



U.S. Army Thin/Zero Client Computing Reference Architecture

**Version 1.0
14 MAR 2013**

CHANGE HISTORY

Version	Date of Change	Author(s)	Page(s) Changed	Comments
0.05	15 June 2012	CIO/G-6 AAIC-AOB	All	Coordinating Draft (Internal AO Staffing)
0.99	21 August 2012	CIO/G-6 AAIC-AOB	All	O6/GS-15 level Review Army-Wide
0.999	06 December 2012	CIO/G-6 AAIC-AOB	All	AAIC Director's Review
1.0	14 March 2013	CIO/G-6 AAIC-AOB	Background & Scope	Inclusion of LWN 2020 & Beyond Institutional Capabilities

Table of Contents

EXECUTIVE SUMMARY2

1 Introduction for Thin/Zero Client Computing Implementation in the Army ..2

1.1 Background.....2

1.2 Overview and Problem Statement.....2

1.3 Purpose.....3

1.4 Vision, End State and Objectives4

1.4.1 Vision.....4

1.4.2 End State.....4

1.4.3 Objectives.....5

1.5 Scope, Assumptions and Intended Audience.....5

1.5.1 Scope5

1.5.2 Overarching Facts/Assumptions.....6

1.5.3 Intended Audience /Stakeholders.....6

1.5.4 Thin/Zero Client Computing Reference Architecture Configuration Management.....7

1.6 Thin/Zero Client Computing Model (Figure 1)7

1.6.1 End-user/Thin Client Devices.....7

1.6.2 Thin/Zero Client Computing Model – Data Center (Back End).....7

1.6.3 Thin/Zero Client Computing Model – Network Link/Display Protocols...8

2 Thin/Zero Client Computing Reference Architecture8

2.1 Relationship between Thin/Zero Client Computing and Other DoD/Army Enterprise IT Efforts.....9

2.1.1 DoD Information Enterprise Architecture Version 2.09

2.1.2 DoD Core Data Center Reference Architecture (CDC RA) Version 1.010

2.1.3 Joint Information Environment (JIE).....10

2.1.4 Common Operating Environment (COE), Oct 201010

2.1.5 Unified Capabilities (UC).....10

2.1.6 Identity, Credential and Access Management (ICAM)10

2.1.7 Network Boundary Security Top Level Architecture (TLA).....11

2.1.8 Army Data Center Consolidation Plan (ADCCP)11

2.1.9 Installation, Information, Infrastructure, Communications and Capabilities (I3C2).....11

2.1.10	Network Operations (NetOps).....	11
2.2	DoD Information Enterprise Architecture Capabilities Line of Sight	12
2.3	Army Thin/Zero Client Computing Reference Architecture Inputs, Processes and Outputs (Figure 5).....	12
3	Thin/Zero Client Computing Reference Architecture Components.....	13
3.1	Operational Capabilities Model Overview	13
3.2	Operational Activities Model Overview.....	14
3.3	Virtualization - Joint Information Environment (JIE) Alignment.....	15
3.4	Thin/Zero Client Computing Reference Architecture Principles & Business Rules	16
3.5	Capability 1: Deliver an Army Thin/Zero Client Computing Solution.	18
3.5.1	Deliver Thin/Zero Client Computing Environment Facts and Assumptions.....	22
3.5.2	Deliver Thin/Zero Client Computing Environment Constraints	22
3.5.3	Deliver Thin/Zero Client Computing Environment Operational Risks... ..	23
3.6	Capability 2: Enhance Security and Information Assurance.....	24
3.6.1	Enhance Security and Information Assurance Facts and Assumptions.....	28
3.6.2	Enhance Security and Information Assurance Constraints.....	28
3.6.3	Enhance Security and Information Assurance Risks	29
3.7	Capability 3: Enhance Maintenance and Support	30
3.7.1	Enhance Maintenance and Support Facts & Assumptions	31
3.7.2	Enhance Maintenance and Support Constraints	31
3.7.3	Enhance Maintenance and Support Risks.....	31
3.8	Capability 4: Maximize Usability and Flexibility	32
3.8.1	Maximize Usability and Flexibility Facts and Assumptions	32
3.8.2	Maximize Usability and Flexibility Constraints.....	32
3.9	Capability 5: Improve Performance Quality and Reliability.....	33
3.9.1	Improve Performance Quality and Reliability Facts and Assumptions	35
3.9.2	Improve Performance Quality and Reliability Constraints	35
3.9.3	Improve Performance Quality and Reliability Risks.....	35
3.10	Capability 6: Enhance Business Processes	36
3.10.1	Enhance Business Process Requirements Facts and Assumptions	37
3.10.2	Enhance Business Process Requirements Constraints	37
3.10.3	Enhance Business Process Requirements Risks.....	38



Appendices:

Appendix A – Standards Views..... 39
Appendix B – Overview and Summary..... 59
Appendix C – Vocabulary (Integrated Dictionary)..... 61
Appendix D – Acronym Listing..... 65
Appendix E – References..... 71

Table of Figures

Figure 1: High Level Operational Concept Graphic ("To Be" Configuration) 3
Figure 2: Thin/Zero Client Capabilities 5
Figure 3: Organizations and Architectural Relationships..... 9
Figure 4: Information Enterprise Architecture Capabilities Line of Sight..... 12
Figure 5: Reference Architecture Inputs, Processes and Outputs..... 13
Figure 6: Thin/Zero Client Computing Capabilities Alignment to DoD IEA..... 14
Figure 7: Thin/Zero Client Operational Activities Alignment with Capabilities 15
Figure 8: Thin/Zero Client Computing Alignment with JIE Capabilities 16

Table of Tables

Table 1: Deliver Thin/Zero Client Computing Requirements	21
Table 2: Enhance Security and Information Assurance Requirements	28
Table 3: Enhance Maintenance and Support Requirements	31
Table 4: Maximize Usability and Flexibility Requirements.....	32
Table 5: Enhance Performance Quality and Reliability Requirements	35
Table 6: Enhance Business Process Requirements	37

EXECUTIVE SUMMARY

14 MAR 2013

The Army will implement a centrally managed, thin/zero client end-user computing technology that will standardize the end-user computing experience, back-end management and control. Implementation will result in improved security, standardization of the end-user experience, increased transparency, enhanced accessibility and reduced costs.

The primary intended audience for this Reference Architecture (RA) is the Assistant Secretary of the Army for Acquisition, Logistics and Technology (ASA(ALT)), designated ASA(ALT) Program Executive Officers (PEOs) and Program Manager (PMs), as well as technical and solutions architects and engineers involved in the planning and execution of Thin/Zero Client Computing. This rules-based Reference Architecture defines underlying principles, business rules and technical standards. It describes Thin/Zero Client Computing in the context of the Department of Defense (DoD) Information Enterprise Architecture v2.0 (IEA, July 2012) and Core Data Center Reference Architecture v1.0 (CDC RA, October 2012) and is intended to guide Army thin/zero client implementation.

This Reference Architecture is informed by and aligned to the Thin/Zero Client Computing Requirements Document, Version 1.0. The scope of this Reference Architecture is limited to the initial implementation of Thin/Zero Client Computing in the Generating Force Army, for selected Army Installations in the Continental United States (CONUS for NIPRNet and SIPRNet) as a component of the Institutional Capability Set (ICS) implementation. This version 1.0 does not include OCONUS (Outside the Continental United States) installations, tactical requirements, or the Reserve Components (Army National Guard and U.S. Army Reserve). Server-side mission applications to support Thin/Zero Client Computing are being addressed in the Army Data Center Consolidation Plan (ADCCP).

This Thin/Zero Client Computing Reference Architecture is approved for immediate use. My POCs for this document are: LTC Eric Van Den Bosch, Division Chief, AOB, Army Architecture Integration Center (AAIC) (703) 545-1445, NIPR: eric.j.vandenbosch.mil@mail.mil or Ms. Reeth Nakka, Action Officer, AAIC-AOB, 703 545-1441, reeth.r.nakka.ctr@mail.mil.



GARY W. BLOHM
Director, Architecture Integration Center
Army Chief Information Officer/G-6

1 Introduction for Thin/Zero Client Computing Implementation in the Army

1.1 Background

The Army relies heavily on personal computing devices throughout the force. In nearly every mission, personal computers (PCs) contribute to continuing improvements in user productivity and organizational effectiveness. Army users today operate in a non-standard computing environment which complicates network defense, support, administration, and device and application management — greatly impacting the user experience. In addition, the Army's current computing environment does not support a centralized Program Objective Memorandum (POM) for IT requirements, leaving leadership with an inaccurate account and visibility of IT expenditures associated with a required end-to-end architecture. Over the past five years, organizations throughout the Army have independently implemented multiple thin/zero client solutions. These instantiations have been analyzed to capture lessons learned in order to establish Army-wide standardized solutions for Thin/Zero Client Computing, and are reflected in this reference architecture.

To realize the full operational capabilities of LandWarNet 2020 and Beyond, it is essential that Network Capability Sets (NCS) integrate operational and institutional requirements, defined as Operational Capability Sets (OCS) and Institutional Capability Sets (ICS). Institutional Capability Sets are comprised of the hardware, applications, services and communications transport necessary for day-to-day Army business and installation management. Institutional Capability Sets also support operational units, providing multiple capabilities resident across various Army/DoD installations as they train, prepare to deploy and deploy. CIO/G-6 will design Network Capability Sets, and G-3/5/7 will select and prioritize the receiving installations and units. Fielding of Thin/Zero Client end user devices is planned to be part of the Institutional Capability Sets for selected installations beginning in FY-15 to achieve a more secure, flexible, and cost effective computing environment.

1.2 Overview and Problem Statement

The Army faces continual threats from enemies who target vulnerabilities in the Army's network, computing, and data storage. Network and information security are paramount for protecting and safeguarding information and communications technologies, as well as Warfighting and business capabilities. The Army therefore must provide a more secure, standardized, and effective computing capability that enables mission command and meets strategic requirements at each Post, Camp and Station. The Army requires networks that are tightly controlled and secured; today the network lacks effective enterprise management to enable and secure all end-user computing devices. As a result, many network vulnerabilities are introduced at the end node. These vulnerabilities occur when users allow the introduction of inadvertent or malicious applications or changes to be introduced. One cause is security patches and version updates that are not pushed uniformly to all end-user devices. The resulting intrusions cost a significant amount of time and money to track, isolate and resolve.

Hackers are shifting from theft to destruction, and this represents a serious threat for which the U.S. needs to prepare. The first step in preparing the country is better training for the people who defend the network. The second is defensible architecture that starts out with a thin-virtual client cloud environment.

—General Keith Alexander, Commander, U.S. Cyber Command (CYBERCOM)

1.3 Purpose

The purpose is to create a Thin/Zero Client Computing environment to provide Army users with a centrally managed computing capability for desktop and application services. Thin/Zero Client Computing employs a computing architecture in which applications, data, processing, and storage are hosted on an Installation Processing Node (IPN) back-end infrastructure, as shown in Figure 1. This Operational Concept Graphic represents the Thin/Zero Client Computing “To Be” configuration for the CONUS Thin/Zero Client Computing Environment. The graphic depicts three major aspects: 1) the end-user environment; 2) the network environment; and 3) the back end or data center environment. The initial Army enterprise Thin/Zero Client Computing instantiation will be installation-centric with regional/remote access from DoD/Army facilities for both classified (SIPRNet – or Secure Internet Protocol Router Network) and unclassified (NIPRNet – or Non-classified Internet Protocol Router Network) data through the Defense Information Systems Network (DISN) cloud, and remote access from untrusted networks (Internet Cloud) at home/hotel for unclassified (NIPRNet). Thin/zero client users will be provisioned to meet all of the Information Assurance (IA) requirements. Thin/zero client users will experience the same quality of service as current thick client users on installations. The Army Installation Campus Area Network (ICAN) will provide the required bandwidth for high Quality of Service (QoS) for all users. Installations’ data centers will further enable services, with the virtualization of operating systems, applications, and profiles.

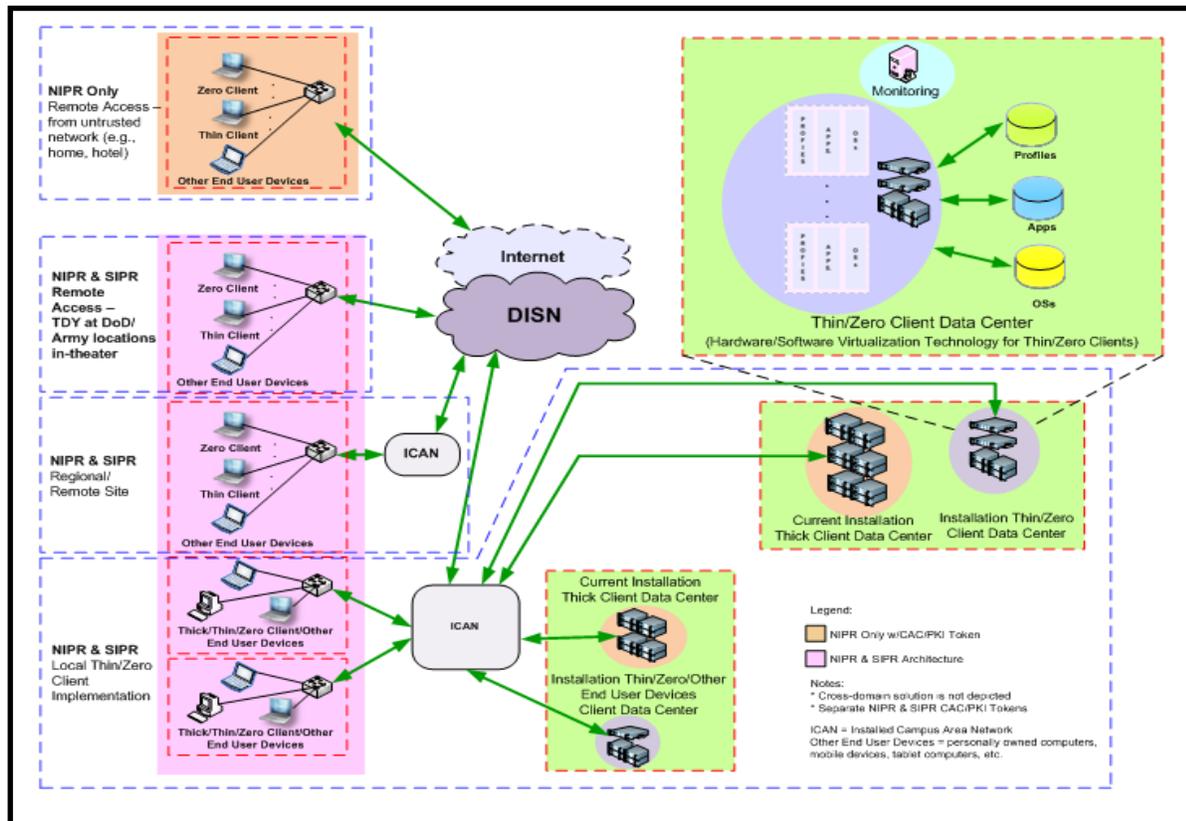


Figure 1: High Level Operational Concept Graphic ("To Be" Configuration)

1.4 Vision, End State and Objectives

1.4.1 Vision

The Army will implement a centrally managed, thin/zero client end-user computing technology. Thin/Zero Client Computing will standardize the end-user computing experience and back-end management and control. Standardization will result in increased mission effectiveness through increased accessibility, streamlined systems administration, improved security and visibility of the computing environment, and improved efficiency.

1.4.2 End State

The end state is a Thin/Zero Client Computing program that provides the Army's end-user computing portion of the Joint Information Environment (JIE) to meet Army business, Warfighting, and unique mission requirements. The Army will virtualize its computing environments, where appropriate, to effectively and efficiently support business and operational mission requirements. Rationalization of users as a specific type based on mission and function is best determined once an analysis has been conducted at the prospective Post/Camp/Station. The Thin/Zero Client Computing end state will:

- Significantly enhance the Army's network security posture by implementing a more standardized and secure architecture aligned with Global Information Grid (GIG) IA architecture and other IA/Security requirements in companion architectures (e.g., Identity Credential and Access Management (ICAM), Army Data Center Consolidation Plan (ADCCP), Unified Capabilities (UC), Network Boundary Top Level Security Architecture (TLA).
- Be scalable to simultaneously migrate 100% of SIPRNet users and approximately 80% of NIPRNet users by FY20.
- Be managed by a Program Manager (PM) to engineer, acquire, build, implement, configure, change control, and perform life cycle technology refresh, per approved requirements.
- Be operated and maintained by Network Enterprise Centers (NECs) and Network Operations Centers (NOCs), and codified through the Army Baseline for IT Services (ABITS) process.
- Align Thin/Zero Client Computing with the Installation Information Infrastructure Communications and Capabilities, (I3C2), Unified Capabilities (UC), Army Baseline IT Services (ABITS), Enterprise Collaboration Services (ECS), and ADCCP.
- Position the Army to use cloud computing services by migrating the back-end infrastructure into Installation Processing Nodes (IPNs) within the approved Army Data Center locations as identified by the ADCCP.
- Centralize IT management, programming, and configuration management through the PM.

1.4.3 Objectives

Figure 2 depicts the Army Thin/Zero Client Computing Objectives to standardize and centralize the computing environment to increase Mission Effectiveness, Security and IT Asset Visibility and describes opportunities for cost efficiencies through the implementation of Thin/Zero Client Computing.

Thin/Zero Client Computing standardizes and centralizes management to increase:		
Mission Effectiveness	Security	IT Asset Visibility
<ul style="list-style-type: none"> • Computing capability • Application/data availability • Network and data resilience and reliability • Remote access • Interoperability • Resource allocation • User device flexibility 	<ul style="list-style-type: none"> • Robust network protection • Fewer end user vulnerabilities • Minimal attack surface area • Comprehensive patch/version management • Rapid/frequent state restoral • Data-at-rest security • Identity and access management 	<ul style="list-style-type: none"> • Improved projection and planning • Accurate budgeting and programming • Clinger-Cohen Act compliance • IT architecture control • Cost control • Mission application/data consolidation
These capabilities provide the opportunity for cost efficiencies through: <ul style="list-style-type: none"> • Efficient Operations & Maintenance (O&M) through reduced touch labor • Reduced tech refresh • Enterprise application/license identification and rationalization • Elimination of outdated software 		

Figure 2: Thin/Zero Client Objectives, Capabilities and Benefits

1.5 Scope, Assumptions and Intended Audience

1.5.1 Scope

This Reference Architecture is driven by the Thin/Zero Client Computing Requirements Document Version 1.0. This Thin/Zero Client Computing Reference Architecture applies to the thin/zero client computing implementations in key locations in support of the Generating Force Army computing environment (e.g. end-user devices, servers, applications, storage) by leveraging existing infrastructure at locations where minimal investment is required through coordination with Installation, Information, Infrastructure, Communications and Capabilities (I3C2) and Unified Capabilities (UC) investments. Implementation will be on NIPRNet and SIPRNet. The sites and networks in the initial phase may be modified based on funding and prioritization from leadership. Implementation plans must be aligned with Active Directory Forest way ahead and other ongoing initiatives to ensure appropriate operation. Out of scope for

Version 1.0 of this Reference Architecture are the Reserve Components (United States Army Reserve and Army National Guard) and tactical forces (tactical infrastructure, tactical applications, and industrial control systems). Remote CONUS user locations will be addressed on a case by case basis. Support for them will be aligned with infrastructure availability and technology enhancements anticipated from industry.

Thin/Zero Client Computing has the potential for cost avoidance with some savings when implemented at locations with high user densities. Thin/Zero Client Computing reduces operation and maintenance (O&M) costs beginning approximately 2 years after implementation, and it will allow savings in touch labor and technical refresh in the out-years. Top-priority sites leverage high user density on NIPRNet and SIPRNet. Limited implementation on SIPRNet and/or NIPRNet will increase the time required to achieve the projected return on investment or negate the return on investment.

A risk assessment was part of the Thin/Zero Client Computing Capability Based Analysis (CBA). Analysis of lessons learned from industry and Army early adopters (e.g., Training & Doctrine Command (TRADOC), Intelligence & Security Command (INSCOM), Human Resources Command (HRC), and Space & Missile Defense Command (SMDC) are included in this document.

1.5.2 **Overarching Facts/Assumptions**

- The initial effort will be scoped to address Generating Forces on designated installations.
- Thin/Zero Client Computing will be implemented on an installation basis, with the back end consolidated under one logical IPN, connected by the Installation Campus Area Network.
- Thin/Zero Client Computing systems will be implemented by an Army enterprise acquisition program.
- Some organizations have computing requirements beyond the baseline requirements.
- Additional CBAs will be required to develop a Thin/Zero Client Computing RA that includes operational and tactical requirements.
- Security Infrastructure will be in place prior to virtualization of end-user environments.
- Baseline virtual applications will be established prior to implementation.
- Virtualization will drive a Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel and Facilities (DOTMLPF) review to be conducted by the PM in coordination with TRADOC.

