United States Army

ITES3-H Thin Client Whitepaper

ITES3-H Contract # W52P1J-16-D-0020

Due: 22 August 2016

DUNS No: 618563720

TIN: 52-1660341

CAGE: 0PF98

This whitepaper includes data that will not be disclosed outside the Government and will not be duplicated, used or disclosed – in whole or in part – for any purpose other than to evaluate this proposal or quotation. If, however, a contract is awarded to this offeror as a result of – or in connection with – the submission of this data, the Government will have the right to duplicate, use or disclose the data to the extent provided in the resulting contract. This restriction does not limit the Government's right to use information contained in this data if it obtained from another source without restriction. The data subject to the restriction is contained in all sheets of this whitepaper

Intelligent Decisions ITES3-H Technical Thin Client Whitepaper

Understanding and Technical Capabilities

Intelligent Decisions has extensive demonstrated expertise in architecting, engineering, deploying and maintaining large-scale VDI infrastructures for a range of U.S. government agency clients in the Intelligence, Department of Defense (DoD) and Civilian communities. ID has developed one of the largest non-persistent Virtual Desktop Infrastructure (VDI) environments in the Federal government; ID architected, engineered, deployed and maintains a 35,000 end point VDI environment for an Intelligence Community customer, across three enclaves: Sensitive but Unclassified (SBU), Secret and Top Secret. Geographically remote users experience more responsive desktop performance with the new VDI interface than they had prior with their desktop computers. ID brings to the US ARMY extensive VDI lessons learned and best practices, and directly relevant knowledge of virtual environment transformations for critical and geographically distributed missions. We understand the challenges associated with US ARMY's technology goals to further US ARMY's future business and collaboration methods. ID has a history of successful performance and advanced multi-vendor platform knowledge including a solid grasp of the following components: desktop, server, storage, network, database and security engineering and virtualization. Our Subject Matter Experts understand the phased transition to VDI in secure, global network enterprises. ID has proven experience and credentials building and sustaining Department of Justice (DOJ), the US Courts, DoD and Intelligence Community VDI infrastructures, engineering and ongoing management, and IT security services. Our objective in responding to this RFI is to demonstrate to US ARMY that ID is the industry leader in VDI projects in the Federal Government. We have engineered both on premise and cloud based solutions using various technologies and FedRAMP certified partners. Our engineers are certified in various desktop presentation and virtual hosting technologies and our implementations have enabled higher reliability with lower operational expenditures for our customers. US ARMY is asking for industry feedback in a well- thought-out and well-articulated RFI. While we cannot respond in detail to every requirement within the draft Statement of Work posed with the limited page count allotted, we certainly understand and know how to deliver on everything US ARMY has described. After review of our response, ID welcomes the opportunity to sit down with the US ARMY stakeholders and discuss in detail our VDI practice. The intention would be to expand upon the work we have done in this domain, and how that can be translated into meeting the needs of US ARMY's VDI initiatives.

ID does not believe a "canned" approach to VDI is appropriate for enterprise customers. There are many factors we take into account when designing and implementing a VDI solution to meet our customers' business, financial and technical requirements. For example, we consider: elements that are in the infrastructure, such as existing storage and virtualization approaches; location of users; mix of users (light user or heavy user) and application usage; security requirements; budget; as well as existing support personnel and processes in designing an optimal solution. ID's solution development process begins with a thorough requirements analysis of the existing infrastructure and business needs. Our approach to desktop virtualization begins with customer analysis, which includes a structured discussion with technical and business stakeholders to accurately characterize the existing environment and collect the complete set of goals and requirements for VDI. We then work with the customers to rank the goals and requirements. The information is then compared with the capabilities of the available VDI offerings based on an analysis of current capabilities and a review of the road map.

When an organization has significant investments in a specific OEM's storage, server, virtualization or network, ID's VDI team works with the customer to develop a VDI architecture that leverages those existing product investments and staff expertise. There is no "one size fits all" pricing model. The complexity of the organization's requirements, topology of their existing IT infrastructure and global network capabilities, the number and types of software applications to be virtualized and delivered to users' desktops, and the COOP/DR approach all drive solution complexity, implementation resource requirements and timelines, and ultimately costs and cost items associated with VDI solution architecture, engineering and deployment. ID believes that any cost estimate given the current parameters would not only be difficult but would also provide the US ARMY with unreliable pricing data. Based on our experience in providing similar solutions, ID recommends that the US ARMY take into the account the following factor when building a cost model.

This Whitepaper includes proprietary data that shall not be disclosed outside the Government.
This data is subject to the restriction included on the Title Page of this proposal.

VDI Cost Components	
▪ Assessment of the Current Environment ▪ Licensing (excluding Virtualization infrastructure and VDI) ▪ Data Capture/Discovery (e.g. apps, Qty, concurrency, method of licensing, app owners) ▪ Identification of a sample representative user group ▪ Collection of in use plugins (e.g. MS IE, MS Word, MS Outlook etc.) ▪ Documentation of Application dependencies (e.g. to other apps, access to data sources etc.) ▪ Application consolidation (too many apps serving the same purpose. Licensing + image complexity) ▪ Level of US documentation (Architecture only? SOPs?) ▪ Security/Patching/Updates (frequency, priority, etc.)	▪ Testing methodology (full prior to deployment or partial prior to deployment + frequent incremental during initial 6 months) ▪ Number of different configurations serving different user groups. ▪ Mobility Endpoint selection (Tablet, Laptop, Desktop, Thin Client, Smartphone) ▪ Definition of ownership of different elements (e.g. who owns the endpoints) ▪ Authentication Integration (PIV/CAC) Application Layer? OS Layer? SAML? ▪ Verification of Data Captured in Discovery (including a monitoring effort to stabilize data) ▪ Identification and prioritization of mission risk (e.g. failing to install an application used only during end of FY)

Corporate Experience

ID's extensive demonstrated experience in providing virtualized desktop infrastructure engineering, implementation, and operations support across the Federal Government is directly relevant to the requirements denoted by US ARMY within the draft Statement of Work. ID is currently implementing and sustaining large-scale VDI solutions for Federal customers. We have proven experience defining and implementing complex, heterogeneous, and distributed VDI environments.

Corporate Experience
Federal Client/Contract: Intelligence Community Customer **Installation Size:** 35,000+ endpoints **Installation Scope and Complexity:** Architecture, Engineering, Deployment and Operations of a VDI Environment—For the past six years, ID has supported the IT consolidation; IT hosting administration; and VDI architecture, engineering and deployment for this customer through an on premise virtualization environment that includes VMware hypervisor, Citrix Desktop Provisioning and various technologies for Virtual Application Provisioning, Our engineering team was responsible for the architecture and engineering of the solution and subsequently the operations of the environment. We designed, developed and implemented a VDI approach, creating a completely virtualized environment that supports approximately 35,000 thin and zero clients within a consolidated campus infrastructure. This environment supports users across three security classifications: Unclassified, Secret, and Top Secret. The infrastructure currently supports geographically remote users.
Federal Client/Contract: US Courts Administrative Office, Cloud and Technology Hosting Office (CTHO) **Installation Size:** 10,000+ **Installation Scope and Complexity:** ID is currently leading the effort to build a Desktop as a Service (DaaS) and Virtual Infrastructure as a Service (IaaS) environment for the US Courts. The US Courts has over 30,000 total users at ~800 locations throughout the US. Their goal is to provide a virtual desktop hosting environment for approximately 10,000 of those users in effort to provide greater functionality and telework capabilities and reduce overall operational expenditures. This centralized infrastructure is hosted at two US Courts Data Centers and provides dynamic provisioning of virtual hosted infrastructure and desktop environments for individual Federal Court offices. The solution stack is comprised of the VMware Suite for hypervisor virtualization, desktop and application provisioning as well as automated provisioning. The environment allows individual Court

This Whitepaper includes proprietary data that shall not be disclosed outside the Government.
This data is subject to the restriction included on the Title Page of this proposal.

administrators to maintain control of their endpoints while gaining economies of scale of larger, centralized environments.

Federal Client/Contract: DOJ - National Security Systems (NSS)
Installation Size: 1,500+ endpoints
Installation Scope and Complexity: Our team is the lead engineering staff responsible for the design and implementation of The Department of Justice JCON Secret and JCON Top Secret VDI environment. The production deployment comprises multiple data centers in an active/passive posture in order to offer a resilient and highly available computing environment. The Production VDI environment supports 1500 users across two security classifications. Our current support efforts include the ongoing design, implementation and operations of the Virtual Desktop Infrastructure that supports Thick, Thin and Zero client footprints across the environment. Additionally, we support the network infrastructure, underlying virtual hosting infrastructure, Active Directory Identity Management environment, SQL Database environment, security solutions and the endpoint vulnerability management solution, IBM Endpoint Manager. **Responsibilities:** We are currently providing the engineering and operations for the CSP IT infrastructure which includes 860 network devices, 80 servers per classification at each data center location (2), and 1500 endpoints across 500 locations on two security classification levels. We are responsible for standing up new sites on a DMVPN network, designing and implementing data center technologies with Cisco Nexus switches (7K, 5K, and 2K), and Cisco ASA firewalls while sustaining security integrity. These deployments have resulted in creating a dependable and redundant infrastructure, while integrating new CSP services to increase availability, reduce downtime and improve the overall security posture and functionality of the environment. We upgraded and expanded the CSP Virtual Hosting Environment. This environment, based on VMware vSphere 5.5, now hosts over 98% of the CSP Application Infrastructure. This include AD infrastructure, Mail infrastructure, File and Print Services, Specialized applications and a series of corollary servers needed to support the infrastructure (e.g. vCenter, NetApp Management, ACS, SQL Cluster, etc.). We have designed and implemented Solarwinds to monitor all of the network equipment for any issues. This installation included mapping out the entire network while configuring Solarwinds to monitor the desired diagnostics. This has resulted in a real-time dashboard view of the environment along with an automated alert notification system for any potential issues that may be occurring in the environment.

