation Outline

- Motivation
- Current Status
- Objectives
- Program Examples
- Design Considerations
- Phase 2 Intro
- Program Challenges
- Scope
- BAA Overview
- Program Structure and Deliverables
- Test and Evaluation
- Technical Milestones and Program Metrics
- Reporting Requirements
- Schedule
- Management Plan and Teaming
- Proposal Evaluation Criteria

VirtUE Bottom Line

Leveraging the Intelligence Community (IC) Move to Virtualization:

VirtUE seeks to rethink the interactive user computing environment** (UCE) – turning it into a more dynamic, secure sensor and defender without alienating users (Phase 1)

VirtUE seeks to develop and demonstrate unique security analytic and control technologies that can directly interact with a new UCE to both detect and prevent unwanted activities within the UCE (Phase 2)

**** Think User's Desktop**

Motivation

- IC ITE initiative moving IC classified infrastructure to a large private cloud
- New threat profile for government users operating in the cloud
- Implications of moving government unclassified infrastructure to public cloud

Motivation

- The new possibilities that virtualization offers
- Recent explosion in virtualization/OS projects that offer different capabilities and performance options
- Frustration with 20 years of failing to protect user’s desktops
- Disappointment with existing “Big Data” security analytic efforts that rely on user workstation data

How is it Done Today?

- Government is simulating physical workstations in the cloud through use of the virtual desktop technology (VDI) Citrix Xen Desktop -Current UCE
- A predefined, general purpose Windows virtual machine is launched on a commercial cloud infrastructure for each user
- Instrumentation is based on resident processes like agent-based technologies running within the Window's VM
- Security analytics consume whatever data is provided by virtual desktops and forward results of basic analytics to a commercial SEIM for human analysts to detect malicious actions

How is it Done Today – Security Analytics

Test & Evaluation Categories	ArcSight ESM	Entrasys Networks SIEM	Cinxi One	QRadar	Symantec SIM	Shapes Vector
Fraction of Logs Analyzed	90%	60%	65%	85%	75%	60%
Attack Detection	4%	0%	21%	0%	0%	4%
Detection of "low and slow" attack incidents	0	0	0	0	0	0

Source: "Independent Validation and Verification (IV&V) of Security Information and Event Management (SIEM) Systems Final Report"
SPAWAR for DARPA/I2O, January 2011

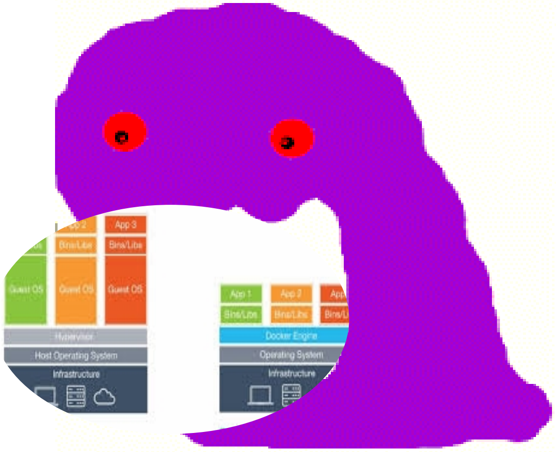
The Problem –
Available virtualization constructs inadequate

- UCEs in the cloud are normally run in a standard Windows VM

- These VMs provide little more protection against traditional external and internal threats than physical workstations

- VMs are also subject to additional threats in the form of malicious peer workloads and hypervisor/management plane attacks and have few innate defenses against them

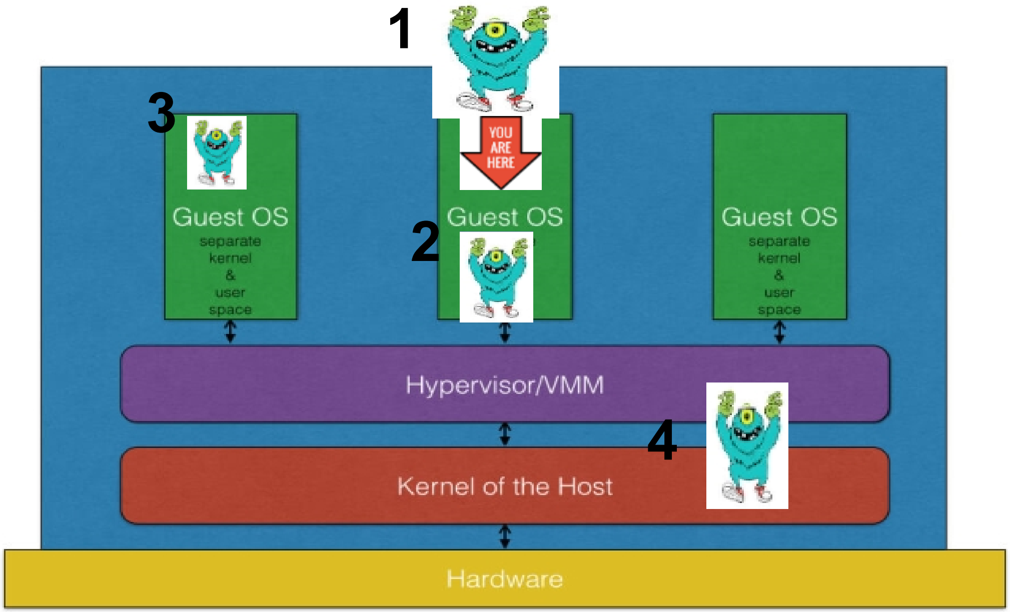
- Another popular virtualization construct is a LXC or Windows container which can be more efficient but has even less isolation from hostile peers than VMs



The Problem – Current UCE paradigm

- Excessive user flexibility makes user behavior hard to profile for security analytics
- Offers no trusted way of obtaining security log information or of implementing internal countermeasures
- Very hard to make this environment dynamic or responsive to attacks
- Attackers use this environment’s shared memory pool, complexity and numerous components to compromise its security
- Not designed to detect or resist security threats of the cloud

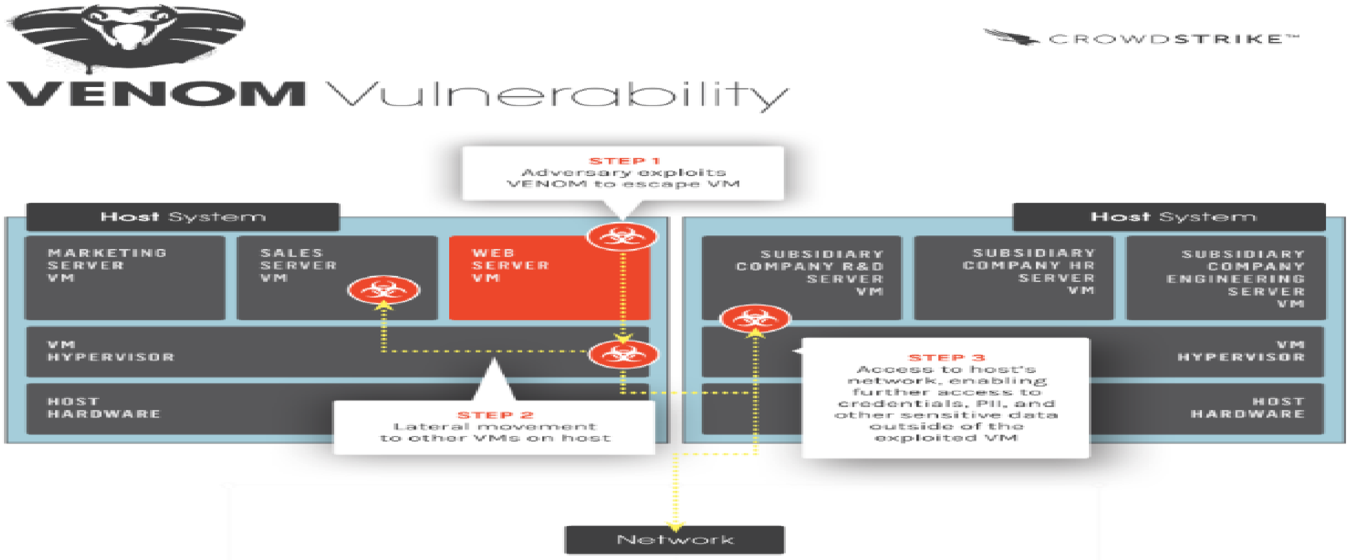
Threats UCE Must Now Counter



Hypervisor based Virtualization

1. External
2. Internal/Insider
3. Peer
4. Hypervisor/Mgmt Plane

Threats UCE Must Now Counter


VENOM Vulnerability
CROWDSTRIKE™
STEP 1
Adversary exploits VENOM to escape VM
Host System
MARKETING SERVER VM
SALES SERVER VM
WEB SERVER VM
VM HYPERVISOR
HOST HARDWARE
STEP 2
Lateral movement to other VMs on host
Host System
SUBSIDIARY COMPANY R&D SERVER VM
SUBSIDIARY COMPANY HR SERVER VM
SUBSIDIARY COMPANY ENGINEERING SERVER VM
VM HYPERVISOR
HOST HARDWARE
STEP 3
Access to host's network, enabling further access to credentials, PII, and other sensitive data outside of the exploited VM
Network