1.5.3 **Intended Audience /Stakeholders**

The primary intended audience for this RA is ASA(ALT), designated ASA(ALT) Program Executive Officers (PEOs) and Program Managers (PMs) as well as technical and solutions architects and engineers engaged in the planning and execution of this Army capability. Other stakeholders and related initiatives include:

- DoD Chief Information Officer (CIO).
- Defense Information Systems Agency (DISA).
- Army Chief Management Officer (CMO)– Business Transformation.

- Army Deputy Chief of Staff, G-3/5/7.
- Army CIO/G-6.
- The Army Training & Doctrine Command (TRADOC).
- U. S. Army Cyber Command (ARCYBER).
- Network Enterprise Technology Command/9th Army Signal Command (NETCOM/9th (A) SC).
- 7th Signal Command (Theater).

1.5.4 Thin/Zero Client Computing Reference Architecture Configuration Management

Change requests to this Reference Architecture shall be governed by the Enterprise Information Environment Mission Area (EIEMA) Architecture Configuration Control Team (ACCT).

1.6 Thin/Zero Client Computing Model (Figure 1)

1.6.1 End-user/Thin Client Devices

Thin-client end-user devices fall into one of three major categories:

1) **Zero or Stateless Thin Clients** that do not contain an embedded Operating System (OS); back-end solutions must provide the client OS and applications. They have a limited set of instructions that enable them to connect to the network, but do not have to be patched.

2) **Thin Clients with embedded OSs** such as UNIX embedded or Windows 7 embedded. These embedded OSs run in firmware that cannot be patched and must be flashed to get the latest security patches. These devices do not allow for migration to another OS, such as from XP to Windows 7.

3) **Diskless PCs** that have no internal hard drive or existing PCs that have had the internal hard drives removed.

1.6.2 Thin/Zero Client Computing Model – Data Center (Back End)

Today, back-end solutions fall into one of the following three basic categories:

1) **Terminal Services**, which are typically Microsoft Windows Terminal Services or Remote Desktop Service (RDS). There are also other third-party solutions that provide the same functionality. All processing is done on the server, and only keystrokes and screen refreshes pass over the network.

2) **Streaming (OS) Applications**: This option streams the server-based OS and/or applications to the thin-client user. Processing is done on the client and requires a robust network to transport data between the back-end infrastructure and the thin client devices, along with robust thin client devices to run the OS and/or applications locally.

3) **Virtual Desktops**, which provide server-based virtual desktops (OS and applications) that are accessed by thin-client users as though they are remote computers. All processing is done on the server and only keystrokes and screen refreshes pass over the network.

Virtualization technologies are evolving, and the Army anticipates that over time there may be more solutions that meet the requirements of this architecture.

1.6.3 Thin/Zero Client Computing Model – Network Link/Display Protocols

Common network protocols comprise both new and old market-based protocols used in thin-client architectures. The new protocols provide capabilities that are unavailable or limited in older protocols, such as video, bi-directional audio, synchronization, and universal serial bus (USB) redirection. New thin-client devices include old and new protocols to provide interoperability with old and new back-end solutions. Examples include Remote Desktop Protocol (RDP), which is a Microsoft protocol available with most thin-clients; Independent Computing Architecture (ICA), a CITRIX proprietary protocol; Simple Protocol for Independent Computing Environments (SPICE), a Red Hat remote display system for virtual environments; and PC-over-IP (PCoIP), a proprietary protocol for remote workstation and desktop solutions.

2 Thin/Zero Client Computing Reference Architecture

The Army Thin/Zero Client Computing Reference Architecture defines the required attributes of the Computing environment. It describes Thin/Zero Client Computing in the context of the DoD Information Enterprise Architecture (IEA), and is intended to guide the implementation of a standardized computing environment. This Thin/Zero Client Computing RA will serve as the primary guidance for Army organizations and programs in developing thin/zero client computing Solution Architectures. This RA will contribute to computing environment standardization consistent with Army Network 2020 and Beyond Objectives. When implemented to the standards described in this RA, Appendix A, Thin/Zero Client Computing contributes to strengthening the Army network security posture and, for larger user densities, reducing the overall Information Technology operating costs over time. Figure 3 below, Organizations and Architectural Relationship, depicts the Reference Architecture hierarchy from DoD/Joint Information Environment (JIE) Architectures to the Army Enterprise Architecture policy and guidance, to PEO/PM-driven Segment and Solution Architectures.

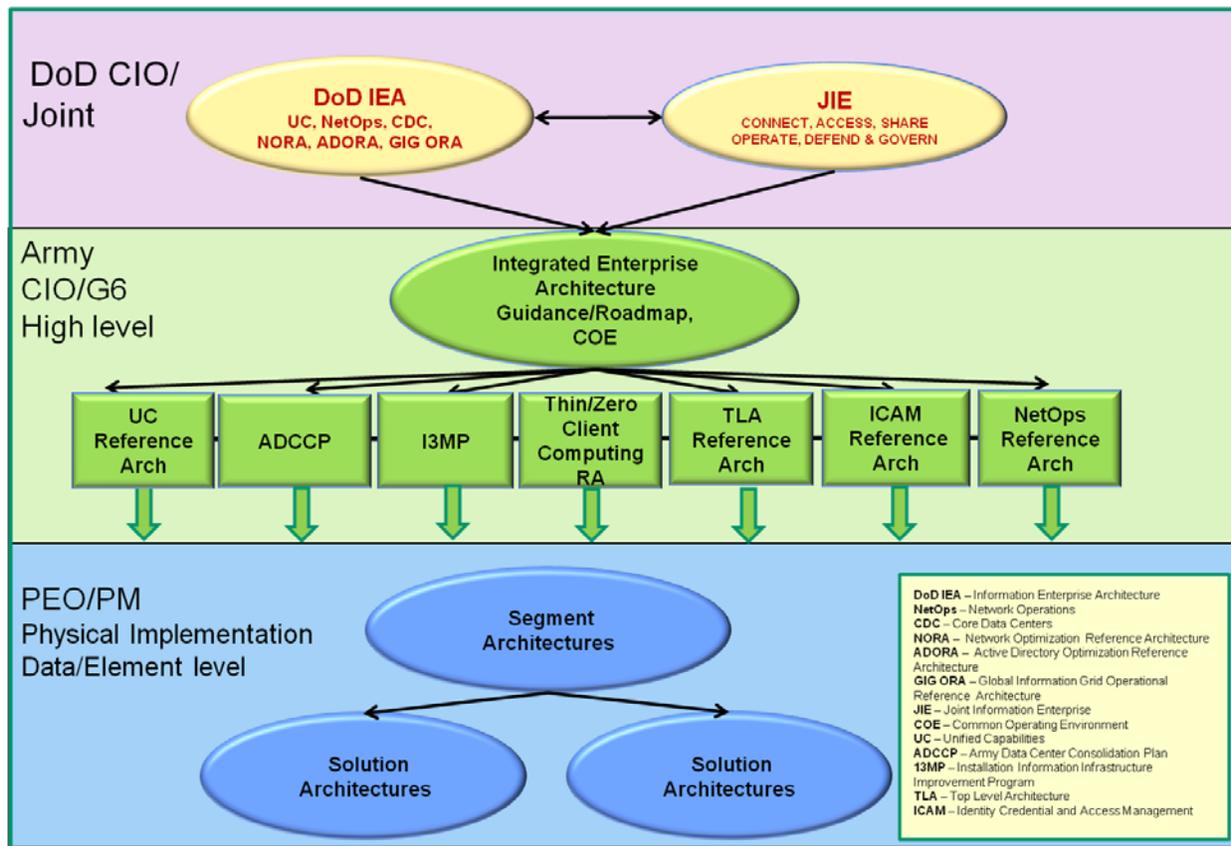


Figure 3: Organizations and Architectural Relationship

2.1 Relationship between Thin/Zero Client Computing and Other DoD/Army Enterprise IT Efforts

The Army Enterprise-level Thin/Zero Client Computing initiative complements other IT initiatives reflected in Figure 3 above. Those relationships are briefly described below. Additional information can be found at: <http://ciog6.army.mil/Architecture/tabid/146/Default.aspx>.

2.1.1 DoD Information Enterprise Architecture Version 2.0

The approved DoD IEA provides a clear, concise description of what the Information Enterprise (IE) must be and how its elements should work together to accomplish such as transformation and deliver efficient, cost effective information and service sharing. The DoD IEA enables proper planning for shaping the DoD IT landscape, managing the acquisition of required resources, and effectively operating the resulting IT environment. The DoD IEA describes the future vision for the IE based on merging operational needs with the concepts previously embedded in separate net-centric strategies. This Thin/Zero Client Computing Reference Architecture is aligned with the DoD IEA capabilities and activities.

2.1.2 **DoD Core Data Center Reference Architecture (CDC RA) Version 1.0**

The approved DoD CDC RA Version 1.0 provides direction in the form of principles, business rules, standards and architectural patterns, as is divided into five functional areas: facility infrastructure; computing infrastructure; security/information assurance; capability delivery; and standardized operations and processes. The requirements are aligned with the JIE capability and security architectural guidance. This Thin/Zero Client Computing RA is aligned with the DoD CDC Reference Architecture.

2.1.3 **Joint Information Environment (JIE)**

The JIE is a secure environment comprised of shared information technology infrastructure, enterprise services, and a single security architecture to achieve full spectrum superiority, improved mission effectiveness, increased security and the realization of IT efficiencies. JIE is operated and managed in accordance with the Unified Command Plan (UCP) using enforceable standards, specifications, and common tactics, techniques and procedures (TTPs). This Thin/Zero Client Computing Reference Architecture is aligned with the JIE capabilities framework.

2.1.4 **Common Operating Environment (COE), Oct 2010**

The Army Common Operating Environment architecture is an approved set of computing technologies and standards that enable secure and interoperable applications to be rapidly developed and executed across a variety of Computing Environments, to include Thin/Zero Client Computing. Each computing environment has a minimum standard configuration that supports the Army's ability to quickly produce and deploy high-quality applications, and to reduce the complexities of configuration, support, training and costs associated with the computing environment.

2.1.5 **Unified Capabilities (UC)**

Army Unified Capabilities (UC) is a secure suite of collaboration, real time communications, and supporting services, including e-mail, chat, voice, video, search, collaboration sites, and records management tools that will be available to the Soldier and Army business user on any device, anywhere in the world. Thin/Zero Client Computing end-users must be able to access and effectively utilize Unified Capabilities in support of mission requirements. In addition, Quality of Service (QoS) standards are outlined in the UC Reference Architecture in Appendix H.

2.1.6 **Identity, Credential and Access Management (ICAM)**

ICAM is also a critical service that must be integrated and synchronized with Thin/Zero Client Computing capability; it comprises the following infrastructure and services: Public Key Infrastructure (PKI); Common Access Card (CAC) Services; Claims-Based Authentication; Enterprise Authentication Services; Attribute-Based Access Control (ABAC); Policy Decision Services; Directory Services. The DoD Enterprise Identity Attribute Service (EIAS) serves to distribute DoD person, persona, and personnel attributes to applications and services in a controlled, consistent, and secure manner. The information provided via EIAS can be used to confirm an individual's identity and affiliation to the DoD for the purpose of enabling Attribute-Based Access Control (ABAC). The Defense Manpower Data Center (DMDC) manages EIAS. The hardware and software provided to the end-user for Thin/Zero Client Computing must enable Identity and Access Management services listed above to meet Army security requirements.

2.1.7 Network Boundary Security Top Level Architecture (TLA)

The Army maintains a security enclave boundary that is referred to as the Top Level Architecture. The Army's TLA effort creates the overarching architecture across the Army Enterprise, integrating with the DoD Information Enterprise Architecture and serving as the interface to the Installation Processing Nodes (IPN) and Installation Campus Area Network (ICAN) to afford connectivity to the TLA. The ICAN will be the network interface for connecting the Thin/Zero Client Computing end-users to the back-end applications and data resources. The Security Technical Implementation Guides (STIGs) and the National Security Agency (NSA) Guides are the configuration standards for DoD IA and IA-enabled devices/systems. Since 1998, DISA Field Security Operations (FSO) has played a critical role enhancing the security posture of DoD's security systems by providing the STIGs. The STIGs contain technical guidance to "lock down" information systems/software that might otherwise be vulnerable to a malicious computer attack. DISA FSO is in the process of moving the STIGs towards the use of the National Institute of Standards & Technology (NIST) Security Content Automation Protocol (S-CAP) in order to automate compliance reporting for the STIGs. The solutions providers for the Army Thin/Zero Client Computing implementation on installations must ensure these STIGs are incorporated into their solutions architecture.

2.1.8 Army Data Center Consolidation Plan (ADCCP)

The ADCCP consolidates Army data centers in order to cut operational costs and improve energy efficiency. The CIO/G-6 ADCCP team is designating the Installation Processing Nodes, those data centers that will not be closed or regionally consolidated. These IPNs will host the installation-level data. Virtualization efforts such as Thin/Zero Client Computing will also contribute to the ADCCP objectives by standardizing hardware and software architecture in the Army. The DoD data center consolidation strategy is built around the establishment of Franchised Resilient Core data centers with robust inter-connectivity and global accessibility as outlined in the DoD Core Data Center Reference Architecture. For additional information reference <https://www.us.army.mil/suite/page/643748>.

2.1.9 Installation, Information, Infrastructure, Communications and Capabilities (I3C2)

The Installation Campus Area Network (ICAN) is provisioned through the Installation, Information, Infrastructure, Communications and Capabilities (I3C2) as a part of the Installation, Information Infrastructure Architecture (I3A), is critical to the success of Thin/Zero Client Computing. A bandwidth analysis will need to be completed at each installation to determine adequacy. I3C2 is planning to upgrade ICAN infrastructure to provision additional bandwidth at selected installations for Thin/Zero Client Computing implementation.

2.1.10 Network Operations (NetOps)

NetOps establishes, operates, manages, protects, and defends the LandWarNet. NetOps consists of three core functions: Network Management/Enterprise Service Management (NM/ESM), Information Assurance/Computer Network Defense (IA/CND), and Information Dissemination Management/Content Staging (IDM/CS). These crucial functions guide Signal entities in the installation, management, and protection of communications networks and information services necessary to directly support both generating and operating forces. NetOps provides the Commander/users, at all levels, with end-to-end network and information system visibility, protection, and priority of timely information delivery. Thin/Zero Client Computing will enhance network operations by enabling centralized management of software and hardware,

patch management, data storage management and bandwidth optimization. The implementation of Thin/Zero Client Computing must be designed to accommodate the suite of Network Operations (NetOps) tools being deployed by the Army and DoD.

2.2 DoD Information Enterprise Architecture Capabilities Line of Sight

This architecture reflects the interrelationships of the Capabilities Line-of-Sight (Figure 4) as depicted in the DoD IEA framework and the associated Department of Defense Architecture Framework (DoDAF) standards. The framework vertically aligns required IE capabilities, activities, functions (systems), services to solutions and delivered Enterprise capabilities, and horizontally connecting principles and business rules to technical standards that guide and constrain the development of solutions. The Capabilities include Doctrine, Organization, Training, Material, Personnel, Leadership and education, and Facilities (DOTMLPF) impacts. In this Thin/Zero Client Computing RA, principles/rules are established and supported by the related technical standards providing the guidelines and constraints for the development of the solutions architectures and implementation plans that will deliver the Thin/Zero Client Computing capabilities to the Army.

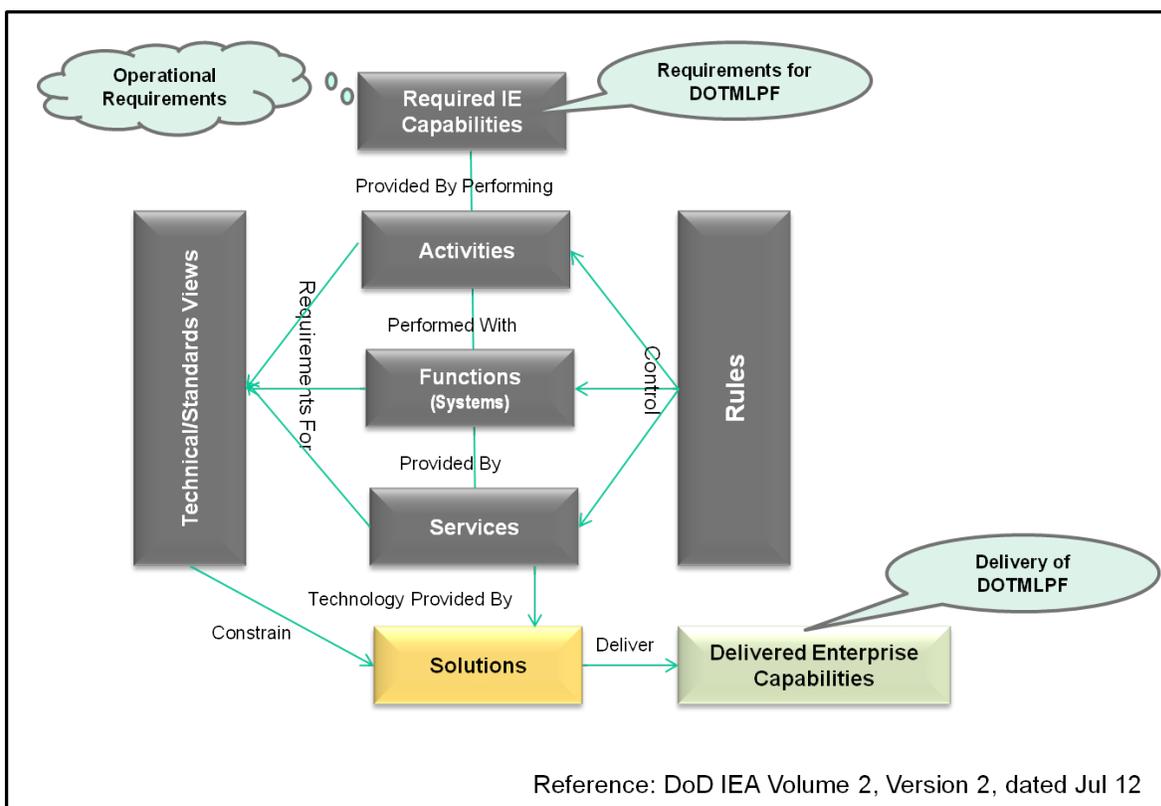


Figure 4: Information Enterprise Architecture Capabilities Line of Sight

2.3 Army Thin/Zero Client Computing Reference Architecture Inputs, Processes and Outputs (Figure 5)

This Thin/Zero Client Computing Reference Architecture is the Army's authoritative source of information to guide and constrain related architectures and solutions to create an Army Enterprise Thin/Zero Client Computing Environment as depicted in Figure 5 on the following

page. The RA establishes Principles that are high-level statements that tie back to the Business/Warfighting Concept of Operations (CONOPS) and Requirements. Supporting Business Rules provide definitive statements to be used as design tenets; they also constrain the implementation of the principles and associated policies, and provide acquisition guidance. The systems architect develops and conducts conformance tests on solution(s) and develops the products list for approval by the Army CIO/G-6. For more information on principles and business rules descriptions refer to the Glossary section of this document.