Federal Client/Contract: Department of Defense - – Joint Task Force Guantanamo – US Southern Command (SOUTHCOM)
Installation Size: ~2,000 endpoint across Unclassified and Secret Classification environments at 11 off-site locations and 1 Campus environment.
Installation Scope and Complexity: Intelligent Decisions created the second successful implementation of Air Force Research Labs (AFRL) SecureView MILS (Multiple Independent Levels of Security) within the Department of Defense at Joint Task Force, Guantanamo Bay, Cuba. Our staff worked closely with the scientists at AFRL, and engineers at Cisco Systems and Dell to leverage the existing NIPRNET campus backbone and the SIPRNET Virtual Desktop Infrastructure (VDI) to design and implement a highly secure, cost effective, and accredited NSA Commercial Solutions for Classified (CSfC) deployment. The solution leverages the Trusted Platform Module (TPM) on Intel Next Unit of Computing (NUC) small form factor workstations combined with AFRL SecureView / Citrix XenClient XT client virtualization and dual tunnel Cisco secure VPN's (ASR1000 routers & ASA 5516-X firewalls) to provide secure SIPRNET connectivity. Benefits of this program include removing classified data-at-rest (DAR) from all SecureView workstations as classified data is accessed through VMware Horizon 6 supporting infrastructure. Additionally, Joint Task Force leadership possess the ability to rapidly deploy SIPRNET connectivity to temporary or permanent enclaves by bypassing the security requirements related to expensive and time consuming cable security Protected Distribution System (PDS) while maintaining an extremely high level of security.

The Joint Task Force, Guantanamo Bay and Headquarters USSOUTHCOM has praised the success of this mission enhancing capability and has moved forward with similar plans to widely distribute this technology across the USSOUTHCOM AoR. Additional enhancements are scheduled to increase availability of SecureView services to the JTF-GTMO to include Citrix NetScaler load balancers and the replacement of the single ASA 5516-X firewall for dual ASA 5555-X firewalls with the goal of providing hardware and software fault tolerance of the VPN tunnels. Intelligent Decisions Systems Engineers are working closely with AFRL to seamlessly

This Whitepaper includes proprietary data that shall not be disclosed outside the Government.
This data is subject to the restriction included on the Title Page of this proposal.

integrate Cisco Systems Jabber client into future iterations of the SecureView platform due to heavy use within the Department of Defense.

Solution Overview and Architecture. ID does not believe a "canned" approach to VDI is appropriate for enterprise customers. There are many factors we take into account when designing and implementing a VDI solution that will meet our customers' business, financial and technical requirements. For example, we consider: elements that are in the infrastructure, such as SAN model; existing virtualization approaches; location of users; mix of users (light user or heavy user); security requirements; budget; and other factors in designing an optimal solution. ID's solution development process begins with a thorough requirements analysis of the existing infrastructure and business needs.

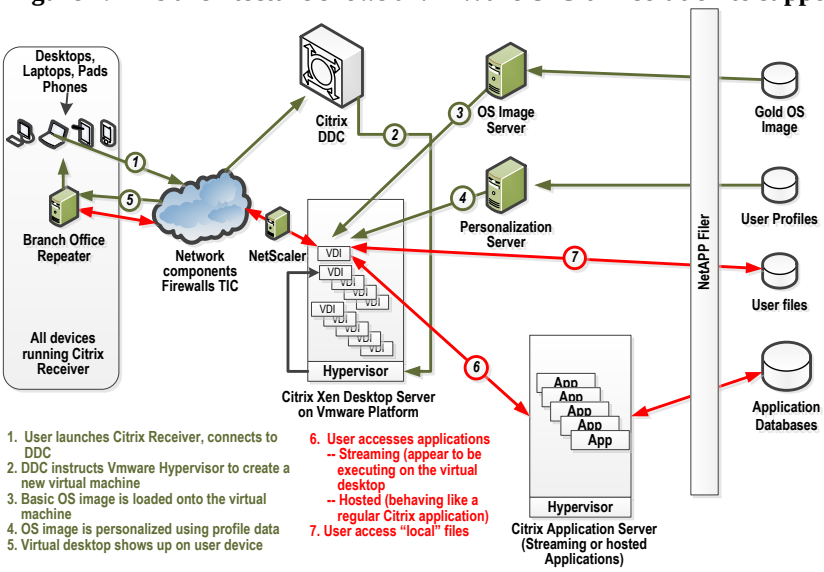
Overall Approach to Desktop Virtualization. Our approach to desktop virtualization begins with customer analysis, which includes a structured discussion with technical and business stakeholders to accurately characterize the existing environment and collect the complete set of goals and requirements for VDI. We then work with the customers to rank the goals and requirements. The information is then compared with the capabilities of the available VDI offerings based on an analysis of current capabilities and a review of the road map. For example, if disconnected VDI is important, we would eliminate the Microsoft VDI solution, as it does not support Type 1 or 2 hypervisors on end user computing devices. Then we rank the remaining candidates based on the criteria, providing pros and cons for each solution. Finally, we present the information to the customer for a final decision.

Logical and Physical Architecture. The major difference between individual VDI approaches is in the core solution. The remaining components are similar across VDI solutions. **Figure 1** shows a typical architecture for a VDI implementation, including:

- Endpoint devices – running either a client or a hypervisor Branch office accelerators, which perform catch
- Elements of network infrastructure such as WAN, LAN, access control, firewalls, DNS, DHCP
- Core VDI solution, including servers, hypervisors, operating systems, profiles, images, applications, management tools
- SAN infrastructure and file services

  Active Directory

Figure 1. This architecture shows a VMWare & Citrix solution to support BYOD.



- Branch office accelerators, which perform cache
- Elements of network infrastructure such as WAN, LAN, access control, firewalls, DNS, DHCP
- Core VDI solution, including servers, hypervisors, operating systems,

profiles, images, applications, management tools

- SAN infrastructure and file services
- Active Directory

Appliances typically combine the core VDI components in a pre-integrated package, and often include attached storage. They provide redundancy across appliances but are more difficult to configure for disaster recovery. They are often more challenging to integrate with rigid access control technologies. A hardware/software-based solution provides greater flexibility by supporting a heterogeneous set of users, and can take advantage of the existing infrastructure.

Technology Features to Address Availability. ID addresses fault tolerance and high availability primarily through:

- Multiple power supplies for all major network and server components
- Virtualized network solutions to avoid single path failures in connectivity
- Virtualized processing resources spread across multiple blades and chassis, eliminating a single point of failure
- Load balancers to distribute the load and transfer load from failed components
- Redundancy within the SAN
- N+1 design for VDI infrastructure servers.
- SQL Mirroring and/or AlwayOn to ensure database availability.

Other options include global site load balancing with transparent redirection; and a Pod design with multiple discrete VDI infrastructure instances. Our disaster recovery solution includes replication of data and processing power between data centers. When network or facility issues prevent access to one data center, the system will provide automatic fail-over, redirecting network traffic to the backup data center.

Level of Transparency. Several factors affect the level of transparency. Input/Output Per Second (IOPS), network bandwidth, allocated memory, client boot configuration and processing power affect the speed of boot-up and response times. Issues such as the VDI delivery model affect desktop personalization. For example, if local clients boot directly into a virtual desktop session and have a dedicated profile that retains settings and user-installed applications, then there should be no discernible difference between physical and VDI desktops. However, if a pooled desktop delivery model without roaming profiles or folder redirection is implemented, the users will have to change settings at each logon.

VDI Delivery. There is no single VDI delivery model that is appropriate for all users. ID determines an optimum mixed delivery model based on an analysis of user requirements, scalability, cost, and business issues. **Figure 3** lists some available delivery models based on each user's preferences with their computer.

Category of Use	Delivery Model
Individuals who use one or two business applications daily	Hosted Shared Desktop or Stand-alone Application Delivery
Users who focus on content creation using Microsoft Office and a select few additional programs. The users browse for content and graphics online.	Hosted Shared Desktop
Users with a core set of applications plus one or more specialized applications required to do their jobs, and need the ability to customize the desktop environment to increase efficiency.	Hosted Virtual Desktop (Dedicated)
Individuals who use applications that consume significant amounts of CPU resources when completing certain activities (video rendering or code compiling).	Hosted Virtual Desktop (Streamed to Blade)
Users who need to use applications that require admin-level privileges.	Hosted Virtual Desktop (Pooled)

This Whitepaper includes proprietary data that shall not be disclosed outside the Government.
This data is subject to the restriction included on the Title Page of this proposal.