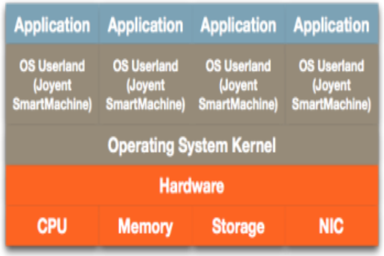
"The VENOM vulnerability has existed since 2004, when the virtual Floppy Disk Controller was first added to the QEMU codebase"
Crowdstrike

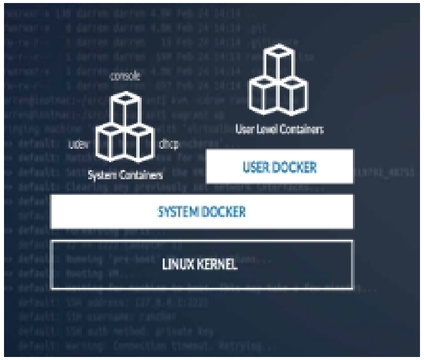
Picture Crowdstrike.com

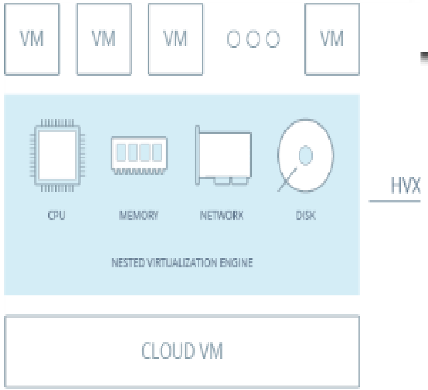
Virtualization Renaissance

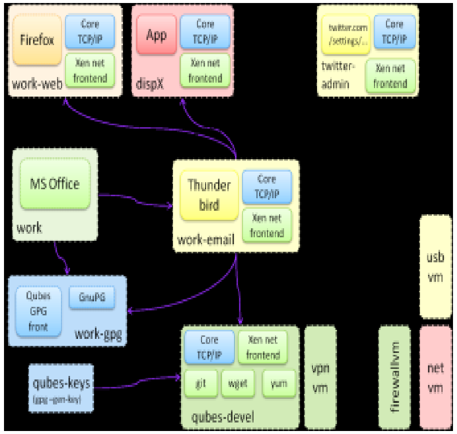
teradici®

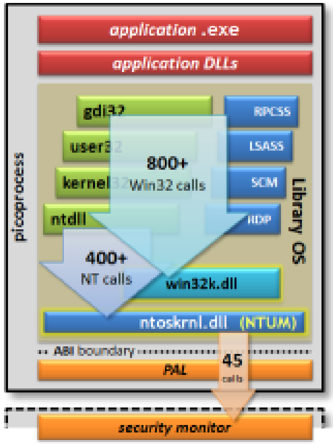
SPICE Project

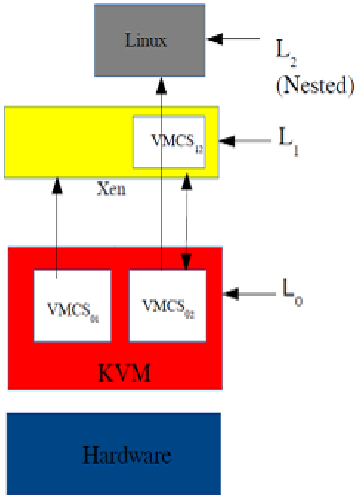

Application
Application
Application
Application
OS Userland (Joyent SmartMachine)
OS Userland (Joyent SmartMachine)
OS Userland (Joyent SmartMachine)
OS Userland (Joyent SmartMachine)
Operating System Kernel
Hardware
CPU
Memory
Storage
NIC











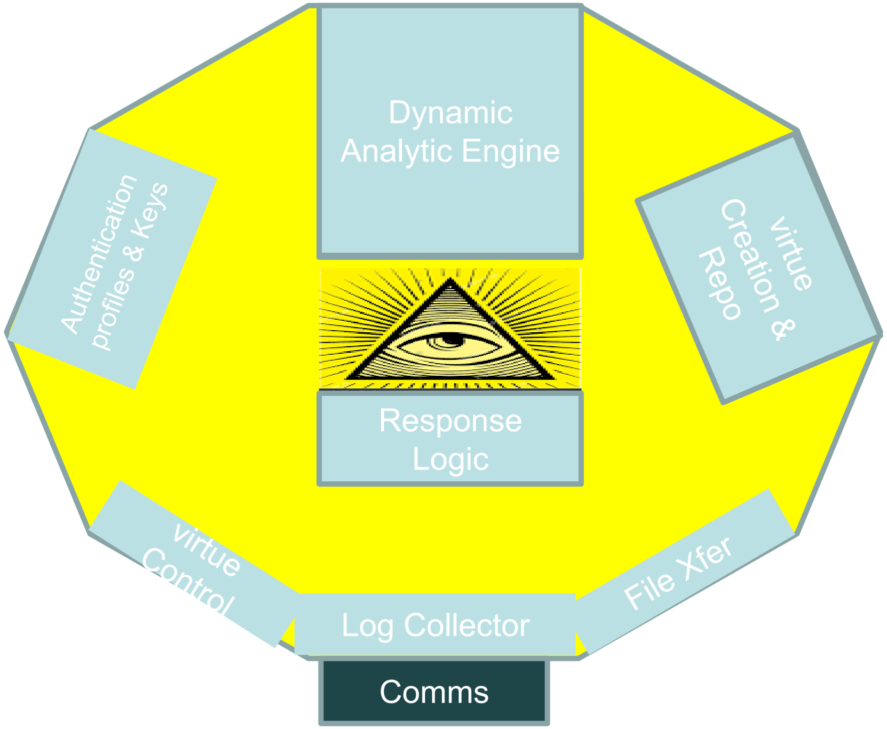
Pictures SmartOS.org, racncher.com, qubes-os.org, www.ravellosystems.com, research.microsoft.com, bitdefender.com, spicespace.org, linux-kvm.org, semanticscholar.org and docker.org

Program Objective – Make a better UCE

Create a "virtue"

& virtue support functions

Phase 1

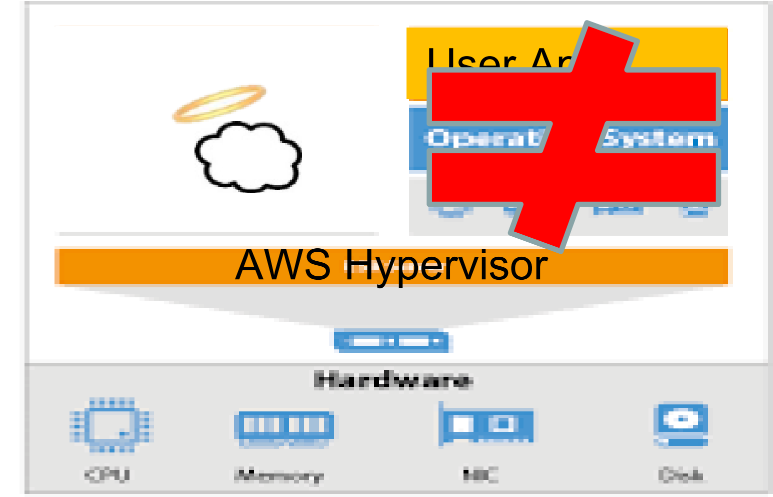


Create VirtUE Analytics and Control Platform

Phase 2

What's a virtue?

- The virtue is a modular, defensible interactive user computing environment running on a typical cloud provider's virtualized infrastructure, but is not restricted to the common construct of a VDI workload



Picture:veeam.com

What's a virtue?