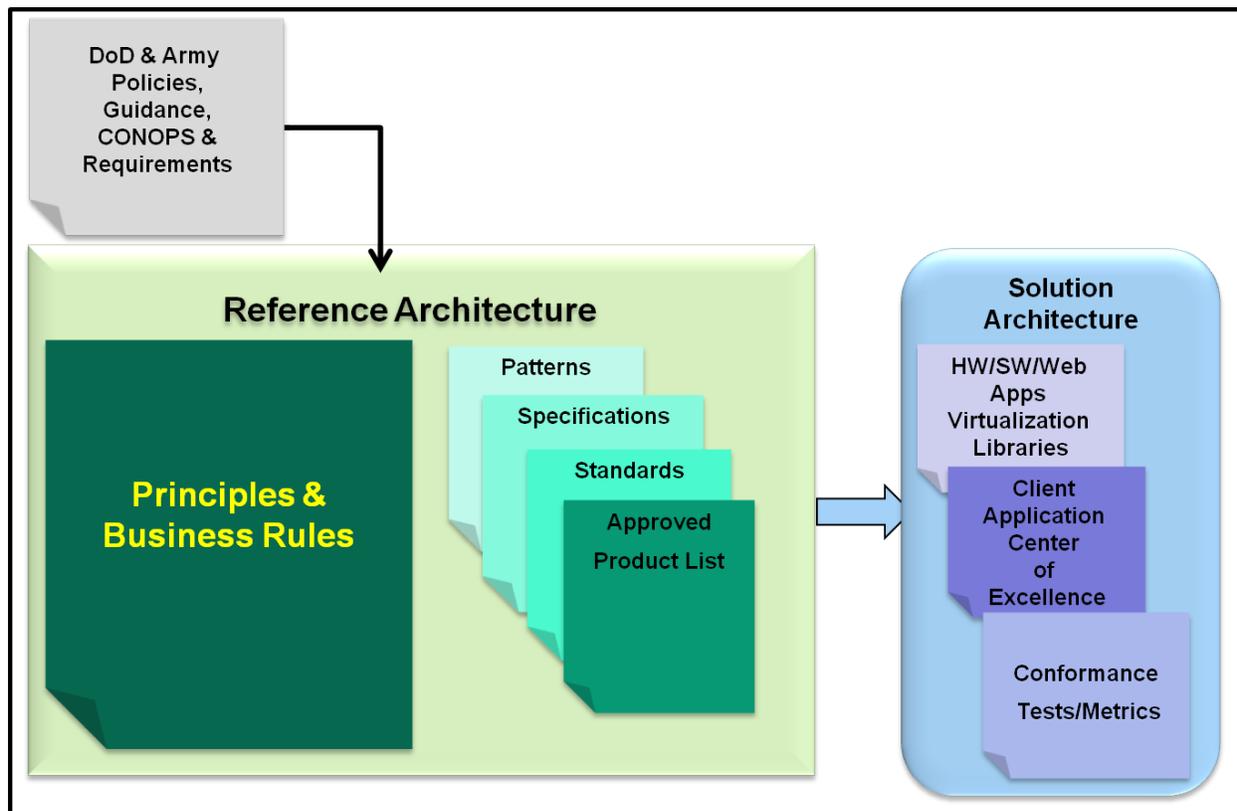


Figure 5: Reference Architecture Inputs, Processes and Outputs

3 Thin/Zero Client Computing Reference Architecture Components

3.1 Operational Capabilities Model Overview

The Army Thin/Zero Client Computing capability requirements are the basis for providing Army stakeholders with enterprise-level technical direction for the implementation of a standardized Computing environment. These Army capabilities are derived from the approved Requirements Document. Figure 6 depicts the DoD IEA and Core Data Center high-level capabilities and the alignment of Army Thin/Zero Client Computing capability requirements.

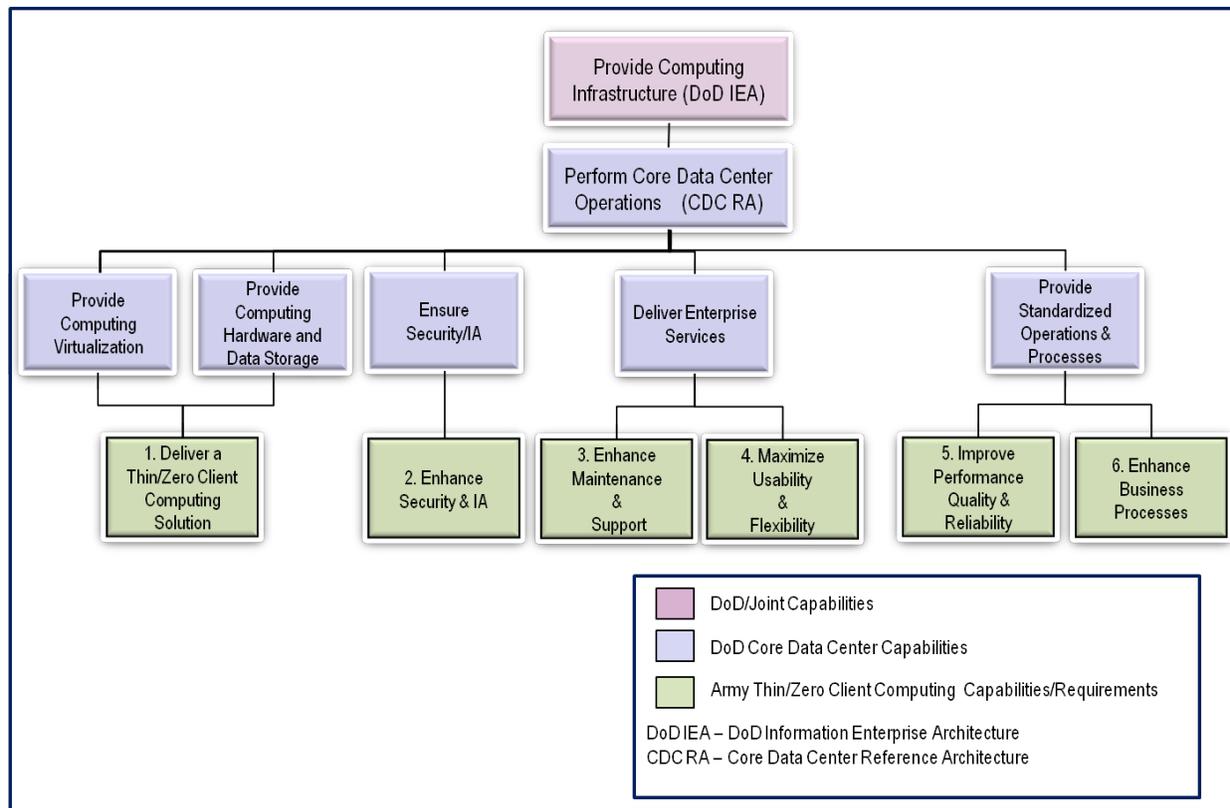


Figure 6: Thin/Zero Client Computing Capabilities Alignment to DoD IEA

3.2 Operational Activities Model Overview

Figure 7, the Operational Activities Model describes the operations that are normally conducted in the course of achieving Army Thin/Zero Client Computing mission or business goal, and describe operational activities (or tasks) that are being conducted with the mission area. The diagram, as depicted in Figure 7 below, will be used to:

- Clearly delineate lines of responsibility for Army Thin/Zero Client Computing activities.
- Uncover unnecessary operational activity redundancy.
- Make decisions about streamlining, combining, or omitting activities.
- Define or flag issues, opportunities, or operational activities and their interactions that need to be analyzed further.
- Provides a necessary foundation for depicting activity sequencing and timing in the Principles and Business Rules as described in Tables 1-6.

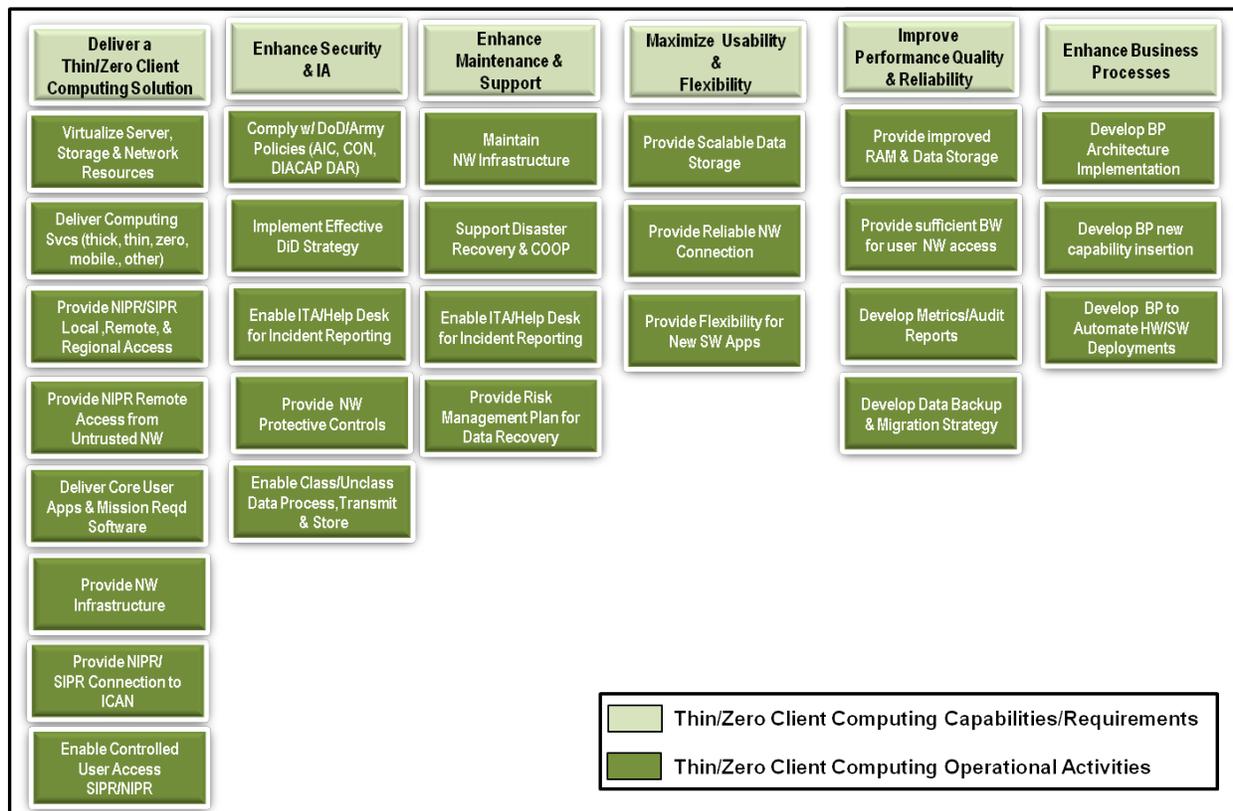


Figure 7: Thin/Zero Client Operational Activities Alignment with Capabilities

3.3 Virtualization - Joint Information Environment (JIE) Alignment

Increased reliance on a common set of virtualized services and capabilities, provided through a joint information infrastructure, will provide greater effectiveness and efficiency in executing the vision for the Army enterprise. Thin/Zero Client Computing capabilities enable the Army user through the establishment and control of processes, procedures, and capabilities to enhance:

- Connecting to the enterprise network anywhere, using the various end-user devices available to Army personnel and mission partners.
- Accessing information, services, and other information assets when needed, using various end-user devices available to Army personnel and mission partners.
- Sharing information and services throughout the Army enterprise, and providing global visibility and availability of information, services, and other information assets.

Enabling capabilities optimize the end-user capabilities described above by creating governance processes, policies, and standards relating to end-user capabilities, by ensuring:

- Effective management of network performance and dynamic allocation of enterprise resources.
- Common access control for all users and devices throughout the Army enterprise.
- Cross-domain security and proactive network defense.
- Data security.
- Effective development and use of architecture.

Figure 8 below reflects the Joint Information Environment capabilities and the associated activities (in green) that align to activities related to implementation of Thin/Zero Client Computing solutions. These capabilities will be updated as the JIE effort matures over time.

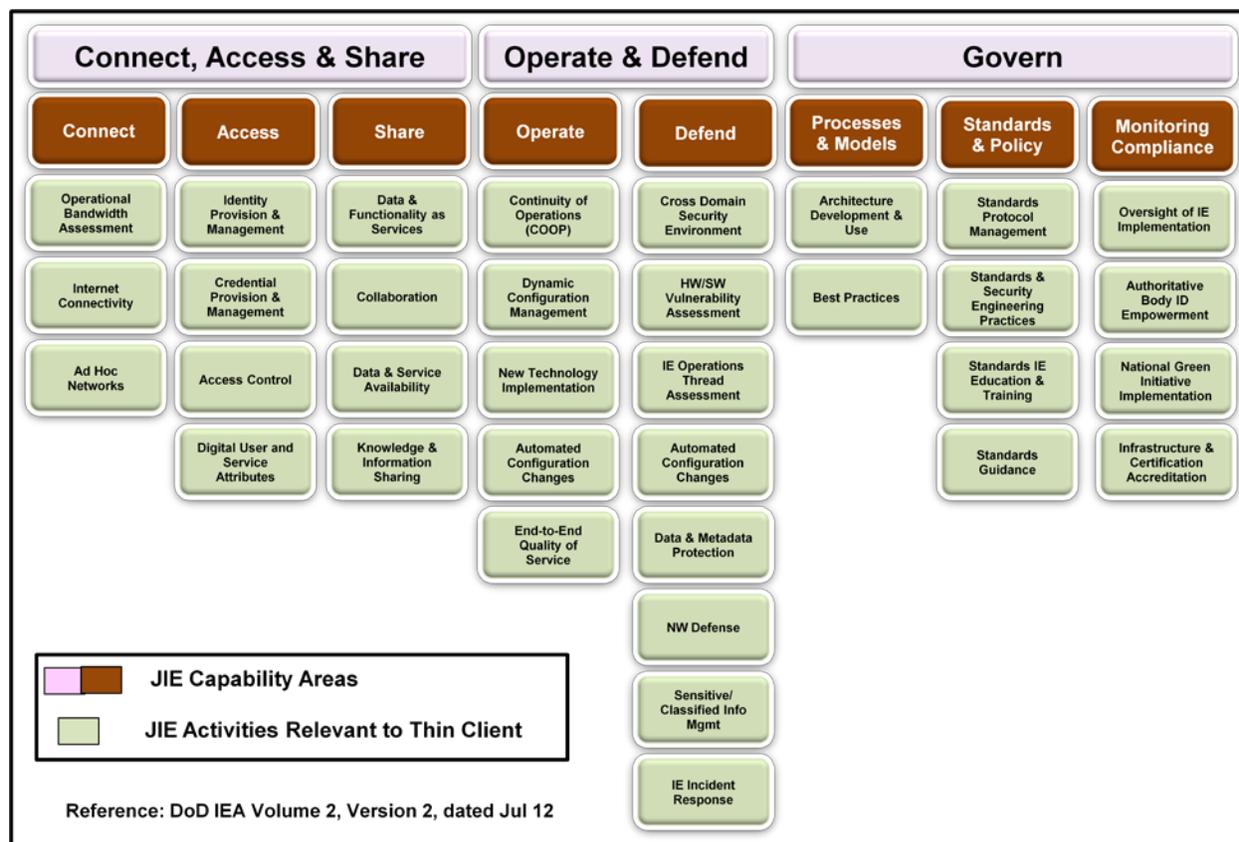


Figure 8: Thin/Zero Client Computing Alignment with JIE Capabilities

3.4 Thin/Zero Client Computing Reference Architecture Principles & Business Rules

Tables 1 thru 6 below reflect the alignment of the Army CIO/G-6 high-level principles and business rules to the DoD IEA Global Principles/Rules, as published in DoD IEA, Volume 2. The tables further associate Army Principles and Business Rules with supporting Technical Positions and Patterns to guide and constrain subsequent architectures, and to further decompose the Army Thin/Zero Client Computing principles and rules as reflected in Tables 1-6. The Tables represent the following major capabilities/operational activities derived from the Thin/Zero Client Computing Requirements Document:

- Deliver a Thin/Zero Client Solution.
- Enhance Security and Information Assurance.
- Enhance Maintenance and Support.
- Maximize Usability and Flexibility.
- Improve Performance Quality and Reliability.
- Enhance Business Processes.

These Thin/Zero Client Computing RA rules and technical standards will guide the Thin/Zero Client Computing solutions architecture technologies. The Thin/Zero Client Computing technical positions/standards can be organized into certain patterns as listed below. These patterns provide the framework for the technical standards presented in Appendix A (Standards View).

- Virtualization of Resources (e.g., OSs, Hardware (HW), storage, and Central Processing Unit (CPU) capacities).
- Application Formats and Protocols.
- Operating Systems.
- Storage.
- Databases.
- Information Assurance.
- Network Perimeter Protection (e.g., Firewalls, Intrusion Detection/Prevention).
- Network Interfaces (e.g., Internet Protocol (IP) routers, Local Area Network (LAN) switches).
- Transport Network (e.g., Synchronous Optical Networking [SONET], Fiber).
- Virtual Private Networks (VPNs) (e.g. Virtual Local Area Network (VLAN), Internet Protocol/Multi-Protocol Label Switching (IP/MPLS), Border Gateway Protocol (BGP), Virtual Private Network (VPN)).
- Quality of Services (QoS).
- Network Management/Operations.

Patterns: A pattern is a set of practices that considers business process and usability, mission-oriented application of guiding principles, and the supporting business rules. The following are the basic patterns relating to this Thin/Zero Client Computing Reference Architecture: DoD IEA, DoDAF, Business Process Models, and emerging industry capabilities such as: Remote Desktop Protocol (RDP), Microsoft solution, Independent Computing Architecture (ICA), Citrix solution, Remote Graphics Software (RGS), HP solution, SPICE, Red Hat solution, Personal Computer over Internet Protocol (PCoIP) and VMware solution.

3.5 Capability 1: Deliver an Army Thin/Zero Client Computing Solution.

DoD IEA Principles & Business Rules Abbreviations:

- GP – Global Principles
- SIP – Shared Infrastructure Principles
- SIR – Shared Infrastructure Business Rules
- CIRP – Computing Infrastructure Readiness Principles
- CIRR – Computing Infrastructure Readiness Rules
- OPR – Derived Operational Rules
- SAR – Shared Availability Rules
- CIRBR – Computing Infrastructure Readiness Business Rules

Table 1: Deliver an Army Thin/Zero Client Computing Solution Principles and Business Rules Mapped to DoD IEA

DoD IEA 2.0 Capabilities	DoD IEA 2.0 Principle/Business Rules	Army Thin/Zero Client Computing Principles (PR)	Business Rules (BR)	Technical Positions
Data & Services Availability	SIR 01 – Global Information Grid (GIG) infrastructure resources shall be discoverable, and available to both meet the dynamic demand of all mission requirements and support the monitoring and management of the GIG.	PR 1 - Thin/Zero Client Computing will be designed to deliver computing services for all end-users (thick, thin, zero, mobile) to meet mission requirements and will not adversely affect existing operations, systems or missions.	BR 1.1 Thin/Zero Client Computing will provide virtualization of server, storage, and networking resources by placing computing devices, operating systems, and applications on servers in the data center using open, standards-based, architecture in accordance with (IAW) DoD/Joint & Army requirements.	Thin-Client Back-End Solutions fall into one of the categories: a) Terminal Services; e.g., MS Remote Desktop Service b) Streaming OS/Applications c) Virtual Desktops All OSs, HW, CPU capacities, storage, and applications resources of servers and clients of Thin/Zero Client Computing will be available and discoverable (e.g. Universal Description, Discovery and Integration or UDDI) when needed by missions, managed and monitored dynamically using open technical standards (e.g. Open Virtualization Format or OVF, Simple Network Management Protocol or SNMP).
		PR 1 - Thin/Zero Client Computing will be designed to deliver computing services for all end-users (thick, thin, zero, mobile) to meet mission requirements and will not adversely affect existing operations, systems or missions.	BR 1.2 The Thin/Zero Client Computing enterprise solution will be scalable to support 100% of SIPRNet users and 80% of NIPRNet users.	Reference: Army Installation Quality of Service (QoS) Reference Architecture.
		PR 1 - Thin/Zero Client Computing will be designed to deliver computing services for all end-users (thick, thin, zero, mobile) to meet mission requirements and will not adversely affect	BR 1.3 Power users must be provisioned to support mission requirement; e.g., streaming media, Defense Connect Online (DCO), bi-directional	Reference: Thin/Zero Client Computing Requirements Document Appendix B Definitions of User Types.