Technical Design. ID approaches VDI design from a full life cycle perspective. We begin with a full requirements analysis that encompasses the current architecture, future architecture, business requirements, funding and supportability. We then evaluate the available VDI offerings and VDI models and design a solution that best addresses all the requirements. The scope of our design includes server and storage utilization, backup/recovery requirements, security compliance, host configurations, network bandwidth allocation, access controls, a deployment approach, management toolsets and ongoing management processes. This process was used to design VDI implementations ranging from 30,000+ clients within a consolidated campus infrastructure for an Intelligence customer to a solution that includes a mix of thick, thin and zero clients for 1,000 users on a classified network within the DOJ.

Customizing, Distributing and Managing Our Technical Design. ID's technical solution supports applications customization, virtual machine deployment and management. We support applications customization through vendor partner software customization solutions provided by Microsoft, VMware and Citrix. We create virtual machines using software management Graphical User Interfaces (GUI) provided by these vendors. Each VM has a unique file name, memory, networking and storage allocated to support the user environment (OS and applications). The VM management software provides start-up, peripherals, security, deployment, applications customization, performance monitoring and shutdown features. We define other requirements such as CPU clock cycles, memory allocations and I/O supporting each virtual machine. The storage requirements consist of defining disk allocations supporting virtual machines, disk management and recovery/backup configurations. The network requirements consist of defining virtual network interfaces, virtual local area networks (VLANs) and mapping to virtual machines.

For VMware environments, the compute servers host the ESXi hypervisor which enables platform virtualization without host OS. The ESXi hypervisor is initiated at system startup within the vmkernel (service console) that provides the hardware abstraction layer (HAL) that turns all physical CPUs, memory, network interfaces, storage interfaces, and other supported hardware into virtual resources available for provisioning. Guest OS (VMs) are launch by the service console. ESXi VMs are managed (provisioning, configuration and admin support) via vCenter management software.

During VM creation, peripheral devices are allocated based upon the US ARMY user profiles and security policies. Data sources are assigned to VMs during creation based upon customer policies (user pools, groups, etc.), and printers can be similarly assigned. There are unique vendor solutions that address printer management in a virtual environment. Hi-resolution video, multiple monitor or interactive applications require additional memory and processing during VM creation and can also be assigned to users or user pools based upon customer policy.

Managing User Rights, Files and Data Transfer. ID's solution implements user rights management policies though the creation of desktop images that support US ARMY security policies. The stateful desktop images consist of data in the operating system image that must be preserved, maintained, and backed up. These images are created with dedicated-assignment pools of linked-clone virtual machines or full virtual machines with persistent disks and folder redirection. Stateless desktop images are created with floating-assignment pools of linked clone virtual machines. Based on the US ARMY security policies, the technical solution can be customized to manage file and data transfers within local and remote user environments.

Hardware Deployment Options. ID's technical design solution supports multiple hardware deployment options based upon the US ARMY user environment. ID considers all hardware deployment listed options when designing a solution. Selection of a customer-specific solution is made after an analysis of workload, network performance, current IT architecture, number and size of remote locations, types of users and types of endpoint devices (laptops, desktops, IOS, Android, thin clients).

ID's typical VDI deployment includes the following components: Virtualization servers, Management servers, DMZ Security and Authentication servers, Virtualization software suite (Server based VM management and VDI endpoint client), storage systems, switched network and WAN optimization/load balancing solutions. When designing a solution, we consider the mix of users and the IOPS per type of user. Based on our experience, the IOPS

This Whitepaper includes proprietary data that shall not be disclosed outside the Government.
This data is subject to the restriction included on the Title Page of this proposal.

approximations for each type of user are as follows(we adjust these estimates based on our analysis of current and projected workload):

- No-load: 4 IOPS per concurrent user when the desktop is idle.
- Light user: 6 IOPS per concurrent user. This user works in a single application and is not browsing the web.
- Normal user: 10-15 IOPS per concurrent user. This user works in a few applications with minimal web browsing.
- Power user: 25-50 IOPS per concurrent user. This user runs multiple applications concurrently and spends considerable time browsing the web.
- Heavy user: 50-100 IOPS per concurrent user. This user does tasks with high I/O requirements like running AutoCAD, compiling code or working with images or video.

There should be a good management capability for storage; thus, a SAN solution is much better than NAS. The SAN is more flexible, easier to expand, and provides better COOP/DR capabilities. The local storage in a meshed appliance infrastructure provides good management capabilities and redundancy, but typically provides less COOP/DR capabilities.

Minimizing End User Impact. ID's technical solution minimizes end user impacts during migration by using enterprise virtual environment management products from vendors such as VMware which provision resources such as memory and monitors performance. Insufficient memory allocations can cause excessive swapping, which can generate I/O that causes significant performance degradations and increases storage I/O load.

Bandwidth Requirements. ID's analysis and design activities address bandwidth requirements for local and remote user environments, including connectivity to internal and cloud-based datastores. We consider bandwidth requirements for display protocols, monitor resolutions and multimedia content, and issues that can cause bandwidth spikes, such as concurrent launches of streamed video multimedia applications. For networks using RDP protocol, a WAN accelerator is required. RDP requires handshakes between client and server, which introduces latency. WAN accelerators hide handshake replies to improve performance. For networks using PCoIP protocol, WAN optimization techniques are built into the base protocol. If using PCoIP protocol within 100Mb or a 1Gb switched network, user environments supporting multiple monitors, flash embedded web browsing, multimedia apps, network printing or USB-based peripherals would not be impacted.

Integrating Solutions. ID's technical design integrates solutions within standard interfaces supported by vendor solutions. The technical solution supports the US ARMY authentication and authorization requirements by integrating with third party solutions such as Cisco ASA, Citrix Access Gateway, Juniper SSL VPN, Microsoft Unified Access Gateway (UAG), VMware View Security Server, McAfee Endpoint Protection Antivirus Protection, Microsoft Active Directory Network Directory System HSPD-12 PIV Smartcards Common identification standard and PING SAML SSO MS Licenses. ID's security management approach consists of performing preventive tasks such as security patch installation, backups and testing data restoration.

Ability to Work Offline. ID's technical design supports both VDI server-hosted and client-based solutions to address offline work requirements. The server-hosted VDI instances consist of applications executed remotely and presented at the endpoint via a remote display protocol such as Microsoft RDP, Citrix ICA/HDX, Teradici/VMware PC-over-IP, etc. The client-hosted VDI instances consist of the applications executed at the endpoint. For users who need to work offline, there are two basic options, with multiple permutations. Both options allow a desktop to stream to a laptop, run without network connectivity, and automatically synchronize when reconnected.

Mitigating VDI Unique Problems. When using non-persistent desktop solutions, non-redirected data is lost at device shutdown / restart. The ID solution identifies information (event logs, data files, etc.) and redirects the data to an external location or configures a local persistent disk to accommodate this data. When using a single image for multiple desktops, user identity issues may occur which result in an application writing a GUID to the registry and multiple instances of the application (of different virtual desktops) subsequently attempting to use this same GUID for licensing or registration purposes. ID has experience customizing non-persistent images via registry edits and/or startup scripts to address this problem.

This Whitepaper includes proprietary data that shall not be disclosed outside the Government.
This data is subject to the restriction included on the Title Page of this proposal.

Concurrent booting across the network and the use of host-based agents designed for stand-alone PCs such as AV products, constitute some of the unique VDI problems that ID considers in VDI design. Alternatives we consider to address boot storms include: cache boot files on SSD in the SAN; the practice of pre-starting desktops in waves each morning; and branch office caching solutions. The best solution to mitigate AV storms is to select and configure an appropriate AV solution that most effectively addresses the problem in each customer's environment, and that minimizes the cost and administrative burden. AV storms are being addressed by all the major AV vendors, who are modifying their products to be VDI-aware. In addition, several integrated VDI management tools such as the VMware® vCenter™ Operations Management Suite™, Microsoft SCCM and tools from BMC, AppSight, SysTrack and Tivoli can address these issues.

Addressing Local Administrative or Power User Privileges. The same non-persistent virtual desktop can be used to support both administrative and non-administrative users. UAC can be used to control access to locally installed applications, and a separate application delivery infrastructure can be used to provide additional administrative applications to only those users who require access. ID's technical solution addresses local administrative and power user privileges by implementing a structured virtual desktop creation, using deployment and management methodology that supports US ARMY local and remote user environments. There are many options, and the selection of the best one is predicated on an analysis of the user requirements. Some alternatives are:

- For disconnected VDI, one solution is to put the NT AUTHORITY\INTERACTIVE user into the local administrator or power user group. Anyone logging in interactively will have administrative rights.
- For a central VDI solution, create a hosted virtual desktop for all administrative users and include them in the Administrators group

Integration and Interoperability with Existing Servers. ID's technical solution integrates with existing servers within standard interfaces supported by vendor virtualization solutions such as VMware, Citrix, etc. The VMware virtualization software suite consists of server (vCenter/vSphere) and desktop (View) software with the following components: View Composer, View Connection Server, View Replica, View Security Server, View Transfer Server, vShield Manager, Database Server, Active Directory, DNS, DHCP, associated databases, and Windows Desktop Operating Systems. VMware View provisions and manages new virtual desktops from a centralized tool into single instances or in groups, supports "On-Demand" or pooled virtual desktop provisioning, provides access through identity or Active Directory authentication, sets up and configures virtual desktop policies and procedures from centralized tool and provides shared templates to provision virtual desktops. The VMware View suite includes application virtualization (ThinApp) and user profile management (Persona).