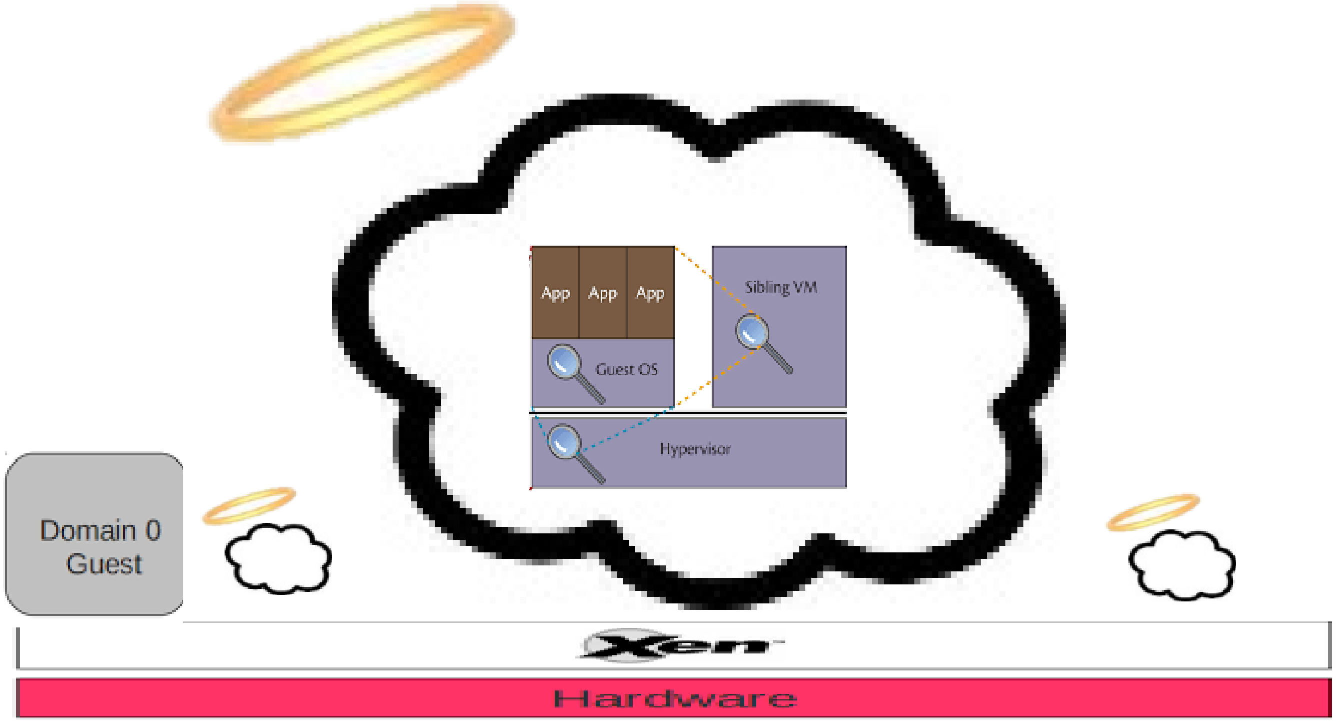
- The performer's key creative task is to devise what an individual virtue should consist of to meet the objectives of the program

- A virtue should:

  - ✓ Present itself as an atomic, immutable entity to other virtues and external processes
  - ✓ Meet the security/performance objectives of the VirtUE program
  - ✓ Capable of running within the Amazon Web Services (AWS) infrastructure.

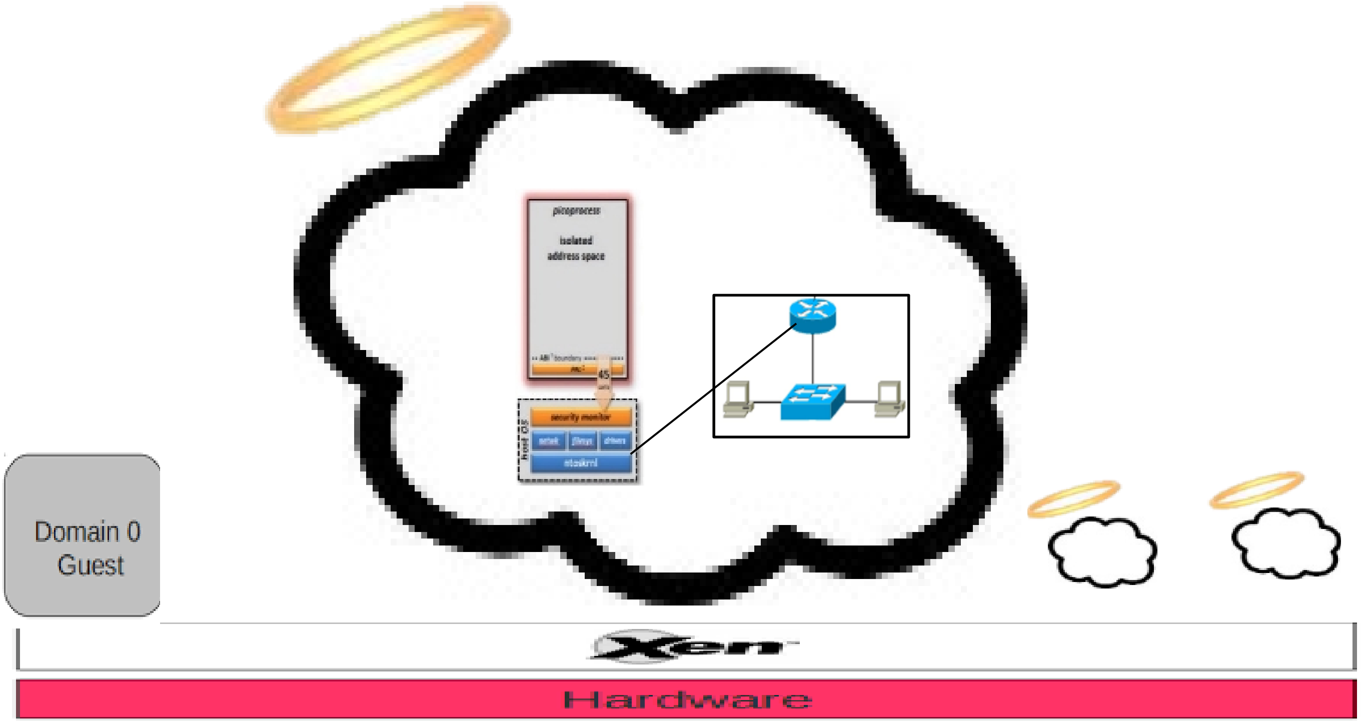
What's a virtue? (not prescriptive)

Maybe this



What’s a virtue? (not prescriptive)

Maybe this



Drawbridge Picture research.microsoft.org

Program Goals- Do it Different

VirtUE phase 1 seeks to build the foundation for Phase 2 by:

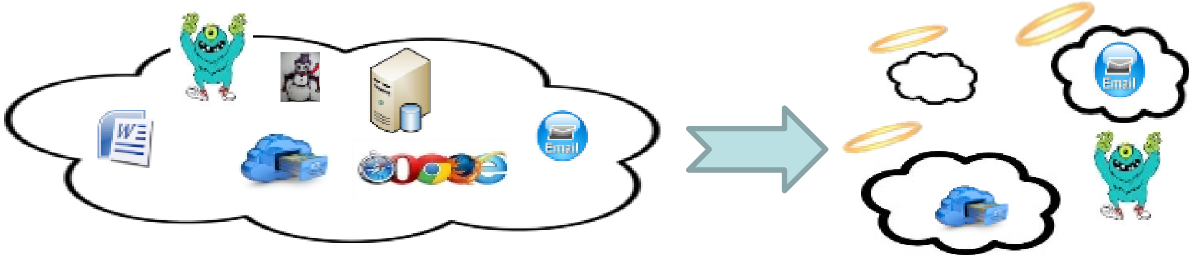
Phase 1

1. Creating a virtue
   - Built on a more defensible virtualized construct than VDI
   - Simpler, modular, role-based
   - Capable of multiple dynamic sensoring/response actions tailored to risks
   - Capable of running several legacy Windows and Linux applications
   - Resistant to all 4 security threat vectors expected on a public cloud

2. Developing a presentation interface combining numerous authorized virtues to provide all the functionality required by a user delivered securely to an end device

3. Inventing methodologies and toolsets to define, construct, control (APIs), and transport virtues (Inspired by Docker Concept)

Goals 1 - 3 Explained

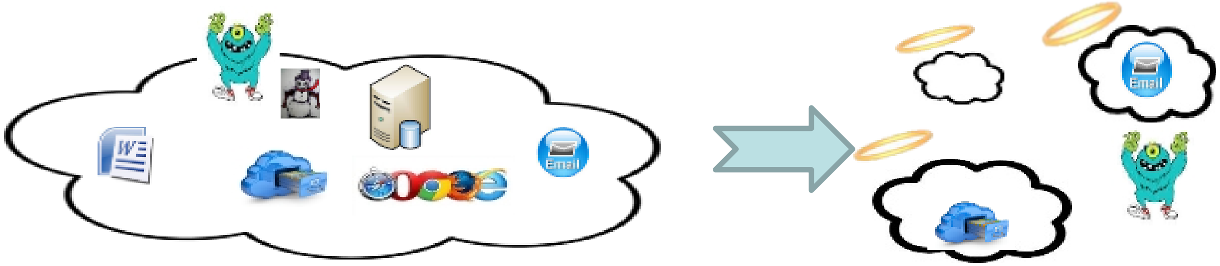


Decompose the generic user desktop environment that currently exists to mimic a physical workstation into specially instrumented role-based virtual environments (virtues)