DoD IEA 2.0 Capabilities	DoD IEA 2.0 Principle/Business Rules	Army Thin/Zero Client Computing Principles (PR)	Business Rules (BR)	Technical Positions
		existing operations, systems or missions.	audio and video, etc., by providing proper engineering configuration for acceptable performance or determining criteria for remaining on a thick client solution.	
Information Sharing with Mission Partners	OPR 09 - Edge users have direct information sharing capabilities with peers in an outside their immediate organization, with central processing for their mission, and with strategic assets per their mission requirements.	PR 1 - Thin/Zero Client Computing will be designed to deliver computing services for all end-users (thick, thin, zero, mobile) to meet mission requirements and will not adversely affect existing operations, systems or missions.	BR 1.4 Thin/Zero Client Computing will deliver core user applications to the end-user at the same (or improved) level of performance and usability as that level provided by the status quo thick client computing environment. These capabilities will include ability to support video, data, and audio.(QoS).	Thin/Zero Client Computing is enhancing performances and usability of client-server computing environments through dynamic sharing of resources on-demand basis using open and market-based standards without being locked into specific resources (e.g. ,OSs, HW, Software (SW), storage, CPU capacities) of certain vendors that are statically allocated in non-interoperable environments.
		PR 1 - Thin/Zero Client Computing will be designed to deliver computing services for all end-users (thick, thin, zero, mobile) to meet mission requirements and will not adversely affect existing operations, systems or missions.	BR 1.5 Thin/Zero Client Computing will be supported with a network infrastructure that is capable of migrating all system users' data and providing users with simultaneous access from each building or facility where users perform their desktop computing.	Open standards-based protocols (e.g. IP, Ethernet LAN) will be used for ICAN connectivity to both client and server-side.
Data & Services Availability	CIRR 06 - Shared computing and data storage resources shall be capable of being discoverable and accessible for virtual management and control across the GIG.	PR 1 - Thin/Zero Client Computing will be designed to deliver computing services for all end-users (thick, thin, zero, mobile) to meet mission requirements and will not adversely affect existing operations, systems or missions.	BR 1.6 Provide the capability for remote users operating on thick, thin/zero, or other clients on trusted or un-trusted networks to access data and applications and meet DoD/Army security requirements.	Thin/Zero Client Computing resources (e.g., OSs, HW, CPU capacities, storage, and application SW) of clients and servers will be discoverable using open and common standards and repositories (e.g., UDDI) in open standards-based secured (e.g., American National Standards Institute (ANSI) X.509, Framework for Implementing Files Systems (FIFS) 201, CAC, DoD Instruction (DoDI) 8520.03) environments.
Data & Functionality as Services	GP01- DoD CIO-governed resources are conceived, designed, operated, and managed to address the mission needs of the Department.	PR 1 - Thin/Zero Client Computing will be designed to deliver computing services for all end-users (thick, thin, zero, mobile) to meet mission requirements and will not adversely affect existing operations, systems or missions.	BR 1.7 Thin/Zero Client Computing will support all standard software included in the AGM baseline and all validated above baseline software required by the mission.	Market-based Thin/Zero Client Computing technical standards (e.g., VMware, Radio Data System (RDS), Remote Desktop Protocol (RDP), Independent Computing Architecture (ICA, Remote Graphics Software (RGS), SPICE, PCoIP) related to OSs, HW, CPU capacities, storage, and applications of servers and clients that will be a part of

DoD IEA 2.0 Capabilities	DoD IEA 2.0 Principle/Business Rules	Army Thin/Zero Client Computing Principles (PR)	Business Rules (BR)	Technical Positions
				the Army Gold Master (AGM) are needed by missions for enhancing reliability, security, interoperability, and economies-of-scale through virtualization of the computing environments.
		PR 1 - Thin/Zero Client Computing will be designed to deliver computing services for all end-users (thick, thin, zero, mobile) to meet mission requirements and will not adversely affect existing operations, systems or missions.	BR 1.8 Provide and allocate sufficient Random Access Memory (RAM) to enable user productivity at the same level as enabled by the status quo thick client computing environment.	The PM will determine systems requirements to meet performance criteria
		PR 1 - Thin/Zero Client Computing will be designed to deliver computing services for all end-users (thick, thin, zero, mobile) to meet mission requirements and will not adversely affect existing operations, systems or missions.	BR 1.9 Support approved peripherals attached locally to the client device (e.g., via Universal Serial Bus (USB), to include printers, CAC readers, scanners, and multifunction devices.	All thin-client solutions must support common applications, including: -CAC authentication to Active Directory (login) -CAC-enabled web server login, email signing and encryption - Defense Travel System (DTS)
		PR 1 - Thin/Zero Client Computing will be designed to deliver computing services for all end-users (thick, thin, zero, mobile) to meet mission requirements and will not adversely affect existing operations, systems or missions.	BR 1.10 Support networked services, to include printers, scanners, multifunction devices, and data storage.	
HW/SW Vulnerability Assessment IE Operational Threat Assessments	SAR 05 - GIG assets must establish and implement a Mission Assurance capability that addresses hardware, software and supplier assurance through engineering and vulnerability assessments.	PR 1 - The capability will not adversely affect existing operations, systems, and missions.	BR 1.11 When migrating to Thin/Zero Client Computing, the PM will install the system and migrate users to the system with minimal impact to operations and mission objectives, to include back-up of user data prior to user migration.	Thin/Zero Client Computing will be based on open and market standards (e.g., VMware, RDS, RDP, ICA, RGS, SPICE, PCoIP) and will provide interoperability between heterogeneous OSs, HW, SW, and storage networks through virtualization, facilitating the graceful migration of the existing systems to new ones.
Identity & Provision Management	SAR 07 – All DoD information services and applications must uniquely and persistently digitally identify and authenticate users and devices. These services, applications, and networks shall enforce authorized access to information and other services or devices according to specified	PR 2 - Thin/Zero Client Computing will provide controlled user access to the NIPRNet and SIPRNet to meet mission requirements.	BR 2.1 Thin/Zero Client Computing solutions will comply with Army ICAM requirements for controlled access to NIPRNet and SIPRNet. For more information see ICAM Reference Architecture.	A market-based Thin/Zero Client Computing storage virtualization standard will be a part of AGM, and will have firewall, intrusion detection/prevention system (IDS/IPS) in SIPRNet/NIPRNet environments, and will allocate storage dynamically on an on-demand basis.

DoD IEA 2.0 Capabilities	DoD IEA 2.0 Principle/Business Rules	Army Thin/Zero Client Computing Principles (PR)	Business Rules (BR)	Technical Positions
	access control rules and quality of protection requirements for all individuals, organizations, Chief Information Officers (CIOs), automated services and devices.			
Automated Configuration Changes	SAR 10 - DoD program should ensure that configuration changes to networks, data assets, services, applications, and device settings can be automatically disseminated and implemented in conformance with GIG-standard configuration processes.	PR 3 - Enable the Army regional construct (e.g., Theater Network Operations and Security Center or TNOSC) to quickly deploy new capabilities while centrally managing controls and configurations.	BR 3.1 Configuration management of the system shall allow change requests for each system to be channeled through standard Command structures.	
Standard Protocol Management	<p>OPR 24 - Develop common standards and policies that serve as enforcement mechanisms to ensure interoperability.</p> <p>OPR 26 - Develop a common set of functional policies so that all components of each IE program or system are developed, tested, certified and deployed with an emphasis on end-to-enterprise commonality.</p>	PR 4 - Thin/Zero Client Computing planning and implementation must synchronize with other Army/DoD/Federal IT initiatives to insure interoperability, compatibility and compliance.	BR 4.1 The system will not impede Army compatibility and compliance with Army, DoD, and Federal IT initiatives described in paragraph 2.1.	Virtual environments created by Thin/Zero Client Computing will be based on open and market standards (e.g., VMware, RDS, RDP, ICA, RGS, SPICE, PCoIP).

Table 1: Deliver Thin/Zero Client Computing Requirements

3.5.1 Deliver Thin/Zero Client Computing Environment Facts and Assumptions

- Mission success is the first priority.
- This Reference Architecture provides for commonality as the default; uniqueness is allowed, but only when it is essential for mission success and approved within the established governance process.
- The Army will operate in an Enterprise Environment IAW the DoD/JIE guiding principles.
- The Thin/Zero Client Computing Environment will maximize utilization of on-going Army virtualization efforts.
- The Installation Campus Area Network will enable the Thin/Zero Client Computing capability.
- Virtualization will contribute to interoperability as common infrastructure, repositories, registries, and standard security solutions are achieved.
- The Thin/Zero Client Computing solution will support clients running Microsoft Windows OS.

3.5.2 Deliver Thin/Zero Client Computing Environment Constraints

- The Traditional Thick-client common peripherals (e.g., DVD(Digital Video Disk) ROM/RW (Read Only Memory/Read and Write) Compact Disc (CD), ROM/RW, digital scanner, etc.) must be provided separately as stand-alone units as required by the mission. (Note: The Army must adhere to the USB Moratorium, and must replace legacy printers with parallel technology.)
- The Army must provide training to all users.
- Applications running on the thin client environment will drive the choice of Link/Display Protocols (e.g., Remote Desktop Protocol, Independent Computing Architecture, and Remote Graphics Software) and will determine the choice of OS.
- Local processing power necessitates more intensive monitoring to prevent users from circumventing security controls. Thin/Zero client solutions implemented on thick-client, end-user devices must limit the user's ability to operate in its full-capacity operating system (e.g., complete Windows Vista, Linux, etc.) when connected to the network.
- Thin/Zero Client Computing infrastructure and clients must be compatible and operate within Army Network Operations tool functionality (i.e., discovery, monitoring, management, etc.).
- Thin client solutions outside of the Post, Camp, and Station (P/C/S) must utilize a proxy in the Demilitarized Zone (DMZ).
- Thin-client solutions that implement a Terminal Server Infrastructure need to support Remote Desktop Protocol (RDP), or the Independent Computing Architecture (ICA) protocol to allow connection to a Terminal Server.
- If the thin-client device is running on MS OS, it must emulate the desktop Army Golden Master as listed for the Windows Baseline Software Configuration, NETCOM Technical Authority 2003-005c Army Enterprise Desktop Standardization, 13 Sep 06, MS based computing.
- Thin client solutions must be in compliance with Executive Order 13423, Electronic Product Environmental Asset Tool (EPEAT) requirements. Reference Section 2, h. For more info: <http://www.epa.gov/oaintrnt/practices/eo13423.htm>. TA 2010-001, 10 Sep 2010, pg 9, 4.3-a.

- Army solutions must be compatible and enable the operations of Host Based Security System (HBSS) components. Note: Detailed information on HBSS is available at: <https://www.intelink.gov/wiki/Hbss> and NetOps Architecture requirements.

3.5.3 Deliver Thin/Zero Client Computing Environment Operational Risks

- **Risk Area: Network Reliance** – I3C2, ICAN upgrades, outages, etc., can impact mission functions if customers lose access to the network. In a virtual environment, loss of connectivity to the network impacts many users' ability to access applications and data, unlike a thick-client user who can do limited work using the off-line capabilities of the thick client device.
- **Mitigation:** Design Thin/Zero Client Computing solutions to increase reliability and availability of the network through ICAN upgrades, and implementation of COOP and Disaster Recovery capabilities.
- **Risk Area: Cost** – Near-term centralized cost by seat in a standardized Thin/Zero Client Computing implementation, with COOP and DR infrastructure requirements, will be higher than the status quo.
- **Mitigation:** Validate assumptions and conduct site surveys to get more accurate assessment of the current infrastructure & computing environment.
- **Risk Area: Testing** – Testing of the objective solution outside of the government computing environment would be inadequate.
- **Mitigation:** Ensure testing of objective solutions for each installation is done in a government testing environment, and not solely in a contractor facility.
- **Risk Area: Change Management** – This is a significant change for users and, if not properly communicated to them in a positive way, will contribute to issues during the implementation.
- **Mitigation:** The Army should develop and implement a plan for strategic communications and change management to communicate the importance of Thin/Zero Client Computing to end-users.
- **Risk Area: Power User Inadequate Performance** (power usage is characterized by video or heavy graphics; complex, rapid screen rolling, as in large Excel spreadsheets, etc.); even with high-speed networks and local connections, power users will likely not get the same level of service as they are experiencing with a thick-client solution.
- **Mitigation:** Create a criteria baseline, based on the end-users' mission requirements, to determine if they are candidates for migration from a thick client to Thin/Zero Client Computing. Test power user requirements to determine the parameters for users classified as power users, versus others.

3.6 Capability 2: Enhance Security and Information Assurance

Table 2: Enhance Security and Information Assurance Principles and Business Rules Mapped to DoD IEA

DoD IEA 2.0 Capabilities	DoD IEA 2.0 Principle/Business Rules	Army Thin/Zero Client Computing Principles (PR)	Business Rules (BR)	Technical Positions
Standards Guidance	GP 05 - The GIG will provide a secure environment for the collaborative sharing of information assets (information, services, and policies) with DoD's external partners, including other Federal Departments and Communities of Interest (e.g., Department of Homeland Security, the Intelligence Community), state and local governments, allied, coalition, non-governmental organizations (NGOs), academic, research, and business partners.	PR 5 - The Army will ensure compliance with DoD Directives and accreditation requirements through the implementation of an effective Defense-in-Depth (DiD) strategy and enforcement of IA strategies that provide Protection, Detection, Reaction, and Restoration (PDRR) capabilities.	BR 5.1 Meet the Information Assurance controls and requirements specified in DoD Directive 8500.01 and DoD Instruction 8500.02 and Army Regulation (AR) 25-2 based on Mission Assurance Category (MAC) level and sensitivity level.	Virtual environments created by Thin/Zero Client Computing will be based on market standards (e.g., VMware, RDS, RDP, ICA, RGS, SPICE, PColP) that provide server-based centralized configuration control of OSs, HW and SW. Thin/Zero Client Computing security will use the ICAM RA technical standards (e.g., ANSI X.509, FIPS 201, CAC, DoDI 8520.03).
		PR 5 - The Army will ensure compliance with DoD Directives and accreditation requirements through the implementation of an effective Defense-in-Depth (DiD) strategy and enforcement of IA strategies that provide Protection, Detection, Reaction, and Restoration (PDRR) capabilities.	BR 5.2 For connecting to the SIPRNet, multi-level security, Cross Domain Solution (CDS) adhere to requirements outlined at: http://disa.mil/connect/classified/index.html and allow single level secure cross domain connectivity (e.g., NIPRNet to the DREN (Defense Research and Engineering Network)).	DISA's Cross Domain Enterprise Services (CDES) provide support to Combatant Commands, Services, and Agencies by implementing, fielding, and providing lifecycle support for cross-domain solution technologies that provide secure, interoperable capabilities throughout the Department of Defense. In addition, Thin/Zero Client Computing will adhere to Cross Domain Solution per SIPRNet IA requirements.
		PR 5 - The Army will ensure compliance with DoD Directives and accreditation requirements through the implementation of an effective Defense-in-Depth (DiD) strategy and enforcement of IA strategies that provide Protection, Detection, Reaction, and Restoration (PDRR) capabilities.	BR 5.3 Comply with Army Data at Rest (DAR) requirements and all applicable DoD and Army security policies and regulations.	
		PR 5 - The Army will ensure compliance with DoD Directives and accreditation	BR 5.4 Communications Security (COMSEC) handling procedures	AR 380-40.

DoD IEA 2.0 Capabilities	DoD IEA 2.0 Principle/Business Rules	Army Thin/Zero Client Computing Principles (PR)	Business Rules (BR)	Technical Positions
		requirements through the implementation of an effective Defense-in-Depth (DiD) strategy and enforcement of IA strategies that provide Protection, Detection, Reaction, and Restoration (PDRR) capabilities.	related to thin/zero clients must meet the requirements of AR 380-40.	
Oversight of Information Enterprise (IE) Implementation	OPR 23 - Develop enterprise acquisition and certification to ensure IE components are purchased and acquired so they are interoperable and universally certified.	PR 6 - Be accredited through the Department of Defense Information Assurance Certification and Accreditation Process (DIACAP).	BR 6.1 The capability solution will be compliant with the applicable Army and DoD Approved Products List (APL).	Thin/Zero Client Computing products will be compliant to open and market-based technical standards (e.g., RDS, RDP, ICA, RGS, SPICE, PCoIP, ANSI X.509, FIFS 201, CAC, DODI 8520.03) that are the part of the Army and DoD Approved Products List.
		PR 6 - Be accredited through the Department of Defense Information Assurance Certification and Accreditation Process (DIACAP).	BR 6.2 Operate using only software with an approved Certificate of Networthiness (CON).	Thin/Zero Client Computing market-based virtualization technical standards as a part of AGM, and open standards-based IA being a part of DISA, will facilitate operations within the Army and DoD IA Framework, including validation through a standard security engineering process.
Identity Provision & Management	SAR 07 - All DoD information services and applications must uniquely and persistently digitally identify and authenticate users and devices. The services, applications, and networks shall enforce authorized access to information and other services or devices according to specified access control rules and quality of protection requirements for all individuals, organizations, Communities of Interest (COIs), automated services, and devices.	PR 6 - Be accredited through the Department of Defense Information Assurance Certification and Accreditation Process (DIACAP).	BR 6.3 Provide the capability to block restricted users from storing data to a client device, and it shall have the capability for the OS and sensitive data to be removed entirely from the device when powered down. As a result, the system shall allow users to openly store client devices when not in use without violating Army IA policy.	
Cyber Security Policy Compliance & Standard Engineering Practices IAW System of Systems Engineering (SoSE) guidelines	SAR 09 - DoD programs must demonstrate that their network, data assets, services, and applications, and device settings that control or enable IA functionality have been established, documented, and validated through a standard security engineering process.	PR 6 - Be accredited through the Department of Defense Information Assurance Certification and Accreditation Process (DIACAP).	BR 6.4 The capability will be considered critical and must have the appropriate physical security protective measures.	Thin/Zero Client Computing market-based virtualization technical standards being a part of AGM, and open standards-based IA being a part of DISA will ensure operations within the Army and DoD IA Framework include validation through a standard security engineering process.
		PR 6 - Be accredited	BR 6.5 The solution will	

DoD IEA 2.0 Capabilities	DoD IEA 2.0 Principle/Business Rules	Army Thin/Zero Client Computing Principles (PR)	Business Rules (BR)	Technical Positions
		through the Department of Defense Information Assurance Certification and Accreditation Process (DIACAP).	restrict access to the virtualization management system to authorized administrators.	
Standard Guidance	SAR 02 - GIG infrastructure, applications and services, network resources, enclaves, and boundaries shall be capable of being configured and operated in accordance with applicable policy. Such policy must address differences in enterprise-wide, system high, community of interest, enclave, and operational mission needs.	PR 6 - Be accredited through the Department of Defense Information Assurance Certification and Accreditation Process (DIACAP).	BR 6.6 Support data protection and encryption, network security and segmentation, host operating systems check, host security scanning, isolation control, remote access security, business continuity, disaster recovery planning, security policy updates, virtual desktop hardening, and virtual desktop access control.	Thin/Zero Client Computing technical standards facilitate implementing client-server-based computing architecture, where all virtualization services are controlled from the centralized servers located in the data centers. As a result, the servers/data centers can be distributed in different enclaves. Different configuration control and security policies can be implemented at different boundaries in meeting mission objectives, because all open- and market- technical standards-based Thin/Zero Client Computing virtualization services are transparent to these policies.
Cross Domain Security Enforcement	SAR 01 - DoD information programs, applications, and computer networks shall protect data in transit and at rest according to their confidentiality level, Mission Assurance Category, and level of exposure.	PR 6 - Be accredited through the Department of Defense Information Assurance Certification and Accreditation Process (DIACAP).	BR 6.7 Enable the user to transmit, store, and process classified data, and must provide protective controls commensurate with the network's level of classification.	Thin/Zero Client Computing IA technical standards will support cross domain solutions (CDS), protecting data in transit and at rest according to their confidentiality level, Mission Assurance category, and level of exposure.
Identity Provisioning & Management	SAR 07 - All DoD information services and applications must uniquely and persistently digitally identify and authenticate users and devices. The services, applications, and networks shall enforce authorized access to information and other services or devices according to specified access control rules and quality of protection requirements for all individuals, organizations, COIs, automated services, and devices.	PR 6 - Be accredited through the Department of Defense Information Assurance Certification and Accreditation Process (DIACAP).	BR 6.8 The capability will support CAC/Public Key Infrastructure (PKI) and Secure Token, via interface internal or external to the client device.	Thin/Zero Client Computing IA architecture support ICAM RA technical standards, supporting CAC/PKI and Secure Token, via interface internal or external to the client device. Core standards: - Federal Information Processing Standards (FIPS) 201 compliance - ANSI X.509 compliance
Infrastructure Certification & Accreditation	SAR 09 - DoD programs must demonstrate that their network, data assets, services, and applications, and device settings that control or enable IA functionality	PR 7 – Ensure that network, data connections and end-user devices are compliant with IA requirements and have been validated through a standard	BR 7.1 Ensure and document Engineering Acceptance Documents security configurations in addition to AGM security guidelines IAW STIGs and NSA security	Thin/Zero Client Computing market-based virtualization technical standards, as a part of AGM, and open standards-based IA as a part of DISA, will facilitate Army and DoD C&A.