Supporting Firewalls, VPNs, and Load Balancers. ID's solution supports firewalls, VPNs and load balancing within a standard interface supported by such vendor solutions as Cisco, F5, Aruba etc. DMZ-based security servers require firewall rules on the front-end and back-end firewalls to allow external client devices to connect to a security server within the DMZ. The front-end firewall allows traffic on certain TCP and UDP ports to facilitate communication with each server instance that resides within the internal network. The back-end firewall must allow inbound traffic on certain TCP ports to enable desktops to communicate with each other. The network infrastructure configuration requires WAN optimization to support throughput requirements. The DMZ server hosts Local Traffic Management (LTM), VPN, and Access Policy Management (APM) functions. The F5 LTM BIG-IP platform Virtual Engine (VE) provides load balancing, health monitoring, and SSL offload. Network and protocol optimizations manage bandwidth efficiently while maintaining and improving the user experience. BIG-IP LTM uses hardware to offload SSL encryption from data center servers. By accelerating encryption and freeing up server resources, BIG-IP LTM improves application performance. F5 BIG-IP Application Delivery Controllers offer SSL offloading, providing relief from the processing burden of encrypting and decrypting traffic sent via SSL.

COOP Support. ID's solution supports COOP sites within a structured virtual desktop management methodology that is compatible with US ARMY operational and COOP production environments. The candidate approaches for virtual environments are an Active/Active (automated) or Active/Passive (manual) environment. The active/active approach provides real-time production and backup environment via load-balancing solutions. The active/passive approach provides a primary site environment with real-time updates and customer-defined data backup at remote site. The

This Whitepaper includes proprietary data that shall not be disclosed outside the Government.
This data is subject to the restriction included on the Title Page of this proposal.

technical solution integrates a vendor solution that addresses the US ARMY requirement. A candidate active-active approach would provide the following features: automated Active Directory (AD) Schema, Global Catalog, and DNS replication leveraging Windows 2008 R2 Active Directory Domain Services (AD DS); automated user file, virtual transfer server repository, application virtualization repositories, and network profile replication leveraging Distributed File System (DFS) replication and single global namespace publishing; automated profile management replication leveraging replication; automated composition of virtual server environment and Server Load Balancing (SLB)/Global Server Load Balancing (GSLB) for DNS redirection for users to be pointed to the first available environment in the event of an individual site failure. In the event of a site failure, replication of AD DS and Microsoft's Distributed File System Replication (DFS-R) will begin automatically. Once replication is complete, SLB/GSLB services will begin to support requests from users; system will load balance and re-provision virtual services.

Specialized Hardware Requirements. ID's solution supports specialized hardware requirements which may be required based upon US ARMY networking environment. We need more information concerning the US ARMY networks to confirm what type of specialized network hardware is required to support the US ARMY remote users. For example, if the network architecture includes VLANs, an external router may be needed to provide InterVLAN Routing and ISL/802.1Q Trunking. We have vendor partners such as Cisco who have solutions that can meet the specialized networking requirements.

Deployment and Installation. We leverage an industry-proven commercial-off-the-shelf (COTS) integration project lifecycle model derived from the Software Engineering Institutes methodology, called the Evolutionary Process for Integrating COTS-based systems (EPIC). We have tailored the methodology to address the typical requirements of a VDI implementation within a client environment. This ID-tailored approach encompasses a maximization of legacy (systems and processes) reuse and an iterative development and fielding plan that manages risk and improves stakeholder ownership and satisfaction. EPIC is a framework designed to effectively assess and leverage the entire set of capabilities available through components of the current enterprise environment and then access and integrate new technologies, applications, and tools available on the commercial market to cover the gap in the solution's required capabilities. ID is confident that the resulting outcome will have greater operational success. This approach forces stakeholder involvement, fosters championed change management activities, and drives stakeholder buy-in. It also drives program evolution by continuously testing and exploiting the capabilities of VDI and its components to rapidly meet operational demands. Our approach provides a unified protocol that encompasses full lifecycle deployment and installation (design, build, field, support, and continues improvement) of the VDI capability. This method also leverages legacy systems, processes, and capabilities to their fullest extent to maximize reuse and minimize costs. In addition,

Common Project and/or Technical Challenges. Common challenges include maintaining network bandwidth, managing user profiles, and virtualizing applications for use by multiple vendors.

- **Network Bandwidth.** VDI solutions require appropriate network resource allocations to support user (admin, normal, power and mobile) environments. As the number of users and number of different user profiles increases, the network traffic between users and data stores increases, which can potentially negatively impact the user experience.
- **User Profile Management.** User profile management has three major considerations that impact implementation. Firstly, user profile and data migration solutions are provided by multiple vendors which could adversely impact VDI performance due to the method for managing user data such as email retention policies. If the legacy environment does not have an enterprise data management plan, the data migration process may negatively impact network bandwidth and storage allocations. In addition, profile management of a large number of Windows user environments requires multiple desktop images, which increases the complexity of VDI management. Finally, peripheral devices such as printers in a virtual environment require additional management software based upon the customer security policies.

This Whitepaper includes proprietary data that shall not be disclosed outside the Government.
This data is subject to the restriction included on the Title Page of this proposal.

- **Applications virtualization.** Application virtualization solutions are provided by multiple vendors. Some legacy applications cannot be fully virtualized, which may produce longer access timelines for users in a virtual environment.

FTE Support. The number of staff involved in a VDI installation will vary depending on a number of factors, including: existing architecture US documentation, customer requirements, existing infrastructure, number of users/locations/profiles, COOP/DR requirements and required completion schedule. The number of staff will also vary over time. For example, typically two senior engineers are involved up front for the requirements analysis and design. During implementation, this figure may rise to 5-6 individuals per VDI implementation site depending on number of sites where VDI instances are being installed, number of profiles and images to be created, complexity of the design, COOP/DR requirements and schedule. As the deployment continues and issues are resolved, deployment staff will be reduced accordingly.

The typical labor categories assigned during a VDI implementation may include: Project Manager Senior, VDI Principal Architect, Virtualization Engineer Senior, Network Engineer Principal, IA Engineer Senior, Systems Engineer Senior, Network Engineer Senior, Systems Engineer Intermediate, Network Engineer Intermediate and Systems Engineer Junior. Some of these individuals will not be physically present at the customer location but will provide SME support to the on-site staff.

Method for Updating Software and Testing Products. ID's Change Management processes ensure that the project team has the tools to make effective decisions regarding implementation of approved changes and the impact of changes on cost, schedule, and system performance. In general, we will identify, define and quantify the impact of change against an approved baseline and develop an assessment. Once that assessment has been completed we will follow a formal change process to implement the change. The formal change process will dictate how change can occur and how it will be verified and validated. The customer-specific VDI solution technology selected and Customer environment will determine the tools that will be used for updates, testing, patch management, and troubleshooting.

On-site Support. During sustainment, the ID project engineer is typically off-site but will remain a resource to the US ARMY effort with ongoing daily and weekly responsibility for task management. The project engineer will work with the applicable Tier 2/3 help desk support personnel. Tier 2 support will manage and resolve Tier 1 escalations and maintenance of the FAQ/common know errors knowledge bases. Tier 3 will provide required patch management, advanced technical support, Tier 2 escalations, and facilitate vendor interactions.

Systems Management. The ID solution provides enterprise system management across the entire lifecycle of the virtual IT environment by incorporating software management solutions from vendors such as VMware, Citrix and Microsoft and third party vendors. Once deployed, the VDI support team will need to continually ensure application delivery, maintain images and user profiles, and optimize storage while providing a seamless user experience.

Installing, Configuring, and Deploying New Desktop Images. The ID enterprise system management process consists of installation, configuration and deployment of virtual desktop images.

Step	Tasks
Configuration	Setup separate development and operational IT environments (storage, networking and user environment (access control, applications and profiles))
	Set up security procedures (trusted boundaries) for both environments
	Establish management toolsets for both environments – Configuration management
	Review user profiles (Windows 7, Windows NT, etc.) for migration to virtual environment
	Review user applications and database for migration to virtual environment
	Establish data management policy (storage performance, data retention, disaster recovery/COOP, etc.)

This Whitepaper includes proprietary data that shall not be disclosed outside the Government.
This data is subject to the restriction included on the Title Page of this proposal.

	Define networking infrastructure for local and remote users
Installation and Deployment	Create standard desktop image (desktop GUI, applications, user profiles, security and endpoints (desktops, mobile devices, etc.) – timelines varies based upon customer environment)
	Set up networking procedures (VM bandwidth allocations based upon user types, networking routing and WAN connectivity) – timelines varies based on customer organization policies)
	Provision virtual machines (VMs) (compute processing, memory and storage) – timeline varies based upon vendor solutions – VMware, Citrix, Microsoft, etc.
	Deploy VMs to user endpoints in development environment with transition to operational environment – timelines varies based on customer regression testing requirements
	Manage VMs (startup, shutdown, system monitoring, troubleshooting, etc.) – problem resolution timelines based upon customer requirements

Management User Interface. The abovementioned vendor, VMware provides the software solutions that we incorporate into our VDI management user interface approach. The VMware® vCenter™ Operations Management Suite™ consists of VDI management software that provides system visibility, automated operations and SLA management using data analytics and an integrated approach to provide performance, capacity and configuration management for virtual IT environments. The management solution provides a holistic view into the status of the virtual and hybrid cloud infrastructure and applications. In addition, it provides several important supports, including data analytics to automate performance, capacity and configuration management supporting resource utilization; real-time performance dashboards that support SLAs and systems alerts; and capacity management to optimize resource usage and policy-based configuration management to assure compliance and to eliminate sprawl and configuration issues.