Roles equate to closely related functions users will be allowed to perform using a particular virtue and will be enclave defined

Limit possible behaviors of individual virtues to make them easier to define and constrain (simpler)

Goals 1 – 3 Explained



Create sensing and response actions tailored to the specific risk profile of the virtue

Make virtues responsive and intuitive for users

Allow users to interact with several virtues at one time to fulfill all their work roles (modular)

Make it easy to create, modify and share virtues among various government participants

Examples of possible Role-Based virtues

(not all-inclusive)

- 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

Document Editor/Creator/Printer virtue

Functions:

- Read, alter, and create Microsoft Work or Adobe documents in a user's home directory
- Read, alter, and create Microsoft Work or Adobe documents in shared directories
- Print these documents
- Copy files to web publisher virtue

Specific Risks to mitigate:

- Deleting needed files
- Altering important files
- Copying files to unauthorized location
- Printing files for stealing

Possible Properties of a Windows Document creator virtue (for document creator role)

A Document Creator virtue's capabilities:

Internet access	No
Printer access	Yes
Email server access	No
Home Dir write access	Yes
Web Publisher virtue access	Yes

Document Creator virtue Possible Response Actions:

Deny writing documents
Freeze and Quarantine virtue
Secretly copy file to security
Display warning to user
Kill WinWord.exe

A Document Creator virtue's components:

Internet Explorer	No
Microsoft Word	Yes
Outlook	No
Power Shell	No
Adobe	Yes
Admin Tokens	No
User Tokens	Yes
PKI keys	No

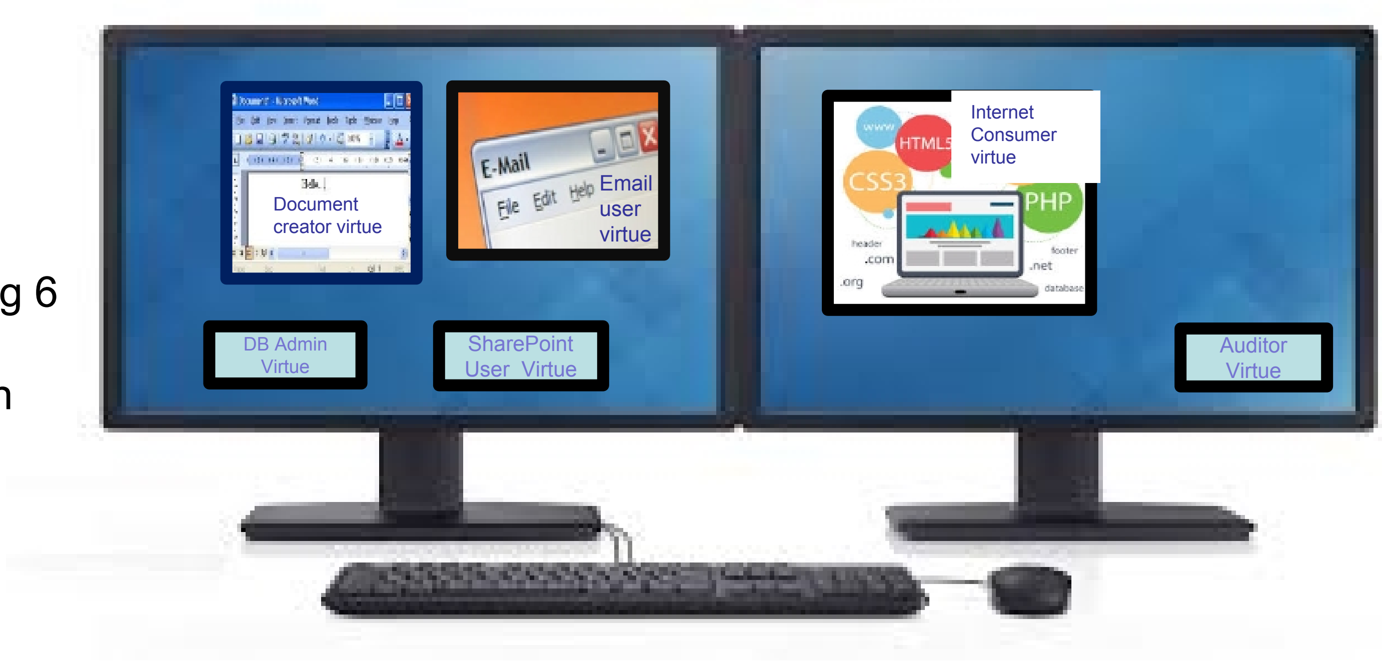
Document Creator virtue Logging:

Documents Printed	Yes
Files Opened	Conditionally
Files Created	Yes
Files altered	Yes
svchost.exe in memory	Conditionally

One Example of a possible presentation interface

(not prescriptive)

User running 6 virtues in presentation interface



Virtue Specific Design Considerations

- Capable/compatible with public cloud infrastructure such as AWS
- Must have formalized methodology to create, audit and distribute virtues
- Instantiations of a virtue are immutable and version controlled, but existing virtues can serve as base for new virtue creation
- Virtues must resist and aid in the detection of threats from the APT, hypervisors, virtualized peers (including other virtues), and internal virtue processes
- Virtues must have numerous inherent logging capabilities and the potential to add more
- Virtues should have the capability of exercising numerous response actions in coordination with control plane
- Virtues must have a well thought out API for future analytics and virtue control plane managers to interface with

Virtue Specific Design Considerations (continued)

- Virtues need to be able to use network printers and access network file shares and resources
- Several virtues will be used by an individual at once. They must be performant
- Certain virtues may need to exchange data such as hyperlinks securely
- A secure mechanism is needed to save some user state for a virtue's use such as favorite web sites, home page, default printers
- Users will require some virtues with the ability to run Microsoft Apps
- Virtues need to be part of an overall user interface strategy that delivers them seamlessly to thin clients over existing network protocols
- User interface must enable users to select which virtues they wish to run from available virtues they will be authorized to access in control plane*
- User interface should enable user to start and stop virtues on demand

*** Control plane is a phase 2 deliverable but both presentation interface and virtues will need to code routines for interacting with one.**

About Phase 2

- Ultimately the purpose of Phase 1 is to produce technologies that can be used by Phase 2 performers to build the virtuous user environment.

- Phase 2 performers will be responsible for the performance and security of any Phase 1 technologies they incorporate into their solutions.

Program Goals - Do it Different

VirtUE phase 2 seeks to develop and demonstrate:

Ph
as
e
2

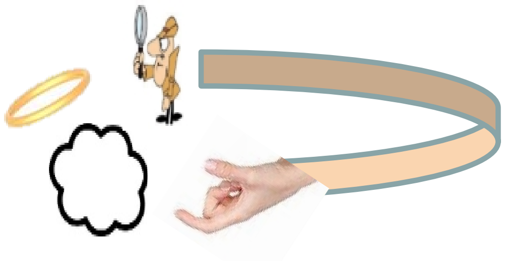
4. Dynamic security analytics and actions that can leverage the unique qualities of the virtue

5. Methodologies and templates to construct and transport dynamic security analytics

6. A control infrastructure to deploy, operate, and manage virtues and dynamic analytics within a commercial public cloud like AWS

Goals 4 & 5 Develop and Demonstrate Dynamic Analytics and Actions:

Develop security analytics for an assortment of IC inspired security problems that can adjust data sources and the monitoring environment dynamically to enable logic far more powerful and efficient than current analytics while potentially reducing* the total amount of security data collected