DoD IEA 2.0 Capabilities	DoD IEA 2.0 Principle/Business Rules	Army Thin/Zero Client Computing Principles (PR)	Business Rules (BR)	Technical Positions
	have been established, documented, and validated through a standard security engineering process.	security engineering process.	guidelines.	
Identity Provisioning & Management	SAR 07 - All DoD information services and applications must uniquely and persistently digitally identify and authenticate users and devices. The services, applications, and networks shall enforce authorized access to information and other services or devices according to specified access control rules and quality of protection requirements for all individuals, organizations, COIs, automated services, and devices.	PR 8 – End-users must uniquely and persistently digitally identify and authenticate users and devices IAW Army IA policies and ICAM reference architecture requirements.	BR 8.1 Support required PKI middleware.	Thin/Zero Client Computing IA architecture support ICAM RA technical standards including PKI middleware. Core standards: - FIPS 201 compliance - ANSI X.509 compliance
		PR 8 – End-users must uniquely and persistently digitally identify and authenticate users and devices IAW Army IA policies and ICAM reference architecture requirements.	BR 8.2 Support authentication to the NIPRNet and SIPRNet.	- DODI 8520.03 establishes and defines sensitivity level for purpose of determining appropriate authentication methods and mechanisms. Core standards: - CAC-based authentication - FIPS 201 compliance - ANSI X.509 compliance
		PR 8 – End-users must uniquely and persistently digitally identify and authenticate users and devices IAW Army IA policies and ICAM reference architecture requirements.	BR 8.3 Provide the capability for a user to sign and encrypt email.	
		PR 8 – End-users must uniquely and persistently digitally identify and authenticate users and devices IAW Army IA policies and ICAM reference architecture requirements.	BR 8.4 Support authentication to PKI enabled websites.	Core Standards: - CAC PKI - Alternate non-CAC PKI
		PR 8 – end-users must uniquely and persistently digitally identify and authenticate users and devices IAW Army IA policies and ICAM reference architecture requirements.	BR 8.5 Support digital signatures and provide the capability for users to digitally sign and encrypt documents.	Core Standards: - International Organization for Standards (ISO)/ International Electrotechnical Commission (IEC) 7816-11:2004 - RSA Labs PKCS #12

DoD IEA 2.0 Capabilities	DoD IEA 2.0 Principle/Business Rules	Army Thin/Zero Client Computing Principles (PR)	Business Rules (BR)	Technical Positions
Cross Domain Security Enforcement	SAR 06 - All DoD services that enable the sharing or transfer of information across multiple security levels shall be centrally planned and coordinated, with proposed service enhancements considered first at the enterprise-wide level, then at the regional/organizational level (e.g., DoD Component), then at the service or application level.	PR 9 - Provide the capability to support the display of multiple security domains/networks via a single user interface (i.e., support future installation of multi-domain solutions).	BR 9.1 Provide the capability to correct the unauthorized transmission of classified data to a lower-classified network (spillage).	Thin/Zero Client Computing IA technical standards (e.g., ICAM RA technical standards) support cross domain solution sharing or transfer of information across multiple security levels (e.g., at the enterprise-wide level, then at the regional/ organizational level). Thin/Zero Client Computing IA technical standards (e.g., ICAM RA technical standards) support cross domain solution , correcting the unauthorized transmission of classified data to a lower-classified network (spillage).

Table 2: Enhance Security and Information Assurance Requirements

3.6.1 Enhance Security and Information Assurance Facts and Assumptions

- 80% of network security compromises occur at the client device.
- Thin/Zero Client Computing will facilitate a more secure network for the Army by providing Information Assurance Vulnerability Alert (IAVA) patch consistency, Containment (Spillage), Data Recovery, and streamlined network management and NetOps (Defend, Detect, and React).
- Compliance with Federal, DoD, and Army Regulations (e.g., mandated Host Based Security System use).
- Thin/Zero Client Computing will increase the potential impact of system compromise, because each user shares computing resources, and therefore infiltration of a single user's system is equivalent to system-wide infiltration.

3.6.2 Enhance Security and Information Assurance Constraints

- Personnel providing system IA procurement/fielding, IA accreditation, and IA support shall meet training and certification requirements identified in DoD Instruction 8500.2 and DoD Regulation 8570.01-M.
- In environments where a Protective Distribution System (PDS) is required to protect the cabling, provisions must be taken to comply with published requirements, references NSTISSI (National Security Telecommunications and Information Systems Security Instruction) No.7003, PDS13 Dec 96, and AR380-27, Control of Compromising Emanation, 19 May 2010.
- Network Ports, Protocols and Services (PPS) must be approved by the Theatre Network Operations & Security Center.
- Network ports for NIPR and SIPR must be allowed by DISA; check the link at: <http://iase.disa.mil/ports/index.html> for the category assurance list and the ports status.

- Local processing power necessitates more intensive monitoring to prevent users from circumventing security controls. A thin client must not operate its full capacity operating system (e.g., complete Windows Vista, Linux etc.).

3.6.3 Enhance Security and Information Assurance Risks

- **Risk Area:** A centralized computing infrastructure increases the impact of a successful cyber attack.
- **Mitigation:** Ensure centralized standardization of NetOps tools and management processes.

3.7 Capability 3: Enhance Maintenance and Support

Table 3: Enhance Maintenance and Support Principles and Business Rules Mapped to DoD IEA

DoD IEA 2.0 Capabilities	DoD IEA 2.0 Principle/Business Rules	Army Thin/Zero Client Computing Principles (PR)	Business Rules (BR)	Technical Positions
Standard Protocol Management	GP 06 -The DoD Information Enterprise (IE) will include global access to common DoD wide capabilities and services that enable access to people and information resources from any computer in the world. To the extent possible, services shall be developed for global use. The use of these globally accessible services will improve warfighting effectiveness, and interoperability, while reducing cost.	PR 10 - Thin/Zero Client Computing platforms, applications, and computing services will interoperate with other similar Army and DoD systems ,and decrease cost and complexity of operations.	BR 10.1 The capability will be suitable for operations and maintenance (O&M) via existing Army O&M policies and processes.	Established technical standards (e.g., OVF, SNMP) will facilitate operations of Thin/Zero Client Computing data assets, services, and applications, and device settings that control or enable IA functionality.
		PR 10 - Thin/Zero Client Computing platforms, applications, and computing services will interoperate with other similar Army and DoD systems, and decrease cost and complexity of operations.	BR 10.2 Enable at least as efficient O&M as the status quo (thick client computing environment)	Cost Benefit Analysis that supports the specific implementation.
Dynamic Configuration Management	CIRR 06 - Shared computing and data storage resources shall be capable of being discoverable and accessible for virtual management and control across the GIG.	PR 10 - Thin/Zero Client Computing platforms, applications, and computing services will interoperate with other similar Army and DoD systems, and decrease cost and complexity of operations.	BR 10.3 Thin/Zero Client Computing will allow for the efficient use of data storage capacity, leveraging vendor tools to implement, manage, support, and sustain service levels.	Thin/Zero Client Computing virtualizes the computing infrastructure resources (e.g., storage, CPU capacities, OSs, HW, SW) including storage using market-based standards (e.g., VMware). All Thin/Zero Client Computing resources, including storage, can be discoverable using technical standards (e.g., UDDI) and can be accessed using IA and other procedures as articulated in the Thin/Zero Client Computing Reference Architecture.
		PR 10 - Thin/Zero Client Computing platforms, applications, and computing services will interoperate with other similar Army and DoD systems and decrease cost and complexity of operations.	BR 10.4 Thin/Zero Client Computing will establish virtual application libraries, allowing for Army-wide release management of applications and for synchronization among libraries.	
		PR 10 - Thin/Zero Client Computing platforms, applications, and computing	BR 10.5 Support the use of thin client devices with a longer life cycle	Use of Approved Products List and centralized purchases .

DoD IEA 2.0 Capabilities	DoD IEA 2.0 Principle/Business Rules	Army Thin/Zero Client Computing Principles (PR)	Business Rules (BR)	Technical Positions
		services will interoperate with other similar Army and DoD systems and decrease cost and complexity of operations.	than status quo thick clients.	
		PR 10 - Thin/Zero Client Computing platforms, applications, and computing services will interoperate with other similar Army and DoD systems and decrease cost and complexity of operations.	BR 10.6 Enable central management and programming for technical refresh (life cycle replacement) of end-user computing equipment.	
		PR 10 - Thin/Zero Client Computing platforms, applications, and computing services will interoperate with other similar Army and DoD systems and decrease cost and complexity of operations.	BR 10.7 Configuration management of the capability shall allow change requests for each system to be channeled through standard Command structures.	

Table 3: Enhance Maintenance and Support Requirements

3.7.1 Enhance Maintenance and Support Facts & Assumptions

- Implementation of Thin/Zero Client Computing will simplify patch, IAVA, and application (load set) management.
- The Implementation of Thin/Zero Client Computing will enable adding and upgrading applications with lower overall administrative effort.
- The implementation of Thin/Zero Client Computing will enable a reduction in software and software licenses.
- The implementation of Thin/Zero Client Computing will enable a reduction in the complexity of end-user device management and administration.

3.7.2 Enhance Maintenance and Support Constraints

- Any back-end solution using MS Windows Server software shall use the AGM to the maximum extent possible.

3.7.3 Enhance Maintenance and Support Risks

- **Risk Area:** Platform Diversity increases O&M complexity.
- **Mitigation:** Centralized management of Thin/Zero Client Computing implementation to decrease platform diversity and O&M complexity.

3.8 Capability 4: Maximize Usability and Flexibility

Table 4: Maximize Usability and Flexibility Principles and Business Rules Mapped to DoD IEA

DoD IEA 2.0 Capabilities	DoD IEA 2.0 Principle/Business Rules	Army Thin/Zero Client Computing Principles (PR)	Business Rules (BR)	Technical Positions
Standard Protocol Management	GP 02 - Interoperability of solutions across the Department is a strategic goal. All parts of the GIG must work together to achieve this goal. Information is made interoperable by following the rules for net-centric sharing of data and services across the enterprise. The DoD achieves infrastructure interoperability through definition and enforcement of standards and interface profile and implementation guidance.	PR 11 - Thin/Zero Client Computing will standardize the Army user computing experience and improve interoperability within DoD, enabling IT infrastructure to adapt to specific user, mission, and strategic requirements.	BR 11.1 Deliver a single Army standard desktop environment to thin client users, agnostic of the user's client hardware.	See Appendix A, Std V-1,2 of this document.
Standard Protocol Management	OPR 28 - Provide and enforce common standards that are utilized across all services to enable any user at the edge to access the data needed from interoperable systems and services.	PR 11 - Thin/Zero Client Computing will standardize the Army user computing experience and improve interoperability within DoD, enabling IT infrastructure to adapt to specific user, mission, and strategic requirements.	BR 11.2 System platforms, applications, and computing services shall interoperate with other similar Army and DoD systems by following common standards.	Thin/Zero Client Computing virtualization, and open- and market-based technical standards will facilitate interoperability in heterogeneous OSs, HW, and SW used by Army and DoD systems.
Standard Protocol Management	OPR 24 - Develop common standards and policies that serve as enforcement mechanisms to ensure interoperability.	PR 11 - Thin/Zero Client Computing will standardize the Army user computing experience and improve interoperability within DoD, enabling IT infrastructure to adapt to specific user, mission, and strategic requirements.	BR 11.3 Support clients running Microsoft Windows OS in accordance with Army policy	Virtual environments created by Thin/Zero Client Computing based on market standards (e.g., VMware, RDS, RDP, ICA, RGS, SPICE, PCoIP) facilitate support for existing OSs used by Army and DoD systems and will be included in the AGM.

Table 4: Maximize Usability and Flexibility Requirements

3.8.1 Maximize Usability and Flexibility Facts and Assumptions

- Thin/Zero client hardware solutions will be hardware agnostic.

3.8.2 Maximize Usability and Flexibility Constraints

- The solutions provider will limit the number of architecture solutions to one per installation.
- Solutions must be scalable to 100% of the SIPRNet population in the Army and 80% of NIPRNet users.

3.9 Capability 5: Improve Performance Quality and Reliability

Table 5: Improve Performance Quality and Reliability Principles and Business Rules Mapped to DoD IEA

DoD IEA 2.0 Capabilities	DoD IEA 2.0 Principle/Business Rules	Army Thin/Zero Client Computing Principles (PR)	Business Rules (BR)	Technical Positions
End-to-End Quality of Service	GP 04 - DoD CIO services shall advertise service-level agreements (SLAs) that document their performance, and shall be operated to meet that agreement.	PR 12 - The combination of three major parts of thin client architecture (thin client devices, thin client back-end solutions and link-display protocols) must be architected to ensure equal or better network performance.	BR 12.1 The system shall provide the capability to recover 99.99% of lost mission critical user data due to failure or error, as defined by DoD Instruction 5000.02.	Thin/Zero Client Computing technical standards facilitate implementing client-server-based computing architecture where all virtualization services (e.g., OSs, HW, SW) are controlled from the centralized servers located in the data centers, where servers/data centers can be geographically distributed, facilitating disaster recovery and Continuity of Operations (COOP) for the virtual environment.
Continuity of Operations	SIP 01 - GIG infrastructure capabilities must be survivable, resilient, redundant, and reliable to enable continuity of operations and disaster recovery in the presence of attack, failure, accident, and natural or man-made disaster.	PR 13 - The client architecture (SW & HW) must be highly available to eliminate single points of failure.	BR 13.1 The Quality of Service will be capable of availability and uptime of 99.99%.	Thin/Zero Client Computing technical standards facilitate implementing client-server-based computing architecture, where all virtualization services (e.g., OSs, HW, SW) are controlled from the centralized servers located in the data centers, where servers/data centers can be geographically distributed, improving operational availability of the end node by reducing recovery time in comparison with the status quo thick client computing environment.
Continuity of Operations	SIP 01 - GIG infrastructure capabilities must be survivable, resilient, redundant, and reliable to enable continuity of operations and disaster recovery in the presence of attack, failure, accident, and natural or man-made disaster.	PR 13 - The client architecture (SW & HW) must be highly available to eliminate single points of failure.	BR 13.2 The capability shall be supported with a network infrastructure that offers redundancy for mission critical network components and back-end equipment, to be determined on an installation-specific basis.	
Continuity of Operations	SIP 01 - GIG infrastructure capabilities must be survivable, resilient, redundant, and reliable to enable continuity of operations and disaster recovery in the presence of attack, failure, accident, and natural or man-made disaster.	PR 14 - Comply with published DoD and Army guidelines for service, disaster recovery and storage of mission data.	BR 14.1 The capability shall be capable of supporting disaster recovery (DR) and COOP plans for mission critical infrastructure and information, based on Mission Assurance Category level and sensitivity level.	DR and COOP are focusing on using technologies such as cloud computing, virtualization, and mobile communications - often in combination - to integrate, rationalize, and simplify recovery, supply chain, loss prevention, and physical security operations. COOP Plans for consideration: a. Alternate Site Plan(s) - a plan to recover technology services at another location

DoD IEA 2.0 Capabilities	DoD IEA 2.0 Principle/Business Rules	Army Thin/Zero Client Computing Principles (PR)	Business Rules (BR)	Technical Positions
				<p>b. Data Center Recovery - a plan to restore the data center at its current location</p> <p>c. Vital Records Management - a plan to secure and retrieve information</p> <p>d. Information Security - a plan to secure information from internal and external threats</p> <p>Thin/Zero Client Computing technical standards facilitate implementing client-server-based computing architecture, where all virtualization services (e.g., OSs, HW, SW) are controlled from the centralized servers located in the data centers, where servers/data centers can be geographically distributed, facilitating disaster recovery and COOP for the virtual environment.</p>
	<p>DoD CDC RA Table 4, Rule 6 - IT services and applications hosted in the computing services provider (CSP) environment must include robust systems management and monitoring.</p>	<p>PR 14 - Comply with published DoD and Army guidelines for service, disaster recovery, and storage of mission data.</p>	<p>BR 14.2 Provide the capability to back up user data in accordance with the replication architecture, to load-balance, and to protect data integrity and availability.</p>	<p>Data Center Core Standards: -TIA (Telecommunications Industry Association) 942 2012 Edition for Data Centers</p> <p>Universal System Restore (USR) software rebuilds complete partitions, regardless of the platform.</p> <p>Thin/Zero Client Computing technical standards facilitate implementing client-server-based computing architecture, where all virtualization services (e.g., OSs, HW, SW) are controlled from the centralized servers located in the data centers, where servers/data centers can be geographically distributed, providing the capability to back up user data in accordance with the replication architecture, to load-balance, and to protect data integrity and availability.</p>
	<p>DoD CDC Table 4, Rule 7 - Data centers that provide enterprise hosting as a managed service for applications must, at minimum, provide security/IA backup, continuity of operations, and disaster recovery services.</p>	<p>PR 14 - Comply with published DoD and Army guidelines for service and disaster recovery and storage of mission data.</p>	<p>BR 14.3 The implementer will ensure that the selected vendors provide a system warranty when fielding the system.</p>	<p>Data Center Core Standards: -TIA 942, 2012 Edition for Data Centers</p> <p>Thin/Zero Client Computing technical standards facilitate implementing client-server-based computing architecture, where all virtualization services (e.g., OSs, HW, SW) are controlled from the centralized servers located in the data centers, where servers/data centers can be geographically distributed, facilitating disaster</p>

DoD IEA 2.0 Capabilities	DoD IEA 2.0 Principle/Business Rules	Army Thin/Zero Client Computing Principles (PR)	Business Rules (BR)	Technical Positions
				recovery and COOP for the virtual environment.

Table 5: Enhance Performance Quality and Reliability Requirements

3.9.1 Improve Performance Quality and Reliability Facts and Assumptions

- The end-user experience will be comparable to the current thick client experience in terms of performance and reliability.
- Zero/Thin Client Computing will be capable of providing availability and uptime of 99.99%.

3.9.2 Improve Performance Quality and Reliability Constraints

- Zero/Thin Client Computing will provide the capability to recover 99.99% of lost mission-critical user data due to failure or error.
- Some power users may still need to use thick clients to support streaming media, Defense Connect Online (DCO), bi-directional audio, and video. If not, Zero/Thin Client Computing must provide proper engineering configuration for acceptable performance.
- Storage optimization capabilities must be considered when designing back-end solutions, to include disk image in streaming or virtual data scenarios and use of data de-duplication on the data storage devices.

3.9.3 Improve Performance Quality and Reliability Risks

- **Risk Area:** Performance quality will be affected with limited scalability. The challenge for the solutions provider is the balance between optimizing resources with scalability to meet end-user mission requirements and demands on bandwidth and storage.
- **Mitigation:** Architect a solution (process and tools) that optimizes resource use but is balanced with scalability to meet changes in user requirements.

3.10 Capability 6: Enhance Business Processes

Table 6: Enhance Business Processes Principles and Business Rules Mapped to DoD IEA

DoD IEA 2.0 Capabilities	DoD IEA 2.0 Principle/Business Rules	Army Thin/Zero Client Computing Principles (PR)	Business Rules (BR)	Technical Positions
Data & Services Availability	CIRR 06 - Shared computing and data storage resources shall be capable of being discoverable and accessible for virtual management and control across the GIG.	PR 15 - Thin/Zero Client Computing implementation will enhance the Army's capability to discover and access LandWarNet assets through virtual management and control across the enterprise.	BR 15.1 The capability will increase Headquarters, Department of the Army (HQDA) visibility of computing assets and software licenses.	Thin/Zero Client Computing virtualizes the computing infrastructure resources (e.g., storages, CPU capacities, OSs, HW, SW) including storage.
		PR 15 - Thin/Zero Client Computing implementation will enhance the Army's capability to discover and access LandWarNet assets through virtual management and control across the enterprise.	BR 15.2 Change requests for implementation of the Thin/Zero Client Computing requirements or solution shall be governed by the Army Business Council (ABC) approval process.	
		PR 16 - Provide the capability to implement a process to leverage virtualized client applications from internal Army and external agencies, resulting in minimal required testing before applications are made available to the enterprise.	BR 16.1 The PM shall be responsible for providing an end-to-end system solution, including systems architecture, client devices, back-end infrastructure (hardware and software), license management strategy, hardware management strategy, and software virtualization strategy. The system implementer shall be responsible for implementing these in support of Army user requirements.	
		PR 17 - Thin/Zero Client Computing implementation funding requirements, to include O&M for tech refresh will be submitted to the CIO/G-6 IAW the PPBE (Planning, Programming, Budgeting & Execution) process.	BR 17.1 The PM shall provide a technology refresh strategy, identify to the CIO/G-6 the programmed funding required to support it, and provide technical refresh as required.	
			BR 17.2 The PM shall be responsible for developing technical, engineering, architectural, operational, implementation, transition, acquisition, and sustainment documentation as indicated by regulation	

DoD IEA 2.0 Capabilities	DoD IEA 2.0 Principle/Business Rules	Army Thin/Zero Client Computing Principles (PR)	Business Rules (BR)	Technical Positions
			and other statutory guidance.	
			BR 17.3 The capability will have fully developed Tactics, Techniques, and Procedures (TTPs) for system use, implementation, integration, operation, and maintenance prior to system installation and fielding.	

Table 6: Enhance Business Process Requirements

3.10.1 Enhance Business Process Requirements Facts and Assumptions

- The Thin/Zero Client Computing Requirements Document will be approved by the Army Business Council (ABC) 3-Star Board.
- An ASA(ALT) Program Manager will design and implement the Thin/Zero Client Computing enterprise solution.
- The PM will develop acquisition strategy and establish cost, schedule, and performance metrics.
- The Cost Review Board will review the PM plan and develop the Army Cost Position.
- The Deputy for Acquisition & Systems (DASM) will review the Thin/Zero Client Computing acquisition strategy and cost position for readiness to proceed to the Army Systems Acquisition Review Council (ASARC).
- A FY12 Unfunded Request (UFR) was submitted for mid-year funding approval; difficulties with being able to execute requested funding late in the year are prohibiting efforts desired in FY12.
- POM 14-18 SIPRNet Thin/Zero Client Implementation has been validated as critical with NIPRNet implementation within the scope of this RA validated as competing with other priorities.