End User Support. As described in the subsection above, the VMware® vCenter™ Operations Management Suite™ provides data analytics to automate performance, capacity and configuration management. These data analytics provide discovery and visualization awareness of the virtual infrastructure supporting customer-defined service levels and disaster-recovery. The solution provides standard interface to third party applications that develop audit reports and custom reports addressing system performance and capacity planning efforts.

Integrating Alert Technology. We leverage existing monitoring and ticketing tools to ensure the least amount of change in incident and problem management processes. The simplest method is to enable SNMP monitoring of VDI components using existing monitoring tools that are integrated with the ticketing system. Other tools, from the VDI vendors or from third party companies such as Solar Winds, can also be incorporated into the solution.

Integrating External Ticketing Systems. If customers have already integrated their infrastructure monitoring tool with their ticketing system, we recommend taking advantage of that, as described in the prior section. Another method is to use a tool such as VMware vCenter Orchestrator BMC Remedy ITSM Plug-in.

Training. ID's VDI implementation approach addresses the entire life cycle of the system. A robust training plan for system administrators and other personnel is an essential element in a successful transition from deployment to ongoing support. The training plan addresses foundational training, solution-specific knowledge transfer, and upgrade training.

Method for Knowledge Transfer. The optimal approach for US ARMY staff training includes the following components:

- Attend training sessions on the base solution.
- Conducting a 1-2 hour orientation for the engineers on the US ARMY-specific configurations (what actions were taken, and why). We will conduct this training at several stages during implementation.

This Whitepaper includes proprietary data that shall not be disclosed outside the Government.
This data is subject to the restriction included on the Title Page of this proposal.

- Conduct a summary class when installation is complete with Q&A and hands-on technique for ongoing support and troubleshooting that builds on prior knowledge transfer
- Create a series of articles for ongoing administration and troubleshooting knowledge US ARMY staff can reference and incorporate into Tier 1 and 2 support processes

Examples of ID's Installation Training. Our staff evaluates the skills of the current system administrators and provides recommendations to customers on which vendor courses the system administrators should take. We provide orientation training sessions at critical points during the installation. In addition, ID provides several weeks of on-the-job training until the system administrators are self-sufficient.

Process for Resolving Product Issues. ID recommends an on-site presence, to remain in place for at least one year following completion of the rollout to provide Tier 3 support and problem resolution. As necessary, ID's Tier 3 support will interface with all product vendors using proven problem management processes that include root cause analysis. We have formal vendor relationships with all major VDI vendors and have access to their senior engineers. At the end of the period, incumbent staff should have sufficient knowledge to provide support, in conjunction with standard VDI maintenance and support agreements.

New Release and Application Training. Training on new releases and applications is performed in a two-stage process. During the first stage, ID engineers gain knowledge of the new releases through one or more methods, including: attendance at formal training classes; participation in vendor webinars provided to our product sales and on-site engineers; and experience in trying the new products in our test lab. In the second stage, our engineers perform a gap analysis of the skills of the current system administrators, identify the type and level of training needed, and provide recommendations on training that ranges from a "what's new" session delivered by an on-site ID engineer to formal classroom courses.

Compliance and Security. Our implementation approach aligns with the NIST Risk Management Framework outlined in NIST SP 800-37 Revision 1 and provides a mechanism for our clients to implement an efficient and effective program for managing risk in accordance with NIST 800-series guidance and CNSSI 1253 while reducing operational cost.

Complying with Federal Regulations. Our risk management plan focuses on the maintenance of security throughout each phase of VDI implementation up to sustainment in order to ascertain that security is incorporated early in the process, reduce the overall cost of security and effectively mitigate risk to the mission allowing US ARMY executives to make risk based decisions regarding system authorizations.

Below we list the activities and deliverables that we will provide for this task. ID continually monitors the security controls within the US ARMY systems via assessing control effectiveness, US documenting changes to the system or its environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to designated US ARMY executives.

Framework Step	Approach and Deliverables
Step 1 – Categorize Information Systems	▪ Annual review and validation of Security Categorization, System Description and Technical Description ▪ Review and update any Memorandums of Understanding/Agreement and Interconnection Security Agreements ▪ Review and update the Privacy Impact Analysis, System of Record Notice, and e-Authentication Risk Assessment
Step 2 – Select Security Controls	▪ Review and support the update the Requirements Traceability Matrix with tailored controls

This Whitepaper includes proprietary data that shall not be disclosed outside the Government.
This data is subject to the restriction included on the Title Page of this proposal.

Framework Step	Approach and Deliverables
	▪ Support the annual review and update of the System Security Plans ▪ Apply FIPS 140-2 standards as applicable
Step 3 – Implement Security Controls	▪ System Security Plan, Incident Response Plan, Contingency Plan, and Configuration Management Plan
Step 4 – Assess Security Controls	▪ Tailored Security Assessment Plan ▪ Security Assessment Report ▪ Updated System Security Plan and Updated Security Assessment Report based on remediation
Step 5 – Authorize Information System	▪ Plan of Action & Milestones Report ▪ Security Authorization Package ▪ Signed Security Authorization Memo ▪ Vulnerability and Risk Assessment Reports
Step 6 – Monitor Security Controls	▪ Security Impact Analysis and Change Control Board Meeting Minutes ▪ Ongoing Security Assessments, Independent Verification and Validation, and Remediation ▪ Updates to SSP, SAR, CP, IRP, CMP, Residual Risk Report, MOU/As, ISAs, Privacy US documentation, Security Authorization package ▪ Monthly FISMA compliance reporting to US ARMY key stakeholders ▪ Quarterly and annual compliance reporting

Intelligent Decisions Recommended VDI Design and Solution

For the purposes of this whitepaper and the US ARMY requirement, ID has designed two different size VDI deployments: 1 deployment for Under 500 users and another deployment for 2500 users. We have also designed optional add-ons to our two VDI designs a CSfC (Commercial Solution for Classified) Mobile Access (MA) Capability Package (CP) cross-domain solution leveraging AFRL's SecureView. As a member of the SecureView Certified Integrator Program, ID partners with AFRL and Assured Information Security (AIS) to provide this cross domain solution as a huge infrastructure saving option for the US ARMY. We have also provided a separate whitepaper in addition to this one that provides a detailed explanation of the SecureView solution, its cost-savings and value, as well as its high level architecture. Below is a brief summary of the SecureView Solution and the CSfC Mobile Access Capability Package.

SecureView is a MILS cross domain solution that ensures endpoint security by leveraging workstations that have the Intel vPro Trusted Platform Module (TPM) and allows users to traverse from the low side of a network to the high side leveraging a virtualized infrastructure within one physical machine. As a hardened client-hosted virtualization (CHV) solution, SecureView enables independent, concurrent access to multiple domains. It provides performance that is independent of network bandwidth and server contention issues, providing analysts with consistent responsiveness for visually intensive analysis and collaboration. SecureView is NIST 800-53 certified as High in both Confidentiality and Integrity, and Medium in availability. SecureView was built from its inception to provide unparalleled security, agility, and performance for IC and DoD workstations while **ALSO** minimizing the total cost of ownership. SecureView is a Government Program which keeps the DoD and IC from getting locked into a proprietary or single-vendor solution that would limit their flexibility and scalability, and drastically increase lifecycle costs for ongoing support, training, and software patches or upgrades.

This Whitepaper includes proprietary data that shall not be disclosed outside the Government.
This data is subject to the restriction included on the Title Page of this proposal.