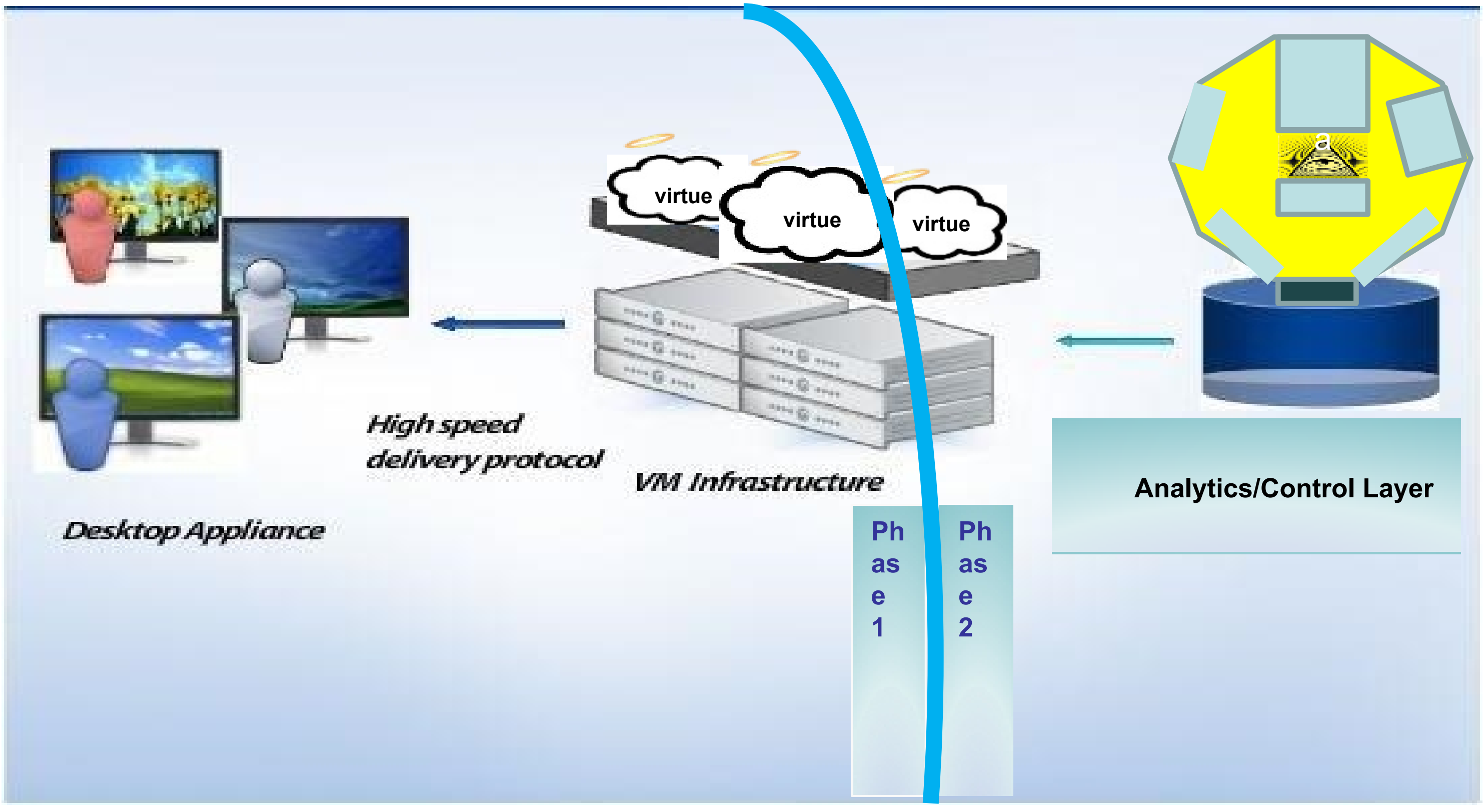


Direct reasonable responses based on the probabilities of compromises

Leverage dynamic response capabilities of virtues to mitigate confirmed compromises in creative/useful ways

* *Amazon RedShift charges about $1000 per TB per year for cloud storage*

Program Objective – Create this



Base Picture Citrix.com

Program Challenges

1. Current virtualization research efforts focus on making low-interaction cloud workloads safer, more performant
2. User interface must be as responsive, and functional as current desktop VDI environment
3. Computational resources required for virtues must not significantly exceed resources already provisioned for conventional VDI
4. Admins must be able to create and or customize new virtues with varying capabilities in a matter of minutes
5. Analytics must be able to adjust virtue behaviors in a matter of seconds
6. Performance in the cloud is often enhanced through hardware sharing, security is not

Program Challenges

7. Different virtues of a user need to exchange data without exchanging risks
8. Analytics must demonstrate measurable reductions in data collected compared to existing analytics
9. Analytics must be able to run on existing AWS cloud offerings
10. Analytics must be able to track state for attacks that can span several weeks
11. Virtues must offer options for both Windows and Linux user apps
12. Virtues must maintain some user state without maintaining adversary persistence
13. VirtUE must support windows authentication tokens without incurring vulnerabilities of traditional Window’s workstations

Threat targets for the Program

Mitigate :

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 currently in scope:

1. DOS
2. hardware alterations
3. Attacks directed against Analysis/Control infrastructure (except from virtues)
4. Guest and hypervisor collusion attacks

VirtUE Research Scope

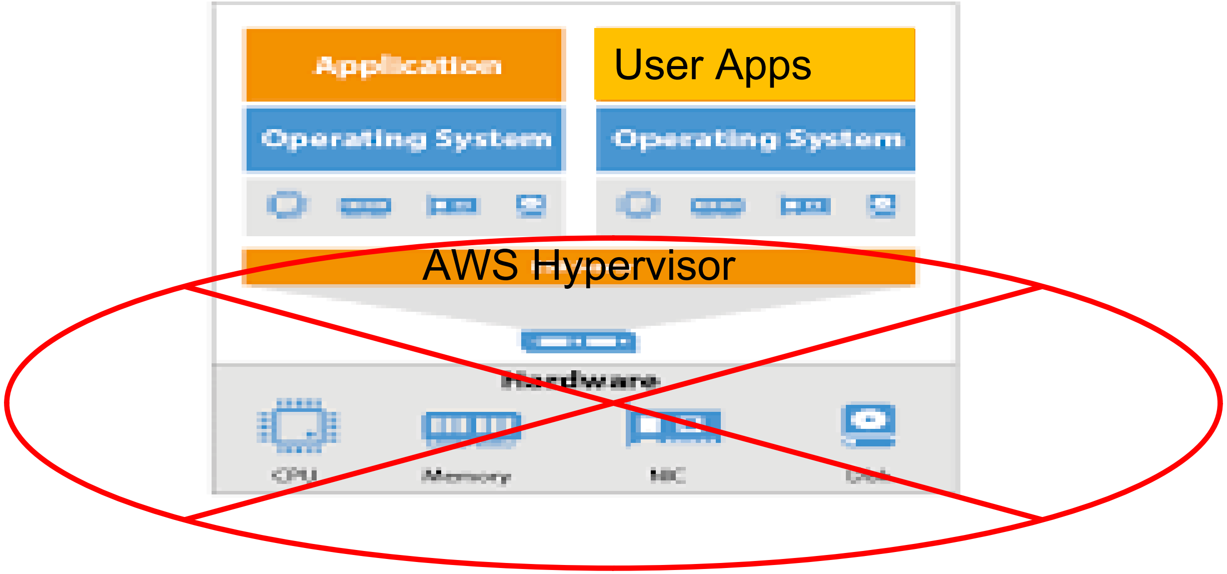
In Scope Research Areas

- Operating Systems
- Computer Security/exploitation
- Hypervisors/virtualization constructs
- Security Analytics/machine learning
- User interface design and human factors
- Secure data exchange protocols and methods

VirtUE Research Scope

Out Of Scope for this effort

Any changes to this (not available by Jan 2018 in AWS)



VirtUE Research Scope

Out Of Scope for this effort

- Recreating remote desktop access technologies such as PCoIP, HDX, Spice, VNC, RDP – Existing access technologies are permissible additions to any proposer solution
- Hardware dependent solutions – based on hardware not already planned for implementation by AWS on cloud production servers by Jan 2018
- SEIM or data aggregation solutions
- Approaches that propose or are likely to result in only incremental improvements over the current state of the art (i.e. strictly agent-based solutions)
- Technology offerings which can't be made available to open source community
- Protections optimized for server, HPC or other low interaction computing workloads
- Analytic methods that depend on proprietary data sources

BAA Overview,
T&E

BAA Highlights

2 BAAs; 2 Sets of proposals – staggered about 12 months apart

Phase 1 BAA Proposals: Create the virtue, the UCE and supporting tools - at program inception

Phase 2/3 BAA Proposals: Build and prototype a virtuous environment - due 12 months later