3.10.2 Enhance Business Process Requirements Constraints

- Information Technology Infrastructure Library (ITIL) processes will be considered in the development of the business processes and implementation.
- The 9th SC (A) will assist the PM in the selection of thin-client technologies; standardize the solutions, including proper sizing, risk mitigation, and security standards, to reduce vendor dependencies that are acceptable to the LWN enterprise operations.
- SW and HW equipment (e.g., Commercial Off the Shelf (COT) equipment, routers, switches, phones, etc.) must be ordered through Army Computer Hardware, Enterprise Software and Solutions (CHESS) to standardize HW/SW equipment, improve interoperability, and reduce cost.

- Requirements for all non-CHESS equipment must be approved via a waiver with rationale/ justification, explaining the extenuating circumstances or unique configurations.
- Implementation of Thin/Zero Client computing architectures on an Army post/camp/station with IT services provided by a local Network Enterprise Center (NEC) must follow TA 2010-001 Technical Guidance. (TA 2010-001, 10 Sep 2010).
- Individual organizations must coordinate with their headquarters (i.e., G6/S6, 9th SC (A)) for implementing SIPRNet and NIPRNet thin client infrastructure and acquisition strategy. (TA 2010-001, 10 Sep 2010).
- Unique Thin/Zero Client Computing models must be kept at a minimum to manage workload. However, the system administrator must save a model from each type of thin client in order to run compatibility tests before deployment. (A 2010-001, 10 Sep 2010, pg 7, g.)
- Deviations from the standard Enterprise thin client configurations/guidance will be submitted to 9th SC(A) through the command channels. Following impact analysis to determine interoperability, security and O&M impacts, the 9th SC (A) will submit its recommendations to the ABC approval.
- The thin client solution must follow the DoD acquisition process, to include provisions addressing IA throughout the acquisition lifecycle. (TA 2010-001, 10 Sep 2010, pg 11, 4.4i DoDD 5000.1 Defense Acquisition System.)

3.10.3 Enhance Business Process Requirements Risks

- **Risk Area:** Lack of clarity in the Performance Work Statement creates lack of synchronization, with modifications that cause schedule slippage and cost overruns.
- **Mitigation:** Establish a PM and contracting agency and build adequate time into the overall execution plan for contracting actions.

Appendix A – Standards View (StdV)

Note: CIO/G6 will submit DoD IT Standards Registry (DISR) Change Requests for all the Non-DISR/Non-Mandated standards that are prescribed in this document.

Standard ID	Standard Title	Standard Status	Sample Vendors
Virtualization of Resources			
OVF	Open Virtualization Format (OVF)	Non DISR	IBM; Microsoft; Oracle; Red Hat; VirtualBoxes;Vmware
RDS/RDP	Remote Desktop Services/Protocol (RDS/RDP)	Non DISR	Microsoft
ICA	Independent Computing Architecture (ICA) Protocol	Non DISR	Citrix
RGS	Remote Graphics Software (RGS) Services	Non DISR	HP
SPICE	Simple Protocol for Independent Computing Environment (SPICE)	Non DISR	Red Hat
PCoIP	Personal Computer-over-Internet Protocol (PCoIP)	Non DISR	Vmware View 5
P2V Server Management	Physical to virtual (P2V) Server Management	Non DISR	Cisco Systems; Dell; Fujitsu; HP; IBM
PC Application Virtualization	PC Application Virtualization	Non DISR	Citrix Systems; InstallFree; Microsoft; Spoon; Symantec; Vmware
VM Live Migration	Virtual Machine Live Migration	Non DISR	Citrix Systems; Microsoft; Oracle; Red Hat; VMware
Virtual Switch	Virtual Switch	Non DISR	Cisco; Citrix Systems; Fujitsu Laboratories; HP; Microsoft; VMware
HVD	Hosted Virtual Desktops	Non DISR	Citrix Systems; Deskton; Microsoft; Quest Software; Red Hat; Virtual Bridges;Vmware
Application Formats and Protocols			
CIM HTTP	Specification for CIM Operations over HTTP Version 1.0, Distributed Management Task Force, Inc., 11 August 1999	Emerging	
CIM Schema v2.10.1	Common Information Model (CIM) Version 2.10.1, Distributed Management Task Force, Inc., 3 Oct 2005	Emerging	
DDMS 3.0	DoD Discovery Metadata Specification 3.0	Mandated	

Standard ID	Standard Title	Standard Status	Sample Vendors
MIL-STD-6040B	United States Message Text Format (USMTF), 30 April 2009	Mandated	
OASIS ebXML RIM v3.0	ebXML Registry Information Model, Version 3.0, OASIS Standard, 2 May 2005	Mandated	
OASIS ebXML RS v3.0	ebXML Registry Services and Protocols, Version 3.0, OASIS Standard, 2 May 2005	Mandated	
Data Distribution Service (DDS)	Army standardized publish/subscribe for sending and receiving data service.	Non DISR	
XSLT 1.0	XSL Transformations: Version 1.0: W3C Recommendations, 16 November 1999	Mandated	
Adobe Acrobat Documents Viewer	No Title	Non DISR	
IETF RFC 1996	A Mechanism for Prompt Notification of Zone Changes (DNS NOTIFY), August 1996	Mandated	
IETF RFC 2136	Dynamic Updates in the Domain Name System, April 1997	Mandated	
IETF RFC 3596	DNS Extensions to Support IPv6, Oct 2003	Mandated	
IETF Standard 13/RFC 1034/RFC 1035	Domain Name System, November 1987	Mandated	
IETF RFC 3315	Dynamic Host Configuration Protocol for IPv6 (DHCPv6), July 2003	Mandated	
IETF RFC 3396	Encoding Long Options in the Dynamic Host Configuration Protocol (DHCPv4), November 2002	Mandated	
CSS2:1998	Cascading Style Sheets, level 2 CSS2 Specification, W3C Recommendation 12 May 1998	Mandated	
DOM Level 3 W3C	Document Object Model (DOM) Level 3 Core Specification Version 1.0, W3C Recommendation, 07 April 2004	Mandated	
IETF RFC 2616	Hypertext Transfer Protocol - HTTP 1.1, June 1999	Mandated	
WSRP OASIS	OASIS Web Services for Remote Portlets Specification, August 2003	Mandated	
JSR-914	Java Specification Request (JSR) JSR-914 Java Message Service (JMS) API, Final Release, Version 1.1, April 12, 2002	Mandated	

Standard ID	Standard Title	Standard Status	Sample Vendors
MIMOSA OSA-CBM v3.1	MIMOSA Open Systems Architecture-Condition Based Maintenance Version 3.1, 1 August 2006	Mandated	
SPARQL Query Language for RDF:2008	SPARQL Query Language for RDF:W3C Recommendation, 15 January 2008	Mandated	
NCES	Net-Centric Enterprise Service	Non DISR	
XHTML 1.1: 31 May 2001	Extensible Hypertext Markup Language (XHTML) Version 1.1 - Module-based XHTML, W3C Recommendation, 31 May 2001	Mandated	
IETF RFC 3376	Internet Group Management Protocol, Version 3, Oct 2002	Mandated	
IETF RFC 2849	The LDAP Data EXchange Format (LDIF), June 2000	Mandated	
IETF RFC 3377	Lightweight Directory Access Protocol (v3): Technical Specification; September 2002	Retired	
IETF RFC 1471	The Definitions of Managed Objects for the Link Control Protocol of the Point-To-Point Protocol, June 1993	Mandated	
Namespaces in XML 1.1	Namespaces in XML 1.1, W3C Recommendation 04 February 2004	Mandated	
JBOSS Enterprise Middleware	No Title	Non DISR	
MIMOSA OSA-EAI-2004	MIMOSA Open Systems Architecture-Enterprise Application Integration	Mandated	
IEEE 1003.13-2003	Standardized Application Environment Profile (AEP) POSIX Realtime and Embedded Application Support	Mandated	
ISO/IEC 14519	POSIX Ada Language Interfaces -Binding for System Application Program Interface (API) - Real-Time Extensions, 1999	Mandated	
IETF RFC 2589	Lightweight Directory Access Protocol (v3): Extensions for Dynamic Directory Services, June 2000	Mandated	
IETF RFC 3673	Lightweight Directory Access Protocol version 3 (LDAPv3): All Operational Attributes, December 2003	Mandated	
UDDI 3.0.2	OASIS Universal Description, Discovery, and Integration Version 3.0.2 UDDI Spec, Dated 2004-Oct-19	Mandated	

Standard ID	Standard Title	Standard Status	Sample Vendors
W3C SOAP 1.2 Part 1	SOAP Version 1.2 Part 1: Messaging Framework (Second Edition), W3C Recommendation 27 April 2007	Mandated	
W3C SOAP 1.2 Part 2	SOAP 1.2 Part 2: Adjuncts (Second Edition), W3C Recommendation 27 April 2007	Mandated	
WSDL 1.1	Web Services Description Language (WSDL) 1.1, W3C Note, 15 March 2001	Mandated	
XML 1.0 (Third Edition)	Extensible Markup Language (XML) 1.0 (Third Edition), W3C Recommendation, 04 February 2004	Mandated	
OASIS CAP-V1.1	Common Alerting Protocol, v. 1.1, October 2005	Emerging	
OWF	Ozone Widget Framework	Non DISR	
HTML 4.01	HTML 4.01 Specification, W3C Recommendation, revised, 24 Dec 1999	Mandated	
IETF RFC 4510	Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map, June 2006	Mandated	
Web 2.0	No Title	Non DISR	
IETF RFC 3253	Versioning Extensions to WebDAV (Web Distributed Authoring and Versioning), March 2002	Mandated	
OASIS WS-BrokeredNotification 1.3	Web Services Business Activity (WS-Business Activity), Version 1.1, OASIS Standard incorporating Approved Errata, 12 July 2007	Mandated	
IETF Standard 66/RFC 3986	Uniform Resource Identifier (URI): Generic Syntax, January 2005	Mandated	
CharModel:2005	Character Model for the World Wide Web 1.0: Fundamentals	Mandated	
WS-Eventing	Web Services Eventing (WS-Eventing), August 2004	Emerging	
OASIS WS-Topics 1.3	Web Services Topics 1.3 (WS-Topics), OASIS Standard, 1 October 2006	Mandated	
OASIS SPML v2.0	Service Provisioning Markup Language (SPML) Version 2.0, 1 April 2006	Mandated	
Smart Google Web Toolkit (GWT)	Google Web Toolkit (http://code.google.com/p/smartgwt/)	Non DISR	

Standard ID	Standard Title	Standard Status	Sample Vendors
WS-I Basic Profile 1.1	Web Services Interoperability Organization (WS-I) Basic Profile 1.1, Final Material, August 24, 2004	Mandated	
Mozilla Firefox	No Title	Non DISR	
MS Internet Explorer	No Title	Non DISR	
OASIS WS-Base Notification 1.3	Web Services Base Notification 1.3 (WS-Base Notification), OASIS Standard, 1 October 2006	Mandated	
IETF RFC 4287	Atom Syndication Format, December 2005	Mandated	
IETF RFC 4627	Media Type for JavaScript Object Notation (JSON)	Non DISR	
REST	Representational State Transfer (REST)	Non DISR	
OASIS WS-BPEL v2.0	Web Services Business Process Execution Language (WSBPEL) v2.0, OASIS Standard, 11 April 2007	Emerging	
WSDM V1.0	Web Services Distributed Management (WSDM)	Mandated	
jBPM	No Title	Non DISR	
Red Hat Enterprise Linux Server	Linux Server	Non DISR	
Database			
ISO 23950/NISO Z39.50	Information Retrieval (Z39.50):Application Service Definition and Protocol Specification	Mandated	
ISO/IEC 13249-1:2007	Information Technology - Database Languages - SQL multimedia and application packages - Part 1: Framework, Third Edition, 12 February 2007	Mandated	
ISO/IEC 13249-3:2006	Information Technology - Database Languages - SQL multimedia and application packages - Part 3: Spatial, Third Edition, 26 October 2006	Mandated	
ISO/IEC 9075-1:2003 with Cor. 1:2005 and Cor. 2:2007	Information technology - Database languages - SQL - Part 1: Framework (SQL/Framework), Second Edition, 15 December 2003 with its Technical Corrigendum 1:2005, 15 November 2005 and its Technical Corrigendum 2:2007, 15 April 2007	Mandated	

Standard ID	Standard Title	Standard Status	Sample Vendors
ISO/IEC 9075-10:2003 with Cor. 2:2007	Information technology - Database languages - SQL - Part 10: Object Language Bindings (SQL/OLB), Second Edition, 15 December 2003 with its Technical Corrigendum 2:2007, 12 April 2007	Mandated	
ISO/IEC 9075-11:2003 with Cor. 2:2007	Information technology - Database languages - SQL - Part 11: Information and Definition Schemas, First Edition, 15 December 2003 with its Technical Corrigendum 2:2007, 12 April 2007	Mandated	
ISO/IEC 9075-2:2003 with Cor. 2:2007	Information technology - Database languages - SQL - Part 2: Foundation (SQL/Foundation), Second Edition, 15 December 2003 with its Technical Corrigendum 2:2007, 12 April 2007	Mandated	
ISO/IEC 9075-3:2003 with Cor. 1:2005	Information technology - Database languages - SQL - Part 3: Call-Level Interface (SQL/CLI), Third Edition, 15 December 2003 with its Technical Corrigendum 1:2005, 25 November 2005	Mandated	
ISO/IEC 9075-4:2003 with Cor. 2:2007	Information technology - Database languages - SQL - Part 4: Persistent Stored Modules (SQL/PSM), Third Edition, 15 December 2003 with its Technical Corrigendum 2:2007, 15 April 2007	Mandated	
Information Assurance			
ANSI/INCITS 359-2004	Information technology - Role Based Access Control (RBAC)	Mandated	
CAPP	Controlled Access Protection Profile for Basic Robustness/C2 systems, Version 1.d, NSA, 8 October 1999	Mandated	
IETF RFC 3415	IETF RFC 3415 View-based Access Control Model (VACM) for SNMP, December 2002	Mandated	
ISO/IEC 7816-11:2004	ISO/IEC 7816-11:2004 - Identification cards - Integrated circuit cards - Part 11: Personal verification through biometric methods	Mandated	
ISO/IEC 7816-8:2004	ISO/IEC 7816-8:2004 - Identification Cards - Integrated Circuit(s) Cards with Contacts - Part 8: Security Related Inter-industry Commands (formerly ANSI/ISO/IEC 7816-8:1999)	Mandated	

Standard ID	Standard Title	Standard Status	Sample Vendors
ISO/IEC 7816-9:2004	ISO/IEC 7816-9:2004 - Identification Cards - Integrated Circuit(s) Cards with Contacts - Part 9: Additional Inter-industry Commands and Security Attributes (formerly ANSI/ISO/IEC 7816-9:2000)	Mandated	
OpenGIS GeoXACML 1.0	OpenGIS Geospatial eXtensible Access Control Markup Language (GeoXACML), Version 1.0, February 2008	Emerging	
RSA PKCS #11 v2.20	RSA PKCS #11 v2.20: Cryptographic Token Interface Standard	Mandated	
RSA Labs PKCS #15:2000	Cryptographic Token Information Format Standard, Version 1.1, RSA, 6 June 2000	Mandated	
SKIPJACK/KEA	SKIPJACK and KEA Algorithm Specification, Version 2.0, NIST, 29 May 1998	Mandated	
NIST FIPS Pub 180-3	Secure Hash Standard (SHS), October 2008	Mandated	
IETF RFC 2845	Secret Key Transaction Authentication for DNS (TSIG), May 2000	Mandated	
IETF RFC 3007	Secure DNS Dynamic Update, November 2000	Mandated	
IETF RFC 4035	Protocol Modifications for the DNS Security Extensions, March, 2005	Mandated	
SLOSPP	Protection Profile for Single-level Operating Systems in Environments Requiring Medium Robustness	Mandated	
IETF RFC 4250	The Secure Shell (SSH) Protocol Assigned Numbers, January 2006	Mandated	
HAIPE 3.0.2	High Assurance Internet Protocol Encryptor (HAIPE) Interoperability Specification, Version 3.0.2, December 2006	Mandated	
FIPS Pub 197	Advance Encryption Standard (AES), 26 November 2001	Mandated	
ITU-T X.509:2005	Information Technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks, August 2005	Mandated	
PKIKMITKNPP	Public Key Infrastructure and Key Management Infrastructure Token (Medium Robustness) PP	Mandated	

Standard ID	Standard Title	Standard Status	Sample Vendors
XACML 2.0 OASIS	eXtensible Access Control Markup Language (XACML) Version 2.0, OASIS Standard, 1 February 2005	Mandated	
IETF RFC 3526	More Modular Exponential (MODP) Diffie-Hellman Groups for Internet Key Exchange (IKE), April 2002	Mandated	
IETF RFC 3664	The AES-XCBC-PRF-128 Algorithm for the Internet Key Exchange Protocol (IKE), Jan 2004	Mandated	
IETF RFC 4307	Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2), December 2005	Mandated	
IETF RFC 2207	RSVP Extensions for IPSEC Data Flows, September 1997	Emerging	
IETF RFC 3566	The AES-XCBC-MAC-96 Algorithm and Its Use With IPsec, Sept 2003	Mandated	
IETF RFC 3602	The AES-CBC Cipher Algorithm and Its Use with IPsec, Sept 2003	Mandated	
IETF RFC 3686	Using Advanced Encryption Standard (AES) Counter Mode with IPsec Encapsulation Security Payload (ESP)	Mandated	
IETF RFC 4301	Security Architecture for the Internet Protocol, December 2005	Mandated	
IETF RFC 4302	IP Authentication Header, December 2005	Mandated	
IETF RFC 4303	IP Encapsulating Security Payload (ESP), December 2005	Mandated	
IETF RFC 4306	Internet Key Exchange (IKEv2) Protocol, December 2005	Retired	
IETF RFC 4308	Cryptographic Suites for IPsec, December 2005	Mandated	
IETF RFC 4835	Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH), April 2007	Mandated	
IETF RFC 5996	Internet Key Exchange Protocol Version 2 (IKEv2)	Emerging	
IETF RFC 3585	IPsec Configuration Policy Information Model, Aug 2003	Mandated	
IETF RFC 4869	Suite B Cryptographic Suites for IPsec, May 2007	Mandated	

Standard ID	Standard Title	Standard Status	Sample Vendors
NIST SP 800-126	National Institute of Standards and Technology, Special Publication 800-126, The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.0, November 2009	Mandated	
IETF RFC 3162	RADIUS (Remote Authentication Dial In User Service) and IPv6 August 2001	Mandated	
Internet-Draft : draft-grant-tacacs-02	The TACACS+ Protocol Version 1.78	Non DISR	
FIPS Pub 140-2	Security Requirements for Cryptographic Modules, 25 May 2001	Mandated	
IETF RFC 3412	Message Processing and Dispatching for the Simple Network Management Protocol (SNMP), December 2002	Mandated	
IETF RFC 3413	Simple Network Management Protocol (SNMP) Applications, December 2002	Mandated	
IETF RFC 3414	User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3), December 2002	Mandated	
IETF RFC 4502	Remote Network Monitoring Management Information Base, Version 2, May 2006	Mandated	
IETF RFC 2587	Internet X.509 Public Key Infrastructure LDAPv2 Schema, June 1999	Mandated	
IETF RFC 2865	Remote Authentication Dial In User Services (RADIUS), June 2000	Mandated	
IETF RFC 4217	Securing FTP with TLS, October 2005	Mandated	
IETF RFC 2634	Enhanced Security Services for S/MIME, June 1999	Mandated	
IETF RFC 3850	Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Certificate Handling, July 2004	Mandated	
IETF RFC 2385	Protection of BGP Sessions via the TCP MD5 Signature Option, June 2000	Mandated	
IETF RFC 2403	The Use of HMAC-MD5-96 within ESP and AH, November 1998	Mandated	
IETF RFC 5246	The Transport Layer Security (TLS) Protocol, Version 1.2, August 2008	Emerging	
IETF RFC 5430	Suite B Profile for Transport Layer Security (TLS), March 2009	Mandated	

Standard ID	Standard Title	Standard Status	Sample Vendors
CIMCPP	The Certificate Issuing and Management Components (CIMC) Family of Protection Profiles (PPs)	Mandated	
IETF RFC 2560	IETF Public Key Infrastructure X.509 (PKIX) Online Certificate Status Protocol (OCSP), RFC 2560, June 1999	Mandated	
IETF RFC 5280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, May 2008	Mandated	
FIPS Pub 201-1	Personal Identity Verification (PIV) of Federal Employees and Contractors, March 2006	Mandated	
ID-WSF 2.0	Liberty Alliance Identity Web Services Framework (ID-WSF) 2.0 Specifications, 4 October 2006	Emerging	
IETF RFC 4346	The Transport Layer Security (TLS) Protocol, Version 1.1, April 2006	Mandated	
IETF RFC 4347	Datagram Transport Layer Security, April 2006	Mandated	
SAML 2.0 OASIS	Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0, OASIS Standard, 15 March 2005	Mandated	
W3C WS Addressing 1.0 - Core	Web Services Addressing 1.0 - Core, W3C Recommendation, 9 May 2006	Emerging	
WS-Security 1.1	Web Services Security v1.1, February 2006	Mandated	
CMS/XML Digital Signature Profiles v1.1	DoD Digital Signature Implementation Profiles	Mandated	
FIPS Pub 186-2	Digital Signature Standard (DSS) Digital Signature Algorithm (DSA), 27 January 2000	Mandated	
IETF RFC 3161	Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)	Mandated	
IETF RFC 3852	Cryptographic Message Syntax (CMS)	Mandated	
XML Signature	XML Signature Syntax and Processing, W3C Recommendation, 12 February 2002	Mandated	
XML- Encryption W3C	XML Encryption Syntax and Processing, W3C Recommendation, 10 December 2002	Mandated	
Network Interfaces			
IETF RFC 5072	IP Version 6 over PPP, September 2007	Mandated	