Security

- Built on Type 1 bare-metal hypervisor architecture
- Ensures 100% Trusted Boot and Secure Isolation in the hardware
- Received highest MILS evaluation to date against NIST 800-53 criteria
- Integrates NSA's new Commercial Solutions for Classified (CSfC)

Capability

- '**NIPR + SIPR**' or '**SIPR** + **JWICS**' on a single PC, laptop, or tablet
- Intuitive user interface that requires minimal training for end users
- Seamlessly supports high performance and high-bandwidth applications
- Supports Secure Mobility and Unified Communications requirements

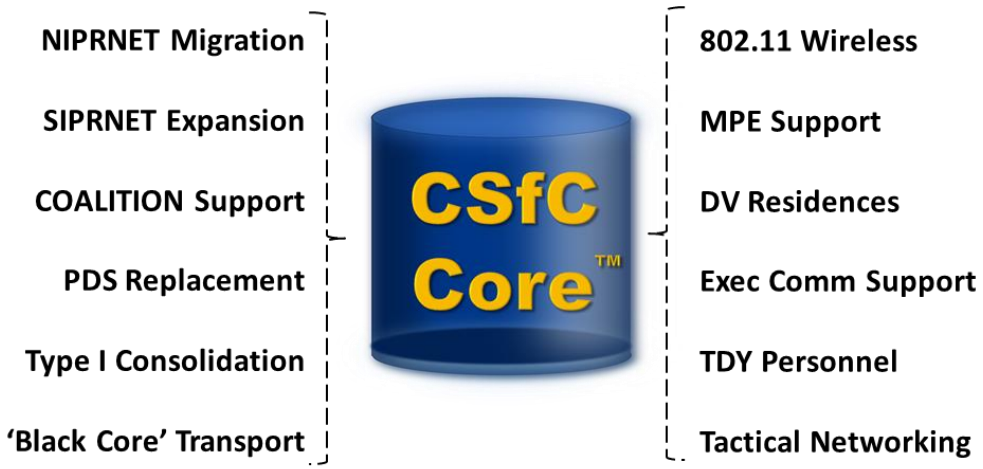
Flexibility

- Supports **BOTH** 'Thick' OS and 'Thin' VDI clients simultaneously
- Enables rapid provisioning and re-configuration of workstations
- Based on Xen which meets DoD's new open-source requirements
- Supported by multiple PC, laptop, and tablet manufacturers

NSA's new Commercial Solutions for Classified (CSfC) program provides US government agencies with unprecedented capabilities to deploy and secure classified networks. Rather than requiring the development of any GOTS or proprietary hardware, CSfC is centered around the integration of NSA's Suite B cryptographic algorithms into COTS IT equipment (VPN concentrators, WLAN controllers, VPN/WLAN clients, etc.). The CSfC program is supported by several Fortune 500 COTS vendors such as Cisco, Juniper, and Aruba. Since its establishment in 2010, the number of products and vendors working with NSA on the CSfC program has continued to grow.

NSA's CSfC program office has established several 'Capability Packages' to provide DoD and Government agencies specific technical architectures and well-documented approaches for leveraging CSfC capabilities. By leveraging the CSfC solutions, the DoD and Government agencies can leverage Suite-B enabled VPN capability to securely tunnel classified networks over their existing NIPRNET or black infrastructure. NSA continues to update their existing CSfC Capability packages and is also establishing new ones to enable even greater functionality, such as the Data-at-Rest and Mobile Access. SecureView is an AFRL-developed and managed software solution that enables a single PC, laptop, or tablet to access multiple independent levels of security. With the revolutionary capabilities enabled by NSA's CSfC program, CSfC functionality and compatibility is integrated directly into the SecureView architecture. By leveraging the CSfC Mobile Access and Data-at-Rest capability, SecureView has become a tremendous solution for DoD and Government agencies to securely access classified networks on-base or while deployed using their unclassified infrastructure—eliminating the need for costly PDS or Type I encryptors.

This Whitepaper includes proprietary data that shall not be disclosed outside the Government.
This data is subject to the restriction included on the Title Page of this proposal.



In addition to the in-garrison use, SecureView + CSfC enables Special Operations Forces (SOF) the ability to streamline tactical networking requirements—providing access to multiple US unclassified/classified networks, as well as Mission Partner Environments, on a single ruggedized laptop or tablet. Using the new CSfC Mobile Access and Data-at-Rest capabilities, the ruggedized laptop or tablet could connect to the unclassified and classified networks over a single black wireline or wireless connection, and become completely unclassified when fully powered off after use. Rather than requiring SOF operators to turn off.

NSA's new Commercial Solutions for Classified (CSfC) program provides US government agencies with unprecedented capabilities to deploy and secure classified networks. Rather than requiring the development of any Type I or proprietary hardware, CSfC is centered around the integration of NSA's Suite B cryptographic algorithms into commercial of the shelf (COTS) equipment (Virtual Private Network gateways, Wireless controllers, etc). By leveraging the CSfC solutions, Government agencies can leverage Virtual Private Network (VPN) capability to securely tunnel classified network traffic over ANY black or unclassified network – including a black wireless Local Area Network. SecureView is a DoD and IC accredited solution for accessing multiple independent levels of security on a single device, such as a workstation, laptop, or even a tablet. SecureView integrated support for NSA's CSfC VPN transport and Data-at-Rest solutions into the software architecture in 2014. So a SecureView laptop or tablet can provide personnel access to Unclassified and SECRET networks, or SECRET and TOP SECRET networks over a single black connection—including over an unclassified wireless local area network using CSfC-approved COTS wireless controllers and access points without any additional Type I encryptors, proprietary equipment, or tethered devices.

This Whitepaper includes proprietary data that shall not be disclosed outside the Government.
This data is subject to the restriction included on the Title Page of this proposal.

ID's Under 500 seat VDI Solution: Bill of Materials (BOM):

Primary Component	Description	Quantity
Server Compute Infrastructure	**Chassis:** Dell PowerEdge FX2 with 4 Half Width Nodes **Integrated I/O Module**: PowerEdge FX2 Dual 10Gbe SFP+Pass through Module **Power Supply:** FX2 Power Supply. Redudant Alerting. 2X2000X @ 200-240V **Licenses:** Win Server 2012R2 - 2 Socket or 2 VM **Blades (Qty3):** FC630 Servers **Processor**: Dual Intel Xeon E5-2683 v4 2.1Ghz, 40M Cache, 9.60 GT/s **Trusted Platform Module:** TPM 2.0 FIPs, Common Criteria **Memory:** 32GB RDIMM, 2400 MT/s, Dual Rank **RAID:** Diskless Configuration, PERC Controller, H330 Controller **Network Daughter Card:** QLogic 57810-K Dual Port 10Gb Blade Card **Virualization HyperVisor:** VMWare ESXI 6.0 **Virtualization Desktop Software:** Vsphere Desktop 100VM Pack (Qty 5)	1
SecureView Management Server	**Chassis:** Dell PowerEdge R220 **Processor**:Intel Xeon G3430 3.3Ghz, 3M Cache **Memory:** 8GB UDIMM **RAID:** RAID 1, H310 2 HDD **Hard Drive:** 500GB 7.2K RPM SATA	1
SecureView Software	SecureView Management Server (Any Workstation Count) Reoccurring Annually	1
	SecureView Workstation - Single Workstation - Reoccurring Annually	499
End Points	Dell Optiplex 9020 SFF Processor: Intel i5-4570 Memory: 16GB (2 x 8GB) NIC: Intel I217LM	499
	Dell E2216H 22 inch Monitor (optional)	499
	NIPR CAC Reader (Identive SCR3310/v2 Smart Card Reader)	499
	SIPR CAC Reader (HID OMNIKEY 3121 USB Card Reader)	499
	VIASAT Eclypt Core Encrypted Internal Hard Drive minimum 256GB	499
	Intel SSD Pro 1500 series (360GB | M.2 Form Factor and 2.5in Form Factor)	499
Storage Infastructure	Dell Compellent SC4020 10GB 4 Ports Single Drives	1
	Dell 1.92TB SAS 12gb SSD	6
	Dell 1 TB SAS 6GB 2.5" 7.2K HHD	12
	Dell 200GB SAS 6GB 2.5" SSD	6
	IO, 10gb iSCSI, 4x SFP+ Optical Adaptor	1
	Software: Dell Storage Center OS Core Base License	1
	Software: Storage Optimization Bundle - Base License	1
Cisco ASA Hardware	ASA 5555-X with SW, 8GE Data, 1GE Mgmt, AC, 3DES/AES	3
	ASA 9.2.2 Software image for ASA 5500-X Series,5585-X,ASA-SM	3
	ASA 5545-X/5555-X AC Power Supply	3
	AC Power Cord (North America), C13, NEMA 5-15P, 2.1m	3
	ASA 5545-X/5555-X Interface Card Blank Slot Cover	3
	ASA 5512-X -- 5555-X Hard Drive Blank Slot Cover	3
	ASA 5500 Strong Encryption License (3DES/AES)	3
	^ASA 5555 IPS Part Number with which PCB Serial is associated	3
	ASA 5545-X/5555-X AC Power Supply	3
Cisco ASA Licensing	Cisco AnyConnect 1-Yr 250 User Apex License	2
	Cisco AnyConnect 1-Yr 250 User Apex Subscription	2
	Cisco AnyConnect 1-Yr 250 User Apex (ASA License Key)	2
Aruba Cloud Services Controller	Aruba 7010, 12x10/100/1000BASE-T PoE/PoE+ (150W), 4x10/100/1000BASE-T, 2x1G	1
	Policy Enforcement Firewall for Aruba 7005 (VIA/VPN users)	1
	Advanced Cryptography (256 Sessions)	2

This Whitepaper includes proprietary data that shall not be disclosed outside the Government.
This data is subject to the restriction included on the Title Page of this proposal.