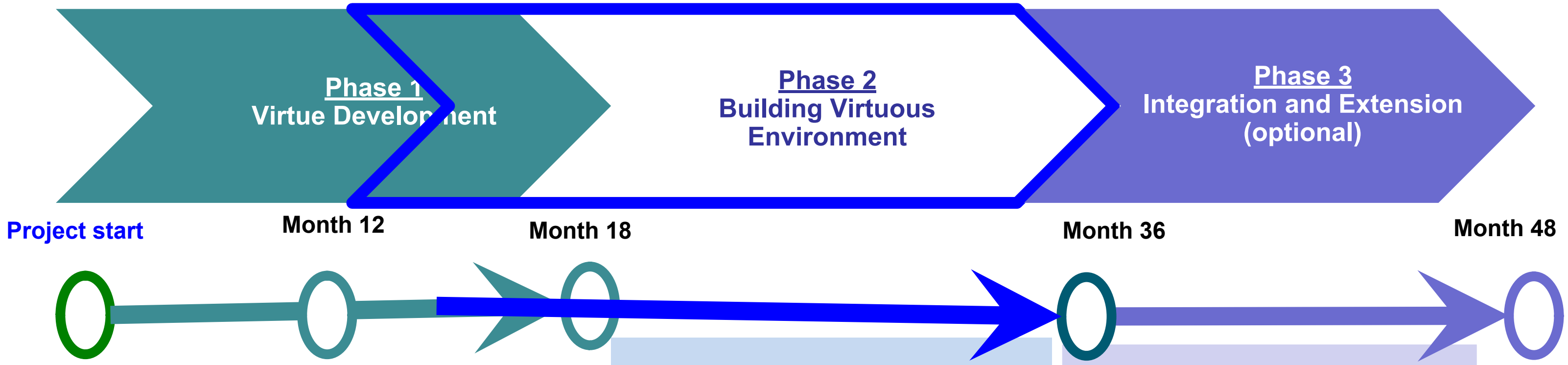
BAA Highlights

- Program duration: Approx. 4 years

  Phase I: 1.5 years
  Phase II: 1.8 years (overlaps phase 1 by about 3 months)
  Phase III: 1 year (optional –at Government's discretion)

- Technical Milestone testing roughly every 9 to 10 month (twice per phase)
- Security, Functionality, & Performance Metrics for each milestone
- Proposers can submit proposals for Phase1, Phase 2, or both

VirtUE Timeline



Phase 1
Virtue Development

Phase 2
Building Virtuous Environment

Phase 3
Integration and Extension (optional)

Project start

Month 12

Month 18

Month 36

Month 48

- virtue technology development "construct" and user interface
- Development of virtue utilities to create and modify virtues
- Develop API to control and query virtues
- Develop virtue methodology to store and share virtues

- Develop an Infrastructure to deliver, manage, and communicate with virtues
- Develop analytics that address representative IC security problems using the unique capabilities of virtues
- Refine virtue capabilities to meet objectives

- Deploy and integrate VirtUE infrastructure within representative IC cloud
- Assist IC analytic developers in instrumenting VirtUE for detection problems
- Create Open Source repository for Unclassified virtue technologies

Deliverables – Phase 1

- Deliverables
  - Virtue code and documentation with API to interface with T&E testing apparatus/Phase 2 products
  - Virtue management toolbox code and documentation
  - Reports
  - Academic quality publication with final results freely available on the Internet
  - Posting all code to publically accessible repository like GitHub, Bitbucket, etc.
- Program Coordination
  - Completed code and documentation are to be available to Phase 2 performers for testing and adoption as part of a spiral development cycle

VirtUE Test and Evaluation

Validation of technical soundness via independent verification by T&E teams as government representatives

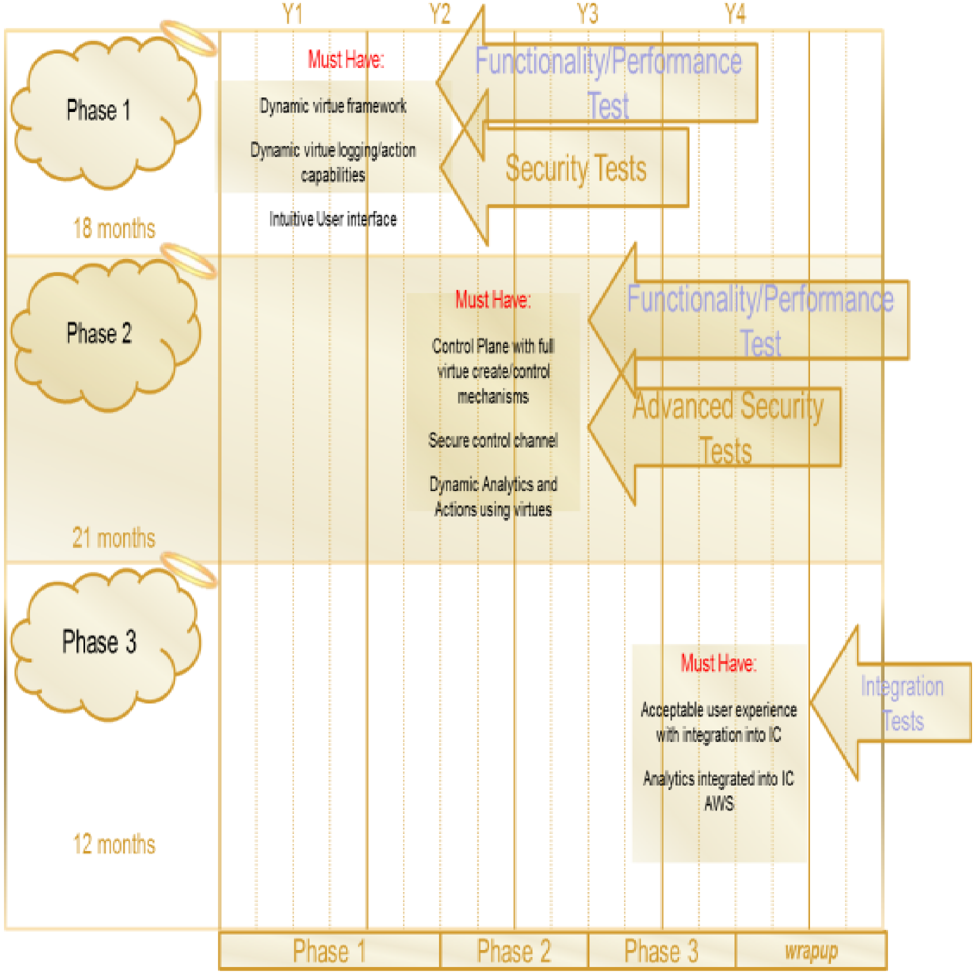
- Will design a testing regimen using a test rig to measure preselected functional, security and performance metrics for performer's products at midterm and final exams
- T&E team will release to performers representative metrics to be assessed and the type of testing to expect
- T&E team will release to performers specific technical interface requirements for ensuring offerings will work on testing rig

- Test rig will be an approximation of the IC ITE environment (test rig) based on AWS
- Capability to simulate increased loads, likely attacks and required functionality

Picture Credit: www.hegewald-peschke.com

Milestones

Goals and Exams


Y1
Y2
Y3
Y4
Phase 1
18 months
Must Have:
Dynamic virtue framework
Dynamic virtue logging/action capabilities
Intuitive User interface
Functionality/Performance Test
Security Tests
Phase 2
21 months
Must Have:
Control Plane with full virtue create/control mechanisms
Secure control channel
Dynamic Analytics and Actions using virtues
Functionality/Performance Test
Advanced Security Tests
Phase 3
12 months
Must Have:
Acceptable user experience with integration into IC
Analytics integrated into IC AWS
Integration Tests
Phase 1
Phase 2
Phase 3
wrapup

Proposed Measurement Criteria:

1.0 **Security test regimen** – Architecture is ultimately able to deter, detect, and/or mitigate representative attacks that target user computing environments

2.0 **Functionality test regimen** – Architecture must meet all desired functional requirements while enabling users an experience that compares favorably with existing VDI environment

3.0 **Performance test regimen** – Architecture must be able to satisfy criteria above under processing loads expected within the government cloud using expected computational resources

How We'll Measure

1.1 Security Deterrence Criteria (Inherent capabilities of virtue constructs):

Permitted – Nothing in the environment inherently prohibits action

Inhibited – Architecture inherently makes action more difficult to accomplish than base VDI environment, but still within the scope of possibility

Prohibited – Architecture prevents the unwanted action from occurring

Mitigated – Architecture allows compromise but reduces compromise impact

Example Security Deterrence Metrics

Objective	Assessed Criteria	Phase 1 Midterm	Phase 1 Final	Phase 2 Final
1.1 Security-Deterrence	Adversary attempts moving unexpected data between virtues	Inhibited	Prohibited	Prohibited
	Adversary uses stolen external credentials	Inhibited	Inhibited	Mitigated
	Insider attempting to exfiltrate data	Inhibited	Inhibited	Prohibited
	Spear Phishing/waterhole attack	Inhibited	Prohibited	Prohibited
	Insider elevates privileges	Inhibited	Inhibited	Mitigated
	Adversary attacks from hypervisor	Inhibited	Inhibited	Mitigated

Example Functionality Metrics

Objective	Assessed Criteria	Phase 1 Midterm	Phase 1 Final
2.0 Functionality	Number of virtues user can connect to concurrently	3	6
	Can open 3 attachments successively	Yes	Yes
	User will be able to save Documents created in a virtue and retrieve in another virtue	Yes	Yes
	Constructing a new virtue with a new role will take	30 Minutes	10 minutes