Standard ID	Standard Title	Standard Status	Sample Vendors
IETF Standard 51/RFC 1661/RFC 1662	Point-to-Point Protocol (PPP), July 1994	Mandated	
IETF RFC 1256	ICMP Router Discovery Messages, Sept 1991	Mandated	
IETF RFC 2545	Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing, March 1999	Mandated	
IETF RFC 4213	Transition Mechanisms for IPv6 Hosts and Routers August 2000	Mandated	
IETF RFC 4760	Multiprotocol Extensions for BGP-4, January 2007	Mandated	
IETF RFC 1772	Application of the Border Gateway Protocol in the Internet, 21 March 1995	Mandated	
IETF RFC 3107	Carrying Label Information in BGP-4, May 2001	Mandated	
IETF RFC 3392	Capabilities Advertisement with BGP-4, November 2002	Mandated	
IETF RFC 4271	A Border Gateway Protocol 4 (BGP-4), January 2006	Mandated	
IETF RFC 3378	Ether-IP: Tunneling Ethernet Frames in IP Datagram	Non DISR	
ANSI T1.602-1996 (R2004)	Network and Customer Installation Interfaces (ISDN) Primary Rate Layer 1 Electrical Interfaces Specification	Mandated	
ANSI T1.607-2000 (R2004)	Integrated Services Digital Network (ISDN) - Layer 3 Signaling Specification for Circuit Switched Bearer Service for Digital Subscriber Signaling System Number 1 (DSS1)	Mandated	
ANSI T1.619	Multi-Level Precedence and Preemption (MLPP) Service, ISDN Supplementary Service Description, 1992	Mandated	
ITU-T I.431 (1993)	Primary rate user-network interface - Layer 1 specification	Mandated	
IETF Standard 41/RFC 894	Transmission of IP Datagrams Over Ethernet Networks, April 1984	Mandated	
IETF Standard 5	Internet Protocol, September 1981. With RFCs 791/950/919/922/792/1112	Mandated	
IETF Standard 54/RFC 2328	Open Shortest Path First Routing Version 2, April 1998	Mandated	
IETF RFC 2460	Internet Protocol, Version 6 (IPv6) Specification, December 1998.	Mandated	

Standard ID	Standard Title	Standard Status	Sample Vendors
IETF RFC 2464	Transmission of IPv6 Packet Over Ethernet Networks, December 1998	Mandated	
IETF RFC 2784	Generic Routing Encapsulation (GRE) March 2000	Mandated	
IETF RFC 3484	Default Address Selection for Internet Protocol Version 6 (IPv6), February 2003	Mandated	
IETF RFC 4193	Unique Local IPv6 Unicast Addresses, October 2005	Mandated	
IETF RFC 4291	IP Version 6 Addressing Architecture, February 2006	Mandated	
IETF RFC 4443	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification, March 2006	Mandated	
IETF RFC 4861	Neighbor Discovery for IP version 6 (IPv6), September 2007	Mandated	
IETF RFC 5340	OSPF for IPv6, July 2008	Mandated	
IETF RFC 5308	Routing IPv6 with IS-IS, October 2008	Emerging	
IETF RFC 1042	IP Datagram over IEEE 802 Network	Non DISR	
IETF RFC 1195	Use of OSI IS-IS for Routing in TCP/IP and Dual Environments (Proposed Standard), Dec 1990	Mandated	
IETF RFC 3787	Recommendations for Interoperable IP Networks using Intermediate System to Intermediate System (IS-IS), May 2004	Non DISR	
IETF RFC 5073	IGP Routing Protocol Extensions for Discovery of Traffic Engineering Node Capabilities, December 2007	Non DISR	
IETF RFC 5443	LDP IGP Synchronization, March 2009	Non DISR	
IETF RFC 3630	Traffic Engineering (TE) Extensions to OSPF Version 2, September 2003	Non DISR	
IETF RFC 5392	OSPF Extensions in Support of Inter-Autonomous System (AS) MPLS and GMPLS Traffic Engineering, January 2009	Non DISR	
IETF RFC 5329	Traffic Engineering Extensions to OSPF Version 3, September 2008	Non DISR	
IETF RFC 5305	IS-IS Extensions for Traffic Engineering, October 2008	Non DISR	
IETF RFC 3468	The Multiprotocol Label Switching (MPLS) Working Group decision on MPLS signaling protocols, February 2003	Non DISR	

Standard ID	Standard Title	Standard Status	Sample Vendors
IETF RFC 4204	Link Management Protocol (LMP), October 2005	Non DISR	
IETF RFC 3031	Multi-protocol Label Switching Architecture, January 2001	Mandated	
IETF RFC 4023	Encapsulating MPLS in IP or Generic Routing Encapsulation (GRE), March 2005	Non DISR	
IETF RFC 4448	Encapsulation Methods for Transport of Ethernet over MPLS Networks, April 2006	Non DISR	
IETF RFC 4618	Encapsulation Methods for Transport of PPP/High-Level Data Link Control (HDLC) over MPLS Networks, September 2006	Non DISR	
ITU-T G.7042/Y.1305 (March 2006)	Link Capacity Adjustment Scheme (LCAS) for Virtual Concatenated Signals, March 2006	Emerging	
ITU-T G.709/Y.1331	Interfaces for the Optical Transport Network, March 2003	Retired	
ITU-T G.707/Y.1322:2007	Node Network Interface for the Synchronous Digital Hierarchy (SDH), January 2007	Mandated	
ITU-T G.692	Optical Interfaces for Multichannel Systems with Optical Amplifiers, Oct 1998	Mandated	
ITU-T G.694.1	Spectral Grids for WDM Applications: DWDM Frequency Grid, June 2002	Mandated	
ITU-T G.703	Physical/electrical characteristics of hierarchical digital interfaces, 1972, revision 3 November 2001	Mandated	
ITU-T G.704	Synchronous Frame Structures Used at 1544, 6312, 2048, 8448, and 44 736 kb/s Hierarchy, October 1998	Mandated	
ITU-T G.7041/Y.1303:2008	Generic Framing Procedure, October 2008	Mandated	
IETF RFC 1332	PPP Internet Protocol Control Protocol (IPCP), May 1992	Mandated	
IETF RFC 1570	PPP LCP Extensions, 11 January 1994	Mandated	
IETF RFC 1990	PPP Multi-link Protocol, 16 August 1996	Mandated	
ITU-T G.983.8	B-PON OMCI support for IP, ISDN, Video, VLAN Tagging, VC Cross-Connections and other select functions, 2003	Non DISR	
ITU-T Q.834.1	ATM-PON requirements and managed entities for the network and network element views, 2004	Non DISR	

Standard ID	Standard Title	Standard Status	Sample Vendors
IETF RFC 1812	Requirements for IP Version 4 Routers, 22 June 1995	Mandated	
IETF RFC 2385	Protection of BGP Sessions via the TCP MD5 Signature Option, June 2000	Mandated	
IETF Standard 7/RFC 793	Transmission Control Protocol, September 1981	Mandated	
IEEE 802.16-2004	802.16-2004 IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Fixed Broadband Wireless Access Systems, 2004	Mandated	
IEEE STD 802.15.4-2006	Local and Metropolitan Area Networks - Specific Requirements - Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs), September 2006	Mandated	
IEEE Std 802.16-2009	IEEE Standard for Local and Metropolitan Area Networks Part 16: Air Interface for Broadband Wireless Access Systems, 29 May 2009	Mandated	
Network Management/Operations			
IETF RFC 1471	The Definitions of Managed Objects for the Link Control Protocol of the Point-To-Point Protocol, June 1993	Mandated	
IETF RFC 1472	The Definitions of Managed Objects for the Security Protocols of the Point-to-Point Protocol, June 1993	Mandated	
IETF RFC 1473	The Definitions of Managed Objects for the IP Network Control Protocol of the Point-to-Point Protocol, June 1993	Mandated	
IETF RFC 4113	Management Information Base for the User Datagram Protocol, June 2005	Mandated	
IETF RFC 4750	OSPF Version 2, Management Information Base, December 2006	Mandated	
IETF RFC 3812	Multiprotocol Label Switching (MPLS) Traffic Engineering (TE) Management Information Base (MIB), June 2004	Non DISR	
IETF RFC 3813	Multiprotocol Label Switching (MPLS) Label Switching Router (LSR) Management Information Base (MIB), June 2004	Non DISR	

Standard ID	Standard Title	Standard Status	Sample Vendors
IETF RFC 3919	Remote Network Monitoring (RMON) Protocol Identifiers for IPv6 and Multi Protocol Label Switching (MPLS), October 2004	Non DISR	
IETF RFC 4220	Traffic Engineering Link Management Information Base, November 2005	Non DISR	
IETF RFC 2863	The Interfaces Group MIB, June 2000	Mandated	
IETF RFC 4133	Entity MIB (Version 3) August 2005	Mandated	
IETF RFC 4011	Policy Based Management MIB	Non DISR	
IETF RFC 3411	An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks December 2002	Mandated	
IETF RFC 3412	Message Processing and Dispatching for the Simple Network Management Protocol (SNMP), December 2002	Mandated	
IETF RFC 3413	Simple Network Management Protocol (SNMP) Applications, December 2002	Mandated	
IETF RFC 3414	User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3), December 2002	Mandated	
IETF RFC 3415	IETF RFC 3415 View-based Access Control Model (VACM) for SNMP, December 2002	Mandated	
IETF Standard 62/IETF RFC 3417	IETF Standard 62/IETF RFC 3417, Transport Mappings for the Simple Network Management Protocol (SNMP), December 2002	Mandated	
IETF RFC 2605	Directory Server Monitoring MIB, June 1999	Mandated	
IETF RFC 2789	Mail Monitoring MIB, March 2000	Mandated	
IETF RFC 3273	Remote Network Monitoring Management Information Base for High Capacity Networks, July 2002.	Mandated	
IETF Standard 62/IETF RFC 3418	IETF Standard 62/IETF RFC 3418, Management Information Base (MIB) for the Simple Network Management Protocol (SNMP), December 2002	Mandated	
IETF RFC 2788	Network Services Monitoring MIB, March 2000	Emerging	
IETF RFC 3635	Definitions of Managed Objects for the Ethernet-like Interface Types, September 2003	Mandated	

Standard ID	Standard Title	Standard Status	Sample Vendors
IETF RFC 3060	Policy Core Information Version 1 Specification, February 2001	Mandated	
IETF RFC 3460	Policy Core Information Model (PCIM) Extensions, January 2003	Mandated	
IETF RFC 3644	Policy Quality of Service (QoS) Information Model, November 2004	Mandated	
IETF RFC 3703	Policy Core Lightweight Directory Access Protocol (LDAP) Schema, February 2004	Mandated	
IETF RFC 2748	The COPS (Common Open Policy Service) Protocol	Non DISR	
IETF RFC 2753	A Framework for Policy-based Admission Control	Non DISR	
Network Perimeter Protection			
Application-level Firewall - Medium:2000	U.S. DoD Application-level Firewall Protection Profile for Medium Robustness Environments, Version 1.0, 28 June 2000	Mandated	
Application-level Firewall - Basic	U.S. DoD Application-level Firewall Protection Profile for Basic Robustness Environments, Version 1.0, June 2000	Mandated	
Application-level Firewall - Medium:2000	U.S. DoD Application-level Firewall Protection Profile for Medium Robustness Environments, Version 1.0, 28 June 2000	Mandated	
PP_FW_TF_MR_v1.1 (Traffic Filt. Firewall - Med. Robustness)	U.S. Government Traffic-Filter Firewall Protection Profile for Medium Robustness Environments, Version 1.1, 2007-07-25	Mandated	
PP_FWPP-MR	U.S. Government Firewall Protection Profile for Medium Robustness Environments	Mandated	
Traffic Filtering Firewall - Low Risk	U.S. Government Traffic Filter Firewall Protection Profile for Low Risk Environments, Version 1.1, April 1999	Mandated	
CAPP	Controlled Access Protection Profile for Basic Robustness/C2 systems, Version 1.d, NSA, 8 October 1999	Mandated	
MLOSPP	Protection Profile for Multilevel Operating Systems in Environments Requiring Medium Robustness	Mandated	
Operating Systems			
Windows Server OS version XP or	No Title	Non DISR	

Standard ID	Standard Title	Standard Status	Sample Vendors
higher			
Red Hat Enterprise Linux Server OS version 5 or higher	No Title	Non DISR	
Windows Vista or higher	Windows Vista	Non DISR	
Windows 2003 Server (or newer)		Non DISR	
Linux 3.1 IA32	Linux Standard Base Core Specification for the IA32 Architecture 1.2, April 25, 2006	Mandated	
C903	X Windows System (X11R6): Protocol, The Open Group, July 1999	Mandated	
ISO/IEC 9945-1:2003 with Cor1:2004	ISO/IEC 9945-1:2003 POSIX Base Definitions, with Technical Corrigendum 1:2004	Retired	
Linux 3.1	Linux Standard Base Core Specification 3.1, April 25, 2006	Mandated	
Linux 3.1 PPC32	Linux Standard Base Core Specification for PPC32 3.1, April 25, 2006	Mandated	
UNIX Version 3	Single UNIX Specification Version 3 (SUS v3), The Open Group, 2002	Mandated	
Win32 APIs-Current	Win32 APIs, as specified in the Microsoft Platform SDK	Mandated	
Sensor Operating System (OSs)	Sensor Operating System (OSs)	Non DISR	
Virtual Machine Hypervisor	Virtual Machine Hypervisor	Non DISR	Citrix Systems; HP; IBM; Microsoft; Oracle; Red Hat; VMware
Quality of Services (QoS)			
IETF RFC 3270	Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers, December 1998	Mandated	
IETF RFC 2205	Resource ReSerVation Protocol RSVP Version 1 Functional Specification, September 1997	Mandated	
IETF RFC 2210	The Use of RSVP with IETF Integrated Services, September 1997	Emerging	

Standard ID	Standard Title	Standard Status	Sample Vendors
IETF RFC 2215	General Characterization Parameters for Integrated Service Network Elements, September 1997	Emerging	
IETF RFC 2474	Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers, December 1998	Mandated	
IETF RFC 2475	An Architecture for Differentiated Services	Non DISR	
IETF RFC 2597	Assured Forwarding PHB Group, June 1999	Mandated	
Storages			
IETF RFC 3530	Network File System (NFS) Version 4 Protocol, April 2003	Mandated	
ANSI INCITS 289-1996 (R2001)	Information Technology - Fibre Channel - Fabric Generic Requirements (FC-FG), December 1996 (R2001)	Mandated	
ANSI/INCITS 332-1999	Information Technology - Fibre Channel Arbitrated Loop (FC-AL-2) (updated by amendment 1: 2003)	Mandated	
ANSI/INCITS 357-2002	Information Technology - Fibre Channel - Virtual Interface Architecture Mapping Protocol (FC-VI)	Mandated	
ANSI/INCITS 303-1998 (R 2003)	Fiber Channel Physical and Signaling Interface - 3 (FC-PH-3)	Mandated	
BMR	Bare-Metal Restore	Non DISR	Acronis; Arkeia Software; Cristie; EMC; IBM; Novell; StorageCraft Technology; Symantec; UltraBac Software; Unitrends
e-grade SSD	Enterprise-Grade Solid-State Drives		Symantec; UltraBac Software; Unitrends
iSCSI	Internet Small Computer System Interface		Electronics; Seagate Technology; STEC; Toshiba; Western Digital
Thin Provisioning	Thin Provisioning	Non DISR	DataCore Software; Dell; EMC; Fujitsu; Hitachi Data Systems; HP; IBM; Infortrend; NetApp; Nexsan; NEC; Oracle; VMware
Transport Network			

Standard ID	Standard Title	Standard Status	Sample Vendors
IEEE 802.3-2008	IEEE Standard for Information technology - Specific Requirements, Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications, December 2008	Mandated	
ANSI T1.105-2001	Synchronous Optical Network (SONET) - Basic Description including Multiplex Structure, Rates, and Formats, May 2001	Mandated	
ANSI T1.105.06-2002	SONET: Physical Layer specification	Mandated	
ANSI T1.416.01-1999	Telecommunications - Network-to-Customer Installation Interfaces - Synchronous Optical NETWORK (SONET) Physical Media Dependent Specification: Multi-Mode Fiber	Mandated	
ANSI T1.416.02-1999	Telecommunications - Network-to-Customer Installation Interfaces - Synchronous Optical NETWORK (SONET) Physical Media Dependent Specification: Single Mode Fiber	Mandated	
ATIS-PP-0900101.2006	Synchronization Interface Standard, November 2006	Mandated	
ATIS 0900105.02-2007	Synchronous Optical Network (SONET)- Payload Mappings, September 2007	Mandated	
ITU-T G.7042/Y.1305 (March 2006)	Link Capacity Adjustment Scheme (LCAS) for Virtual Concatenated Signals, March 2006	Emerging	
ITU-T G.808.1 (March 2006)	Generic Protection Switching - Linear Trail and Subnetwork Protection, March 2006	Emerging	
IETF RFC 5795	The RObust Header Compression (ROHC) Framework, March 2010	Emerging	
IEEE 802.11-2007	Local and Metropolitan Area Networks - Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications	Mandated	
IEEE 802.16-2004	802.16-2004 IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Fixed Broadband Wireless Access Systems, 2004	Mandated	

Standard ID	Standard Title	Standard Status	Sample Vendors
IEEE STD 802.15.4-2006	Local and Metropolitan Area Networks - Specific Requirements - Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs), September 2006	Mandated	
IEEE Std 802.16-2009	IEEE Standard for Local and Metropolitan Area Networks Part 16: Air Interface for Broadband Wireless Access Systems, 29 May 2009	Mandated	
Virtual Private Networks			
IETF RFC 4301	Security Architecture for the Internet Protocol, December 2005	Mandated	
IETF RFC 4346	The Transport Layer Security (TLS) Protocol, Version 1.1, April 2006	Mandated	
IETF RFC 4364	BGP/MPLS IP Virtual Private Networks (VPNs), February 2006	Mandated	
IEEE 802.1X:2004	Local and Metropolitan Area Networks - Port Based Network Access Control	Mandated	

Appendix B: Overview and Summary

The purpose of this overview and summary is to briefly describe a Project's Vision, Goals, Objectives, Plans, Activities, Events, Conditions, Measures, Effects (Outcomes), and products. It provides executive-level summary information in a consistent form that allows quick reference and comparison between Architectural Descriptions. The overview and summary serves two Purposes:

- In the initial phases of architecture development, it serves as a planning guide.
- When completed, it provides summary information concerning *who, what, when, why, and how* of the plan as well as a navigation aid to the models that have been created.