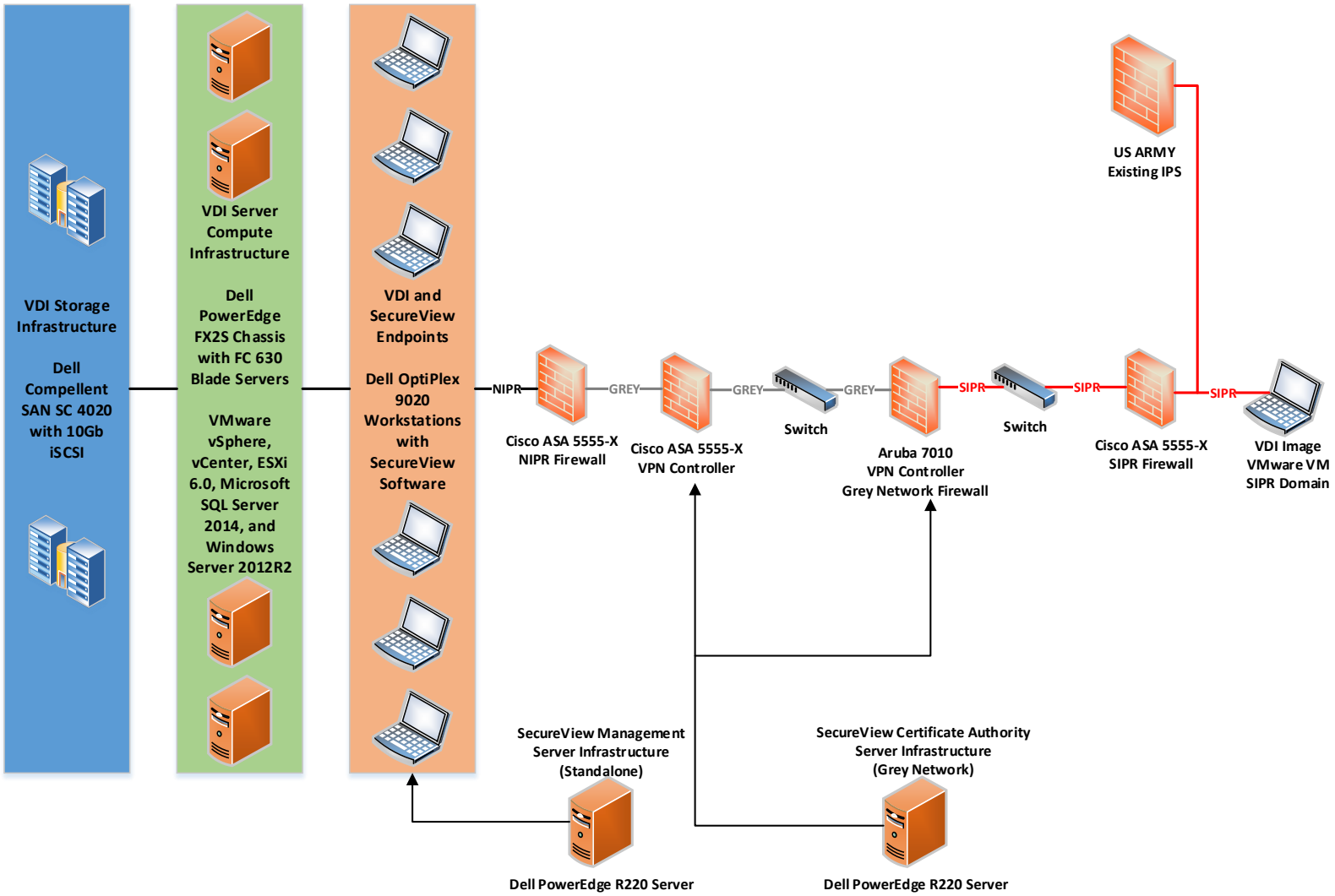


Figure 2: ID's 500 seat VDI Design High-Level Architecture with CSfC MA CP and SecureView Cross Domain Solution

This Whitepaper includes proprietary data that shall not be disclosed outside the Government.
This data is subject to the restriction included on the Title Page of this proposal.

ID's 2500 Seat VDI Solution: Bill of Materials (BOM):

Primary Component	Description	Quantity
Server Compute Infrastructure	**Chassis:** Dell PowerEdgeM1000E Blade Server Enclosure **Integrated I/O Module**: Redundant 10GbE Pass Through Module **Power Supply:**Redundant Power Supplies. 6x3000W @ 200-240V **Blades (Qty7):** M630 Server (Qty 16) **Processor**: Dual Intel Xeon E5-2683 v3 2.0Ghz, 35M Cache, 9.60 GT/s **Trusted Platform Module:** TPM 2.0 FIPs, Common Criteria **Memory:** 32GB RDIMM, 2400 MT/s, Dual Rank **RAID:** Diskless Configuration, PERC Controller, H330 Controller **Network Daughter Card:** QLogic 57810-K Dual Port 10Gb Blade Card **Virualization HyperVisor:** VMWare ESXI 6.0 **Virtualization Desktop Software:** Vsphere Desktop 100VM Pack (Qty 25)	1
SecureView Management Server	**Chassis:** Dell PowerEdge R220 **Processor**:Intel Xeon G3430 3.3Ghz, 3M Cache **Memory:** 8GB UDIMM **RAID:** RAID 1, H310 2 HDD **Hard Drive:** 500GB 7.2K RPM SATA	1
SecureView Software	SecureView Management Server (Any Workstation Count) Reoccurring Annually	1
	SecureView Workstation - Single Workstation - Reoccurring Annually	2500
End Points	Dell Optiplex 9020 SFF Processor: Intel i5-4570 Memory: 16GB (2 x 8GB) NIC: Intel I217LM	2500
	Dell E2216H 22 inch Monitor (optional)	2500
	NIPR CAC Reader (Identive SCR3310/v2 Smart Card Reader)	2500
	SIPR CAC Reader (HID OMNIKEY 3121 USB Card Reader)	2500
	VIASAT Eclypt Core Encrypted Internal Hard Drive minimum 256GB	2500
	Intel SSD Pro 1500 series (360GB | M.2 Form Factor and 2.5in Form Factor)	2500
Storage Infastructure	Dell Compellent SC8000 64GB Memory	1
	Compellent SC8000 Controller	2
	1600GB SAS 12Gb, SSD, WI, 2.5	24
	1.8TB 12 Gb, 10K, 2.5 HDD	24
	1.92 TB SAS 12Gb, SSD	7
	IO, 6Gb SAS, 4-Port PCI-E Low Profile	8
	Software: Dell Storage Center OS Core Base License	2
	Software: Storage Optimization Bundle - Base License	1
	Software: Storage Center Expansion Lic, Data Progression Expansion, FastTrack Expansi	5
	Dell Networking S4048-ON, 48X 1-GbE SFP+ and 6x 40GbE QSFP+ ports, IO to PSU	2
Cisco ASA Hardware	ASA 5555-X with SW, 8GE Data, 1GE Mgmt, AC, 3DES/AES	3
	ASA 9.2.2 Software image for ASA 5500-X Series,5585-X,ASA-SM	3
	ASA 5545-X/5555-X AC Power Supply	3
	AC Power Cord (North America), C13, NEMA 5-15P, 2.1m	3
	ASA 5545-X/5555-X Interface Card Blank Slot Cover	3
	ASA 5512-X -- 5555-X Hard Drive Blank Slot Cover	3
	ASA 5500 Strong Encryption License (3DES/AES)	3
	^ASA 5555 IPS Part Number with which PCB Serial is associated	3
	ASA 5545-X/5555-X AC Power Supply	3
Cisco ASA Licensing	Cisco AnyConnect 1-Yr 250 User Apex License	10
	Cisco AnyConnect 1-Yr 250 User Apex Subscription	10
	Cisco AnyConnect 1-Yr 250 User Apex (ASA License Key)	10
Aruba Cloud Services Controller	Aruba 7010, 12x10/100/1000BASE-T PoE/PoE+ (150W), 4x10/100/1000BASE-T, 2x1G BASE-X	1
	Policy Enforcement Firewall for Aruba 7005 (VIA/VPN users)	1
	Advanced Cryptography (256 Sessions)	2

This Whitepaper includes proprietary data that shall not be disclosed outside the Government.
This data is subject to the restriction included on the Title Page of this proposal.