Example Performance Metrics

Values compared to reference VDI or stated criteria

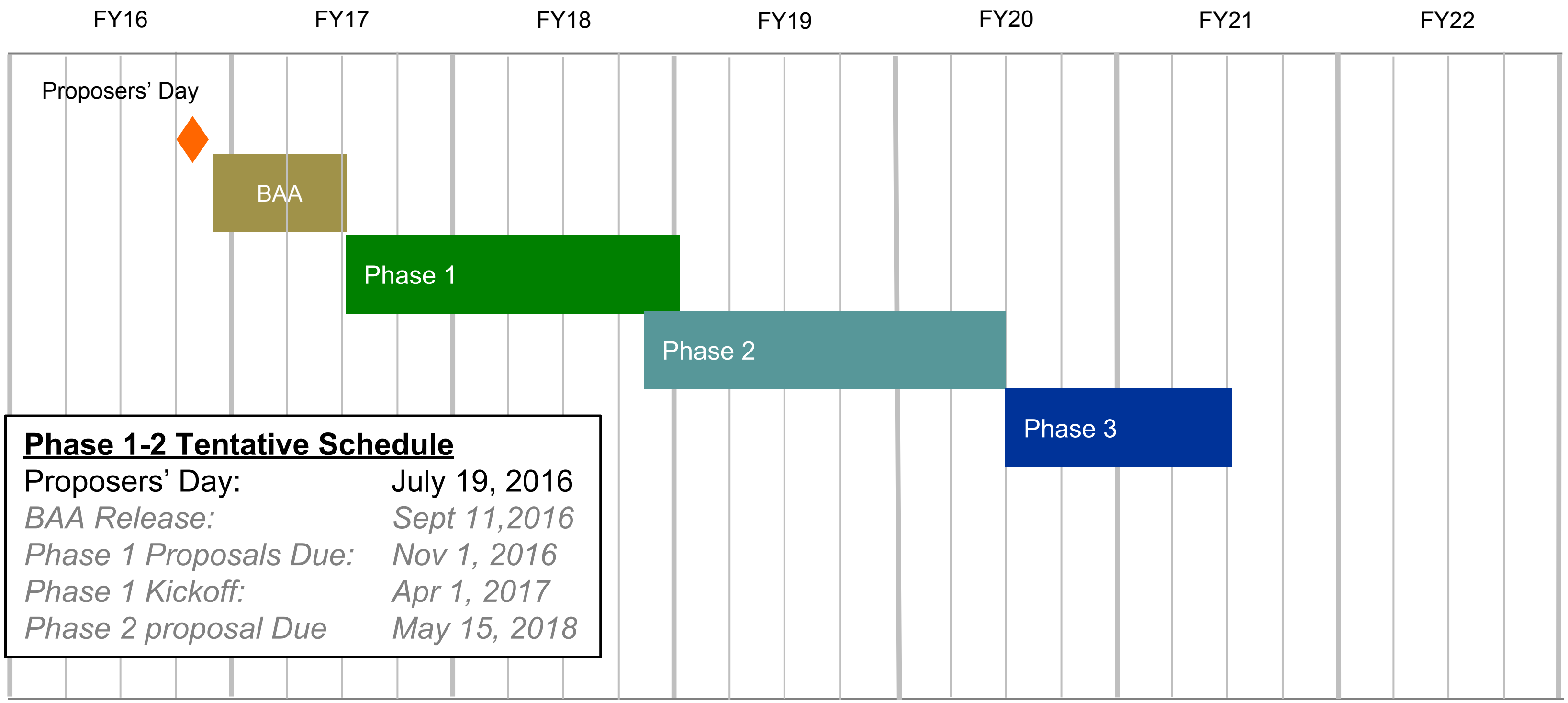
Ideal: parity or better
Acceptable: < +10%
Degraded: < +30%
Unaccept: > +30%

Objective	Assessed Criteria	Phase 1 Midterm	Phase 1 Final	Phase 2 Final
3.0 Performance	Opening an new virtue while 100 users interacting with the architecture with 5 virtues already open	Degraded	Acceptable	Ideal
	Opening a new virtue with 1000 users interacting with architecture with 5 virtues already open	Degraded	Degraded	Acceptable
	CPU/Memory performance for reading email	Acceptable	Ideal	Ideal
	LOC for a virtue	10% less than VDI VM	20% less than VDI VM	30% less than VDI VM

Performer Deliverables/Attendance Requirements

- Monthly technical report and telcon – highlight progress from past month and plans for next month.
- Monthly financial report – form will be provided
- Presentation detailing technical approach and research work plan for each performer for each phase due at kickoff and revised for site visit
- Phase kick-off meeting – first month of each phase
- Performer site visit – first quarter of each phase
- Mid-Term and Final Exams hosted at APL
- Phase 2 Proposers' Day (Phase 1 performers brief progress and techniques to potential phase 2 proposers – Approx. 1.5 month after midterm exams)
- Final Reports – submitted at the end of each phase
- Academic Publication & software public posting – by end of Phase 1

Notional/Target Schedule



Phase 1-2 Tentative Schedule

Proposers' Day:	July 19, 2016
BAA Release:	*Sept 11,2016*
Phase 1 Proposals Due:	*Nov 1, 2016*
Phase 1 Kickoff:	*Apr 1, 2017*
Phase 2 proposal Due	*May 15, 2018*

BAA & Review and Source Selection

Management Plan - Teaming

Depth and diversity will be essential to accomplish the many challenges in each phase

- Team Scalability and Optimization
  - ➢ Make sure you have enough people, with both academic and practical knowledge to accomplish the goals from proof-of-concept to performant prototype
  - ➢ Sufficient resources to follow critical path while still exploring new approaches.

Management Plan - Teaming

- Team Completeness – teams should acquire or develop all necessary components for success, e.g. should not rely upon future results/enabling technologies from the community at large
- Team Cohesion:
  - ➢ Clear, strong management; single point of contact
  - ➢ No pointless confederations; No teaming for teaming’s sake.
  - ➢ Each team member should contribute significantly to the program goals

Proposal Evaluation Criteria

•Evaluation criteria in descending order of importance are:

- Overall technical merit
- Relevance to IARPA mission and VirtUE program goals
- Effectiveness of proposed work plan
- Relevant experience and expertise of the members of the team
- Cost realism

•All responsive proposals will be evaluated by a board of qualified government reviewers.

Thanks

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

IARPA Overview

Dr. Stacey Dixon, IARPA Deputy Director

Office of the Director of National Intelligence

Central Intelligence Agency

Defense Intelligence Agency

Department of State

National Security Agency

Department of Energy

National Geospatial-Intelligence Agency

Department of the Treasury

National Reconnaissance Office

Drug Enforcement Administration

Army

Federal Bureau of Investigation

Navy

Department of Homeland Security

Air Force

Coast Guard

Marine Corps

IARPA Mission and Method

IARPA's mission is to invest in high-risk/high-payoff research to provide the U.S. with an overwhelming intelligence advantage

- **Bring the best minds to bear on our problems**
  - Full and open competition to the greatest possible extent
  - World-class, rotational Program Managers
- **Define and execute research programs that:**
  - Have goals that are clear, measureable, ambitious and credible
  - Employ independent and rigorous Test & Evaluation
  - Involve IC partners from start to finish
  - Run from three to five years
  - Publish peer-reviewed results and data, to the greatest possible extent

Analysis R&D

"Maximizing insight from the information we collect, in a timely fashion"

Large Data Volumes and Varieties

Providing powerful new sources of information from massive, noisy data that currently overwhelm analysts

Social, Cultural, and Linguistic Factors

Analyzing language and speech to produce insights into groups and organizations

Improving Analytic Processes

Dramatic enhancements to analytic process at the individual and group level

Collection R&D

"Dramatically improve the value of collected data"

Novel Access

Reach hard targets in denied areas

Asset Validation and Identity Intelligence

Assess trustworthiness and advance biometrics in real-world conditions

Tracking and Locating

Accurately locate emitters and other intelligence interests

Anticipatory Intelligence R&D

"Detecting and forecasting significant events"

S & T Intelligence

Detecting and forecasting the emergence of new technical capabilities

Indications & Warnings

Early warning of social and economic crises, disease outbreaks, insider threats, and cyber attacks

Strategic Forecasting

Probabilistic forecasts of major geopolitical trends and rare events

Operations R&D

"Operate effectively in a globally interdependent and networked environment"

Computational Power

Revolutionary advances in science and engineering to solve problems intractable with today's computers

Trustworthy Components

Gain the benefits of leading-edge hardware and software without compromising security

Safe and Secure Systems

Protecting systems against cyber threats

How to engage with IARPA

- **Website: www.IARPA.gov**
  - Reach out to us, especially the IARPA PMs. Contact information on the website.
  - Schedule a visit if you are in the DC area or invite us to visit you.

- **Opportunities to Engage**:
  - **Research Programs**
    - Multi-year research funding opportunities on specific topics
    - Proposers' Days are a great opportunity to learn what is coming, and to influence the program
  - “**Seedlings**”
    - Allow you to contact us with your research ideas at any time
    - Funding is typically 9-12 months; IARPA funds to see whether a research program is warranted
    - IARPA periodically updates the topics of interest
  - **Requests for Information (RFIs) and Workshops**
    - Often lead to new research programs, opportunities for you to provide input while IARPA is planning new programs

Concluding Thoughts

- **Our problems are complex and truly multidisciplinary**
- **Technical excellence & technical truth**
  - Scientific Method
  - Peer/independent review
  - Full and open competition
- **We are always looking for outstanding PMs**
- **How to find out more about IARPA**:

  www.IARPA.gov
- **Contact Information**

  Phone: 301-851-7500

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

Doing Business with IARPA

Ms. Katie Cole

INTELLIGENCE ADVANCED RESEARCH PROJECTS ACTIVITY (IARPA)

VirtUE Program Proposers’ Day Agenda

Time	Topic	Speaker
9:00 am – 9:30 am	Registration and Check In	
9:30 am – 9:45 am	IARPA Overview and Remarks	Dr. Stacey Dixon, Deputy Director IARPA
9:45 am – 10:45 am	VirtUE Program Overview	Kerry Long Program Manager
10:45am – 11:10 am	BAA Overview, T&E, GFI	Kerry Long Program Manager
11:10 am – 11:30 am	Break	
11:30 am – 12:00 pm	Doing Business with IARPA	Katie Cole IARPA Acquisition
12:00 pm – 12:30 pm	VirtUE Program Questions & Answers	Kerry Long Program Manager
12:30 pm – 1:30 pm	Lunch	
1:30 pm – 3:00 pm	Proposers' 5-minute Capability Presentations	Attendees (**No Government**)
3:00 pm – 5:00 pm	Proposers’ Networking and Teaming Discussions	Attendees (**No Government**)

Doing Business with IARPA - Recurring Questions

- Questions and Answers (**http://www.iarpa.gov/index.php/faqs**)
- Eligibility Info
- Intellectual Property
- Pre-Publication Review
- Preparing the Proposal (Broad Agency Announcement (BAA) Section 4)
  - Electronic Proposal Delivery (**https://iarpa-ideas.gov**)
- Organizational Conflicts of Interest (**http://www.iarpa.gov/index.php/working-with-iarpa/iarpas-approach-to-oci**)
- Streamlining the Award Process
  - Accounting system
  - Key Personnel
- IARPA Funds Applied Research
- RECOMMENDATION: Please read the entire BAA

Responding to Q&As

- Please read entire BAA before submitting questions
- Pay attention to Section 4 (Application & Submission Info)
- Read Frequently Asked Questions on the IARPA @

  http://www.iarpa.gov/index.php/faqs
- Send your questions as soon as possible
  - VIrtUE BAA: **dni-iarpa-baa-16-12@iarpa.gov**
  - Write questions as clearly as possible
  - Do NOT include proprietary information

Eligible Applicants

- Collaborative efforts/teaming strongly encouraged
  - Content, communications, networking, and team formation are the responsibility of Proposers
- Foreign organizations and/or individuals may participate
  - Must comply with Non-Disclosure Agreements, Security Regulations, Export Control Laws, etc., as appropriate, as identified in the BAA

Ineligible Organizations

Other Government Agencies, Federally Funded Research and Development Centers (FFRDCs), University Affiliated Research Centers (UARCs), and any organizations that have a special relationship with the Government, including 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.

Intellectual Property (IP)

- Unless otherwise requested, Government rights for data first produced under IARPA contracts will be UNLIMITED
- At a minimum, IARPA requires Government Purpose Rights (GPR) for data developed with mixed funding
- Exceptions to GPR
  - State in the proposal any restrictions on deliverables relating to existing materials (data, software, tools, etc.)
- If selected for negotiations, you must provide the terms relating to any restricted data or software, to the Contracting Officer

Pre-Publication Review

- Funded Applied Research efforts, IARPA encourages:
  - Publication for Peer Review of **UNCLASSIFIED** research

- Prior to public release of any work submitted for publication, the Performer will:
  - Provide copies to the IARPA PM and Contracting Officer Representative (COR/COTR)
  - Ensure shared understanding of applied research implications between IARPA and Performers
  - IARPA PM decides on approval for release or receiving courtesy copy

Preparing the Proposal

- Note restrictions in BAA Section 4 on proposal submissions
  - Interested Offerors must register electronically IAW instructions on: https://iarpa-ideas.gov
  - Interested Offerors are strongly encouraged to register in IDEAS at least 1 week prior to proposal “Due Date”
  - Offerors must ensure the version submitted to IDEAS is the “Final Version”
  - Classified proposals – Contact IARPA Chief of Security
- BAA format is established to answer most questions
- Check FBO for amendments & IARPA website for Q&As
- BAA Section 5 – Read Evaluation Criteria carefully
  - e.g. “The technical approach is credible and includes a clear assessment of primary risks and a means to address them”

Preparing the Proposal (BAA Sect 4)

- Read IARPA's Organizational Conflict of Interest (OCI) policy: **http://www.iarpa.gov/index.php/working-with-iarpa/iarpas-approach-to-oci**
- See also eligibility restrictions on use of Federally Funded Research and Development Centers, University Affiliated Research Centers, and other similar organizations that have a special relationship with the Government
  - Focus on possible OCIs of your institution as well as the personnel on your team
  - See Section 4: It specifies the non-Government (e.g., SETA, FFRDC, UARC, etc.) support we will be using. If you have a potential or *perceived* conflict, request a waiver as soon as possible

Organizational Conflict of Interest (OCI)

- 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 waiver request by e-mail to the mailbox address for this BAA at **dni-iarpa-baa-16-12@iarpa.gov**.
- 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.

Streamlining the Award Process

- Cost Proposal – we only need what we ask for in BAA
- Approved accounting system needed for Cost Reimbursable contracts
  - Must be able to accumulate costs on job-order basis
  - DCAA (or cognizant auditor) must approve system
  - See **http://www.dcaa.mil** , “Audit Process Overview - Information for Contractors” under the “Guidance” tab
- Statements of Work (format) may need to be revised
- Key Personnel
  - Expectations of time, note the Evaluation Criteria requiring relevant experience and expertise
- Following selection, Contracting Officer may request your review of subcontractor proposals

IARPA Funding

- IARPA funds Applied Research for the Intelligence Community (IC)
  - IARPA cannot waive the requirements of Export Administrative Regulation (EAR) or International Traffic in Arms Regulation (ITAR)
  - Not subject to DoD funding restrictions for R&D related to overhead rates
- IARPA is not DoD

Disclaimer

- This is Applied Research for the Intelligence Community
- Content of the Final BAA will be specific to this program
  - The Final BAA is being developed
  - Following issuance, look for Amendments and Q&As
  - There will likely be changes
- The information conveyed in this brief and discussion is for planning purposes and is subject to change prior to the release of the Final BAA.

Point of Contact

Kerry Long
Program Manager
IARPA, Office of the Director of National Intelligence
Intelligence Advanced Research Projects Activity
Washington, DC 20511

Phone: (301) 851-7512

Electronic mail: dni-iarpa-baa-16-12@iarpa.gov
(include IARPA-BAA-16-12 in the Subject Line)

Website: www.iarpa.gov

Questions? Please fill out cards.

VirtUE Program Proposers’ Day Agenda

Time	Topic	Speaker
9:00 am – 9:30 am	Registration and Check In	
9:30 am – 9:45 am	IARPA Overview and Remarks	Dr. Stacey Dixon, Deputy Director IARPA
9:45 am – 10:45 am	VirtUE Program Overview	Kerry Long Program Manager
10:45am – 11:10 am	BAA Overview, T&E, GFI	Kerry Long Program Manager
11:10 am – 11:30 am	Break	
11:30 am – 12:00 pm	Doing Business with IARPA	Katie Cole IARPA Acquisition
12:00 pm – 12:30 pm	VirtUE Program Questions & Answers	Kerry Long Program Manager
12:30 pm – 1:30 pm	Lunch	
1:30 pm – 3:00 pm	Proposers' 5-minute Capability Presentations	Attendees (**No Government**)
3:00 pm – 5:00 pm	Proposers’ Networking and Teaming Discussions	Attendees (**No Government**)