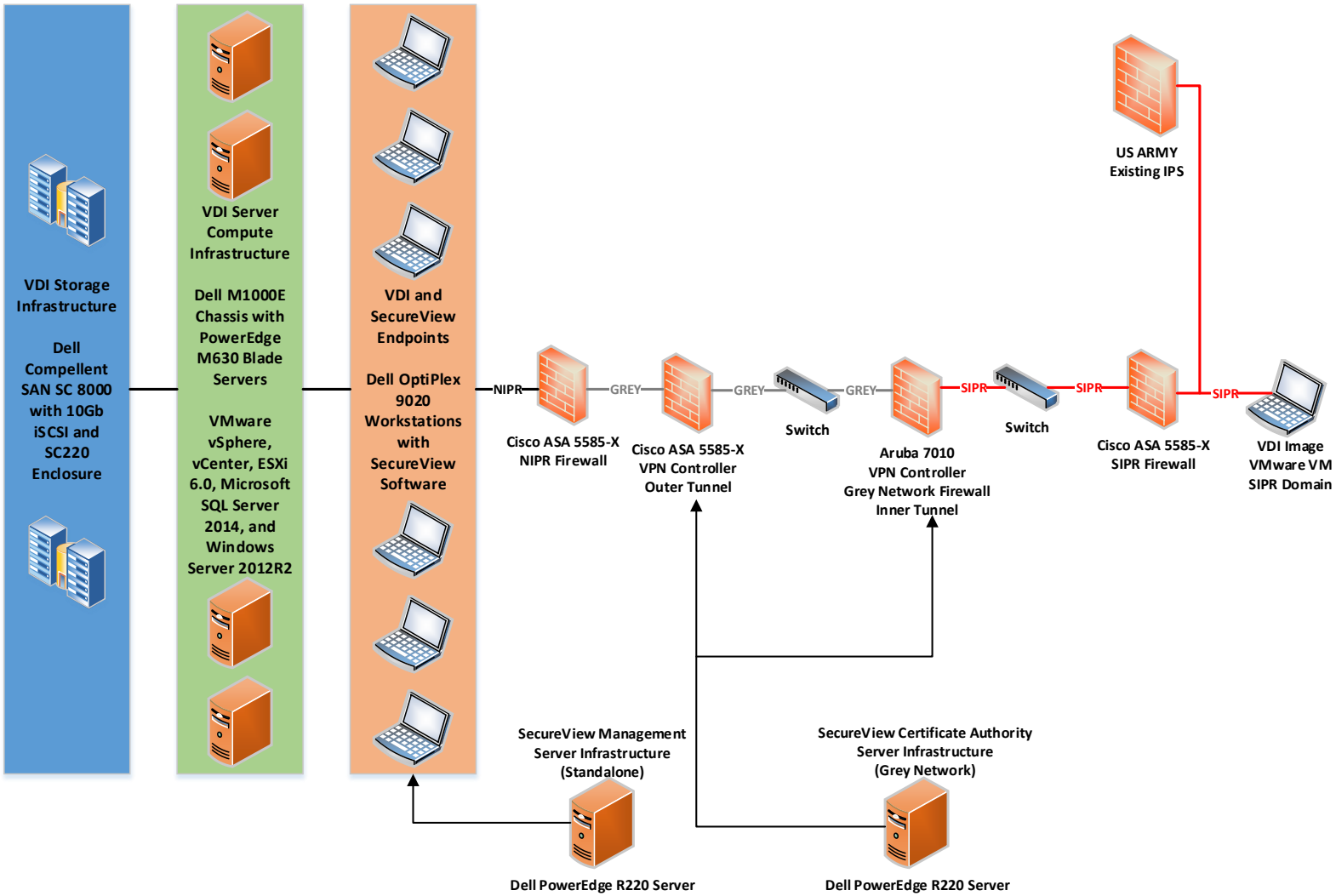


Figure 3: ID's 500 seat VDI Design High-Level Architecture with CSfC MA CP and SecureView Cross Domain Solution

This Whitepaper includes proprietary data that shall not be disclosed outside the Government.
This data is subject to the restriction included on the Title Page of this proposal.

Pricing and Licensing. A critical step in the VDI implementation initiative is the initial assessment task, during which we conduct key analysis activities that drive primary decisions around platform architecture and the OEM products within that architecture (hardware and software), as well as the service delivery model to be implemented (On-premises VDI, secure private cloud VDI as a service). This analysis determines the future operational requirements for the VDI environment, while assessing the existing network, server, storage and virtualization capabilities present within the organization. When an organization has significant investments in a specific OEM's storage, server, virtualization or network, ID's VDI team works with the customer to develop a VDI architecture that leverages those existing product investments and staff expertise. There is no "one size fits all" pricing model. The complexity of the organization's requirements, topology of their existing IT infrastructure and global network capabilities, the number and types of software applications to be virtualized and delivered to users' desktops, and the COOP/DR approach all drive solution complexity, implementation resource requirements and timelines, and ultimately costs and cost items associated with VDI solution architecture, engineering and deployment.

Hardware and Software Licensing. There is no standard hardware and software licensing model for VDI components. Most organizations have enterprise licenses for a subset of the licenses required for VDI, and our requirements analysis includes a review of these US documents in order to minimize costs. We also include license costs and how they affect COOP/DR, test environments, redundancy and scalability.

There are two primary cost models. For an on-premises implementation, the customer incurs up-front costs for hardware and software licensing and annual recurring maintenance. We would recommend that, at a minimum, a Development and Production environment be implemented; as part of the Assessment task, we would work with US ARMY to determine appropriate sizing for each environment and the scalability strategy for the Production environment. For cloud-based implementations, the customer pays a per-user VDI service charge (with a fee schedule that is based on the user profile(s)), and ID is responsible for hardware and software licensing fees, along with annual recurring maintenance.

Product Licensing Methodology. Product licensing methodology depends on the recommended VDI approach. ID follows ITIL asset and configuration management processes to provide customers with a capability to effectively manage licensing, software keys, etc.

Data Storage Licensing. Unless a customer does not have a SAN structure that can accommodate VDI, our recommended approach is to take advantage of the existing SAN and its licensing. If the SAN cannot be used, we will research and recommend an optimal solution from a price/performance perspective.

Training and Professional Services Costs. Orientation training and onsite support during installation is included in the installation cost. See Section 6 for ID's approach to training. Post-installation support costs are dependent on level of support required, location where services are provided, and service level agreements.

To begin installation, ID conducts an initial assessment task that includes developing a robust understanding of the organization's prioritized VDI requirements and evaluation of the organizations existing IT infrastructure across all elements of the organization to be supported by the VDI implementation: network, servers, storage, virtualization technologies, remote access solution(s), user authentication solution, inventory of applications to be virtualized, and determination of the number of unique user profiles to be created. This initial assessment can be conducted on a Firm Fixed Price basis, and can span from as little as 4 weeks to as much as 6 months, depending on the size and complexity of the organization and their VDI objectives. A key element in minimizing the cost of this assessment is the organization's ability to provide in a timely and complete manner required information and staff resources knowledgeable about the existing IT environment.

Subsequent VDI architecture, engineering and deployment tasks are delivered under a Time and Materials or Firm Fixed Price basis. ID's VDI team would work onsite with US ARMY's IT staff throughout the Architecture, Engineering and Deployment phases. For DOJ and our Intelligence Community client, ID maintains scaled-down Sustainment teams that provide ongoing operational support and administration for Production VDI environments.

We recommend that, if US ARMY intends to have its own employees maintain the VDI infrastructure, such IT staff pursue advanced training in OEM components comprising the VDI solution. We also recommend that staff work

This Whitepaper includes proprietary data that shall not be disclosed outside the Government.
This data is subject to the restriction included on the Title Page of this proposal.

closely with the ID VDI team during the latter part of the Engineering process, and throughout the Deployment process, so that they are fully "up to speed" when VDI is put into Production. For a cloud-based VDI delivery model, customers can determine the SLAs and associated response times they require, which will determine the monthly fees paid for Tier 1, 2 and 3 support.

Ongoing/Support Fees. If the VDI is deployed on premises, ongoing fees will depend on existing licensing agreements. These fees will be identified and included in our recommended approach. Upgrade and maintenance fees for a cloud-based deployment are included in the standard monthly charge. For upper tier support, ID recommends including Tier 3 follow-on support for at least the first year because each VDI implementation has a level of unique configurations that need to be understood in order to provide the required level of support. After the first year, we expect current staff to have gained experience, and that at that time, standard hardware and software vendor support will be sufficient.

Return on Investment (ROI)/Savings. Return on Investment (ROI) is realized through:

- Reduced costs for end-point refreshes as significant percentages of an organization's user population transition to zero client connection devices; in the short term, these cost savings are offset by IT infrastructure investments required to stand up the VDI services and consolidation of end-user data to centralized data center locations.
- Cost savings through elimination or deferral of end-point refreshes as user's transition to the VDI interface, and many or most users transition to zero client devices, since the VDI connection requires minimal computing resources at the end user's desktop. Also, existing thick clients can be repurposed as thin clients, greatly extending their usable life, and thereby eliminating or delaying significant end-point refresh costs.
- Elimination or significant reduction of regional/field-based desktop support staff, as desktop support, profile and user management functions are consolidated, as part of the consolidation of user data, desktops and profiles to the data center(s).

ROI in Similar Organizations. ROI estimates based on ID's own VDI implementations, as well as guidance provided by major VDI OEMs with whom ID is a VAR (VMWare, Citrix, Cisco and Dell) demonstrate a Return on Investment of between 12 – 24 months, with continued reductions in operations costs realized post-ROI. The most significant long term cost savings is a reduction in O&M staffing required to support end users. ROI can be accelerated through eliminating or delaying end point refreshes, and instead investing in VDI servers and storage.

Potential Points of Savings. Organizations undertaking large-scale implementation of VDI can realize both one-time and recurring cost savings in the following areas:

- Significant infrastructure cost reductions by eliminating the need for multiple physical workstations across multiple network domains and eliminates the need for KG-175 TACLANE Encryptors
- Transition to zero-client workstations across a significant percentage of the end user community; zero clients cost significantly less than traditional desktop/laptops. They do not require refresh cycles and can be utilized until they experience an electrical or mechanical failure.
- Significant O&M staff reductions, as the requirement to maintain staff in the field to support VDI users is virtually eliminated. For example, ID is currently supporting an Intelligence Community VDI concurrent user community of 30,000 with an operations team of 20 FTEs.
- Significantly enhanced security posture, which has the dual benefit of long term cost savings in: end-point security and costs associated with responding to end point security compromises (such as stolen or lost laptops). With consolidation of user data from their local hard drives to the organization's data center, end point devices no longer present an entry point for cyber-attacks.

This Whitepaper includes proprietary data that shall not be disclosed outside the Government.
This data is subject to the restriction included on the Title Page of this proposal.