Attributes	Description
Vision	The Army will implement a centrally managed, thin/zero client end-user computing technology. Thin/Zero Client Computing will standardize the end-user computing experience and back-end management and control. Standardization will result in increased mission effectiveness through improved security and visibility, enhanced accessibility, streamlined systems administration of the computing environment, and improved efficiency.
Purpose and Perspective	The purpose is to provide Army customers with centrally provisioned desktop and application services using virtualization. Thin/Zero Client Computing creates a computing architecture in which applications, data, processing, and storage are moved from the end-user, thick-client device to Army enterprise back-end infrastructure. This Thin/Zero Client Computing Reference Architecture provides alignment with capabilities at the DoD/Joint/Army level, and establish a common set of principles/rules, process patterns, and technical positions for use within the Army to guide the development of Segment or Solution Architectures for Thin/Zero Client Computing implementation.
Scope	This Reference Architecture is driven by the approved Thin/Zero Client Computing Requirements Document. The scope is limited to the Generating Forces' end-user computing on selected CONUS installations, and does not include server-side mission applications that are being addressed in the Army Data Center Consolidation Plan.
Objectives	<ul style="list-style-type: none"> • Contribute to improving the Army network defense posture. • Improve the end-user experience and accessibility to applications and data. • Achieve cost efficiencies.
	The CIO/G-6 intends for Thin/Zero Client Computing to be

Attributes	Description
Plans	implemented in the Army through an ASA(ALT)-assigned PM and transitioned to NETCOM 9 th (A) SC for Operations and Maintenance.
Activities	A Cost Benefit Analysis (CBA) was conducted and approved. The ABC Process was being used to secure approval of the Requirements Document.
Conditions	Early implementation of Thin/Zero Client Computing will depend on securing FY-13/14 funding for standing up a PM and implementing for selected CONUS SIPRNet and NIPRNet users.
Measures	The Army is developing Cost, Schedule, and Performance measures.
Effects (Outcomes)	End-user applications and data will be moved from the workstation to the server room (Installation Processing Node) for NIPRNet and SIPRNet users at the largest CONUS installations. Thin/Zero Client Computing will align with other enterprise initiatives such as Unified Capabilities, Army Baseline IT Services, Army Data Center Consolidation, and the Army Top Level Security Architecture.
Produced Architecture Viewpoints	High Level Operational Concept View, Organizational and Architectural Relationships View, Capabilities Alignment View, Operational Activities View, Alignment with DoD IEA and JIE Capabilities View, Principles/Business Rules/Technical Positions View, Technical Standards Views, Integrated Dictionary.
Assumptions and Constraints	See Tables 1-6.
Status	CIO/G-6 is awaiting ABC requirement approval, funding approval, and PM assignment by ASA(ALT).
Schedule	Initiate in FY-13 and complete in FY-14 for selected installations within the scope of this architecture.
Tools and File Formats Used	IBM Rational System Architect, MS Access Database, MS Word, MS PowerPoint, Army Capabilities & Architecture Development Integrated Environment (ArCADIE). https://cadie.army.mil/cadie/portal/default.aspx
Stakeholders	DoD CIO, DISA, ASA(ALT), DUSA-BT (Deputy Undersecretary of the Army for Business Transformation), DCS G-3/5/7, TRADOC, U.S. Army CYBERCOM, NETCOM/9 th (A) SC, 7 th SC(T), End-users.
Relationship/Interdependencies with other Architectures	DoD Information Enterprise Architecture, Joint Information Environment, DoD Core Data Center Reference Architecture, and the following Army CIO/G-6 initiatives/architectures: UC, ADCCP, I3C2, TLA, ICAM, NetOps.

Appendix C: Vocabulary (Integrated Dictionary)

Applications Management: Provide a management process based upon a set of best practices proposed to improve the overall quality of IT software development and support through the life-cycle of software development projects, with particular attention to gathering and defining requirements that meet Army/DoD enterprise-level IT objectives.

Assumptions: Assumptions forecast how the terrain will look over time and describe the established “rules of the road”. An assumption is a statement about the existing and future environment (operational, functional or technical) in which a Business Rule would be applied. Assumptions identify the Thin/Zero Client Computing steady state environment and how it will look over time, and the rules of how the sustainment and ongoing capabilities are determined. They expand on and provide additional information based on the principles provided.

Authentication and Access Management: Provide a way of authenticating and authorizing users to gain access to web applications and services, establishing the validity of a transmission, message, or originator, and verifying an individual’s authorization to receive specific categories of information.

Availability Management: Manage the availability of IT services through definition, analysis, planning, measurement, and improvement as the party responsible for ensuring that all IT infrastructure, processes, tools, and roles are appropriate for established service-level targets.

Backup and Recovery: Provide application and service backup and recovery as one of the risk mitigation/incident management factors in assuring service continuity across the Army/DoD Enterprise.

Business Rules: Business rules are definitive statements that provide design tenets and also constrain the implementation of principles and associated policies, as well as acquisition guidance. Business rules represent relationships among the Thin/Zero Client Computing inputs, controls, outputs, and the mechanisms and resources used. For example, a business rule can specify who can do what under specified conditions, the combination of inputs and controls needed, and the resulting outputs. Thin/Zero Client Computing business rules are based on best practices, provide design tenets, and constrain the implementation of principles and relevant policies

Capacity Management: Provide a process for ensuring that IT services and IT infrastructure are able to deliver established service-level targets in a cost-effective and timely manner.

Change Management: Provide control of the lifecycle of all changes to enable beneficial modifications to be made with minimum disruption of enterprise-level IT services.

Cloud Computing: Cloud Computing is the delivery of computing and storage capacity as a service to a community of end-recipients. The name comes from the use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts services with a user's data, software, and computation over a network. End-users access cloud-based applications through a web browser or a light-weight desktop or mobile app, while the business software and user's data are stored on servers at a remote location.

Common Applications: Common applications are those established by NETCOM as the minimum set of software prescribed for the Army Computing Environment, including user applications (e.g., Army Gold Master, Defense Travel System (DTS)) and system applications that enable CAC authentication to Active Directory (login) (such as CAC-enabled web server login, email signing, and encryption).

Configuration Management: Provide a process for maintaining information about configuration items (including their relationships) required to deliver an IT service throughout the lifecycle of the computing infrastructure.

Connection Server: A connection server performs load balancing within the back-end data center, manages terminal server connections, and re-establishes broken terminal server sessions when a connection between the end-user and server is broken.

Constraints: A constraint is a factor that limits freedom of action; for example, boundaries that limit or constrain the implementation of a capability. Constraints provide the Army with the applicable rules, laws, and policies set forth by the Army and DoD/Joint guidance.

Core Data Center: Core Data Centers are the most robust and capable DoD Data Centers, designated as mandatory providers of all Enterprise-wide computing and storage capabilities.

Data Center and/or Back-end Infrastructure: The data center, also known as the back-end infrastructure, comprises a group of servers that are configured to provide thin-client services. These services can include applications and operating systems hosting. The data center can provide remote desktop functionality or image deployment capabilities.

Guiding Principles: Guiding Principles are high-level statements that apply to the subject area and tie back to business/Warfighting requirements. Reference architecture principles are enduring guidelines that describe how Thin/Zero Client Computing will fulfill its mission. Principles express the intent of the capability and fundamental values to be achieved with Thin/Zero Client Computing. Thin/Zero Client Computing principles tie back to installations' CONUS/OCONUS requirements and drive technical positions and patterns. They inform and support how the Army achieves the Thin/Zero Client Computing mission and are intended to be enduring and seldom amended.

Hypervisor: A hypervisor, also called a virtual machine manager, is a program that allows multiple operating systems to share a single hardware host. Each operating system appears to have the host's processor, memory, and other resources all to itself. However, the hypervisor is actually controlling the host processor and resources, allocating what is needed to each operating system in turn, and making sure that the guest operating systems (called virtual machines) cannot disrupt one another.

Incident Management: Provide a management process to restore normal service operation (as defined with SLAs) as quickly as possible, while minimizing adverse effect on operations, ensuring that the best possible levels of service quality and availability are maintained.

Integrated Solutions: Provide solutions for the roll-out or deployment of applications and services within the Army/DoD enterprise computing infrastructure, including design, development, test, and release management.

Patterns: Patterns are generalized architecture representations/viewpoints, graphical/textual models, diagrams, etc., that show relationships among elements and artifacts specified by the technical positions.

Reference Architecture: A reference architecture is considered an organizational asset in:

- Providing common language for the various stakeholders.
- Providing consistency in implementation of technology to solve problems.
- Supporting the validation of solutions against proven reference architectures.
- Prescribing adherence to common standards, specifications, and patterns.

Risk: Risks are technical, political, cultural and governance inhibitors that conflict with guiding principles and target business rules. They are factors that would significantly impact the realization of a Business Rule.

Service Management: Provide process-focused management for Army/DoD enterprise IT systems focused on providing a framework to structure IT-related activities and the interactions of IT technical personnel with Enterprise users.

Service Support: Provide support services for ensuring that users have access to the appropriate services to support mission functions.

Stateless: No disk drives or data reside on the end-user device.

Technical Positions: Technical Positions are a minimal set of enduring technical standards arranged and associated to guide implementation; a set of core or critical technical standards required to establish the capabilities required a Business Rule. Technical positions describe the technical guidance and standards established for Thin/Zero Client Computing. This technical

guidance documentation allows for system owners' and PEOs/PMs' justification to resource their systems, and identifies potential choices and tradeoffs to perform.

Thick Client: Thick clients, also called heavy clients, are full-featured computers that are connected to a network. Unlike thin clients, which lack hard drives and other features, thick clients are functional whether they are connected to a network or not. While a thick client is fully functional without a network connection, it is only a "client" when it is connected to a server. The server may provide the thick client with programs and files that are not stored on the local machine's hard drive. It is not uncommon for workplaces to provide thick clients to their employees. This enables employees to access files on a local server or use the computers offline. When a thick client is disconnected from the network, it is often referred to as a workstation.

Thin Client Terminal: The thin-client terminal is an end-user device. The thin client terminal will replace user's current desktop personal computer. End-user devices in Thin/Zero Client Computing rely on network access to backend infrastructure for these functions. These virtual user devices, known as thin or zero client devices, have no (or a limited) local hard drive and require a Common Access Card (CAC) or secure token to log on and operate. Virtualized client applications, backend servers, and data storage are located in the backend infrastructure.

Vocabulary: The vocabulary establishes a common understanding of terms and consistency of definitions across the subject area.

Appendix D: Acronym Listing

ACRONYM	LONG TITLE
ABAC	Attribute Based Attribute Control
ABITS	Army Baseline IT Services
ABC	Army Business Council
ACCT	Architecture Configuration Control Team
ADCCP	Army Data Center Consolidation Plan
ADORA	Active Directory Optimization Reference Architecture
AEN	Army Enterprise Network
AEP	Application Environment Profile
AES	Advanced Encryption Standard
AGM	Army Gold Master
ANSI	American National Standards Institute
APL	Approved Products List
ArCADIE	Army Capabilities and Architecture Development Integrated Environment
ARNG	Army National Guard
ASA(ALT)	Assistant Secretary of the Army for Acquisition, Logistics and Technology)
ASARC	Army Systems Acquisition Review Council
AS-SIP	Assured Services – Session Initiation Protocol
BGP	Border Gateway Protocol
C&A	Certification and Accreditation
CAC	Common Access Card
CAPP	Controlled Access Protection Profile
CBA	Cost Benefit Analysis
CCB	Change Configuration Board
CDC	Core Data Center
CDES	Cross-Domain Enterprise Services
CDS	Cross-Domain Solution
CHESS	Computer Hardware, Enterprise Software and Solutions
CIM	Common Information Model
CIO	Chief Information Officer
CIRP	Computing Infrastructure Readiness Principles
CIRR	Computing Infrastructure Readiness Rule
CMS	Cryptographic Message Syntax
COA	Course of Action
COE	Common Operating Environment
COI	Communities of Interest
COMSEC	Communications Security
CON	Certificate of Networthiness
CONOPS	Concept of Operations

ACRONYM	LONG TITLE
CONUS	Continental United States
COOP	Continuity of Operations
COPS	Common Open Policy Service
COTS	Commercial Off The Shelf
CRV	Computing Resources Virtualization
CSI	Crypto Systems Interface
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CSP	Computing Services Provider
CTS	Compound Telecommunications Security
CYBERCOM	Cyber Command
DAA	Designated Approving Authority
DAR	Data-at-Rest
DAS	Data Abstraction Services
DASM	Deputy for Acquisition and Systems Management
DCS	Deputy Chief of Staff
DCO	Defense Connect Online
DDMS	DoD Discovery Metadata Specifications
DHCP	Dynamic Host Configuration Protocol
DHTML	Dynamic Hypertext Markup Language
DIACAP	DoD Information Assurance Certification and Accreditation Process
DiD	Defense-in-Depth
DISA	Defense Information Security Agency
DISR	DoD IT Standards Repository
DISN	Defense Information Systems Network
DM-2	DoD Architecture Framework Data Meta-Model
DMDC	Defense Manpower Data Center
DMZ	Demilitarized Zone
DNS	Domain Name System
DoDAF	Department of Defense Architecture Framework
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
DOM	Document Object Model
DOTMLPF	Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel and Facilities
DR	Disaster Recovery
DREN	Defense Research and Engineering Network
DSS1	Digital Subscriber Signaling System Number 1
DTS	Defense Travel System
DUSA-BT	Deputy Undersecretary of the Army for Business Transformation
DVD	Digital Video Disk
EAD	Engineering Acceptance Documents
ECS	Enterprise Collaboration Services

ACRONYM	LONG TITLE
EIAS	Enterprise Identity Attribute Service
EIS	Enterprise Information Systems
EKMS	Electronics Key Management System
EoIP	Everything over Internet Protocol
EPC	Embedded Programmable Cryptographic
EPEAT	Electronic Product Environmental Assessment Tool
EPS	Enterprise Presentation Service
ESB-P	Enterprise Service Bus - Proxy
ESP	Encapsulation Security Payload
FC-FG	Fabric Channel – Fabric Generic Requirements
FIPS	Federal Information Processing Standards
FSO	Field Security Operations
GENFOR	Generating Forces
GIG	Global Information Grid
GP	Global Principle
GRE	Generic Routing Encapsulation
HAIPE	High Assurance Internet Protocol Encryptor
HBSS	Host Based Security System
HQDA	Headquarters, Department of the Army
HRC	Human Resources Command
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HW	Hardware
I3C2	Installation Information Infrastructure Communications and Capabilities
IA	Information Assurance
IAVA	Information Assurance Vulnerability Alert
IAW	In Accordance With
ICA	Independent Computing Architecture
ICAN	Installation Campus Area Network
ICAM	Identity Credentials and Access Management
IDS/IPS	Intrusion Detection System/Intrusion Prevention System
IE	Information Enterprise
IEA	Information Enterprise Architecture
IEC	International Electrochemical Commission
IETF	Internet Engineering Task Force
IKEv2	Internet Key Exchange Protocol Version 2
INSCOM	Intelligence & Security Command
IP	Internet Protocol
IP/MPLS	Internet Protocol/Multi-Protocol Label Switching
IPN	Installation Processing Node
IPS	Intrusion Prevention System
IPSEC	IP Security

ACRONYM	LONG TITLE
IPV4	Internet Protocol Version 4
IPV6	Internet Protocol Version 6
ISDN	Integrated Services Digital Network
ISO	International Organization for Standards
IT	Information Technology
ITIL	Information Technology Infrastructure Library
JIE	Joint Information Environment
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LDIF	Lightweight Data Exchange Format
LSC	Local Session Controller
LWN	LandWarNet
MAC	Mission Assurance Category
MIB	Management Information Base
NCES	Net-Centric Enterprise Services
NEC	Network Enterprise Centers
NETCOM	Network Enterprise Technology Command
NetOps	Network Operations
NGO	Non-Governmental Organizations
NIE	Network Interoperability Exercise
NIPRNet	Non-classified Internet Protocol Router Network
NIST	National Institute of Standards & Technology
NORA	Network Optimization Reference Architecture
NSA	National Security Agency
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
OASIS	Organization for the Advancement of Structured Information Standards
O&M	Operations & Maintenance
OCONUS	Outside of Continental United States
OS	Operating System
OPR	ORA-Derived Operational Rules
OVF	Open Virtualization Format
OWF	Ozone Widget Framework
PC	Personal Computer
P/C/S	Posts, Camps and Stations
PCIM	Policy Core Information Model
PCoIP	Personal Computer over Internet Protocol
PDRR	Protection, Detection, Reaction and Restoration
PDS	Protective Distribution System
PEO	Program Executive Officer
PKI	Public Key Infrastructure
PIV	Personal Identity Verification

ACRONYM	LONG TITLE
PM	Program Manager
POM	Program Objectives Memorandum
PPBE	Planning, Programming, Budgeting & Execution
PPP	Point-to-Point Protocol
PPS	Ports, Protocol and Services
QoS	Quality of Service
RA	Reference Architecture
RACE	Rapid Access Computing Environment
RADIUS	Remote Authentication Dial in User Services
RAM	Random Access Memory
RDS	Remote Desktop Services
RDP	Remote Desktop Protocol
REST	Representational State Transfer
RGS	Remote Graphics Software
ROHC	RObust Header Compression
ROM	Read Only Memory
RNM	Remote Network Monitoring
R/W	Read/Write
SAML	Security Assertion Markup Language
SAR	Secured Availability Rules
SCAP	Security Content Automation Protocol
SFTP	Secure File Transfer Protocol
SHS	Secure Hash Standard
SIP	Shared Infrastructure Principle
SIPRNet	Secret Internet Protocol Router Network
SIR	Shared Infrastructure Business Rule
SLA	Service Level Agreement
SMDC	Space & Missile Defense Command
SNMP	Simple Network Management Protocol
SOAP	Simple Object Access Protocol
SONET	Synchronous Optical Network
SOSE	System of Systems Engineering
SPICE	Simple Protocol for Independent Computing Environments
SPML	Service Provisioning Markup Language
SQL	Structured Query Language
SSH	The Secure Shell
StdV	Standards View
STIG	Security Technical Implementation Guide
SW	Software
TA	Technical Architecture
TCP	Transport Control Protocol
TIA	Telecommunications Industry Association

ACRONYM	LONG TITLE
TLA	Top Level Architecture
TLS	Transport Layer Security
TNOSC	Theater Network Operations & Security Center
TTP	Tactics, Techniques and Procedures
TRADOC	Training and Doctrine Command
TRANSEC	Transmission Security
TSIG	Secret Key Transaction Authentication for DNS
TSP	Time Stamp Protocol
USAR	United States Army Reserve
UC	Unified Capabilities
UCP	Unified Command Plan
UDDI	Universal Description Discovery & Integration
UFR	Unfunded Requirement
USB	Universal Serial Bus
USM	User-based Security Model
USMTF	U.S. Message Text Format
USR	Universal Systems Restore
USSTRATCOM	United States Strategic Command
VDI	Virtual Desktop Infrastructure
VLAN	Virtual Local Area Network
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WOA	Web-oriented Architecture
WPAN	Wireless Personal Area Network
WSDL	Web Services Description Language
XACML	eXtensible Access Control Markup Language
XHTML	eXtensible Hypertext Markup Language
XML	eXtensible Markup Language

Appendix E: References

The references listed below are general references that are applicable to the Army Enterprise operations and the Thin/Zero Client Computing architecture:

1. The Clinger-Cohen Act of 1996.
2. DoDI 8270.bb, DoD Enterprise Architecture (EA), 27 Sep 12.
(<http://dtic.mil/whs/directives>)
3. DoD Directive 8320.02, Data Sharing in a Net-Centric Department of Defense, 2 December 2004.
4. DoD Chief Information Officer, "Department of Defense Architecture Framework (DoDAF) Version 2.02", August 2010.
5. Federal Cloud Computing Strategy, 8 February 2011.
6. DoD Cloud Computing Strategy, 9 January 2012.
7. Draft DoD Information Enterprise Architecture (IEA) v2.0, Jul 2012.
8. Draft DoD Core Data Center (CDC) Reference Architecture (RA) v0.85, 23 Oct 2012.
9. Department of Defense Memorandum, "Enterprise-wide Access to the Network and Collaboration Services (EANCS) Reference Architecture" version 1.0., December 2009.
10. Office of the Assistant Secretary of Defense Networks and Information Integration (OASD/NII) "Reference Architecture Description", June 2010.
11. DoD Directive 8000.1, Information Assurance, 24 October 2002.
12. DoD Instruction 8500.2, Information Assurance (IA) Implementation, 6 February 2003.
13. DoD Regulation O-8530.01-M, Department of Defense Computer Network Defense (CND) Service Provider Certification and Accreditation Program, 17 December 2003.
14. DoD Regulation 8570.01-M, Information Assurance Workforce Improvement Program, Change 2, 19 December 2005.
15. DISA STIG, Windows 2008 R2 Guidance Document, Version 1, Release 2, 28 October 2011.
16. AR 380-40, Policy For Safeguarding and Controlling Communications Security – (COMSEC) Materiel.
17. Army Thin Client Computing Guidance, 15 NOV 2010.
18. Army Enterprise Thin Client Architecture Standardization Memorandum, 20 Sep 2010.
19. Army Enterprise Thin Client Architecture Standardization Technical Authority (TA) v1.0, 30 June 2010 (NETCOM).
20. Army Regulation 25-1, Army Knowledge Management and Information Technology, 4 December 2008.
21. Virtual End-user Environment (Thin/Zero Client Computing) Requirements v1.0, 18 April 2012
22. Army Regulation 25-2. "Information Assurance" Rapid Action Revision (RAR), 23 March 2009.
23. Technical Criteria for the Installation Information Infrastructure Architecture, Feb 2010.

24. Concepts of Operations (CONOPS) 1.0, 16 Dec 2011 (NETCOM).
25. Thin Client Computing, Audit Report, A-2008-0220-FFI, U.S. Army Audit Agency, 28 August 2008.
26. Selected Thin Client Computing Implementations, Audit Report: A-2009-0145-FFFI, U.S. Army Audit Agency, 29 June 2009.
27. Memorandum, CIO/G-6 and ASA(ALT), Subject: use of Computer Hardware, Enterprise Software and Solutions (CHESS) as the Primary Source for Procuring Commercial IT Hardware and Software, 04 May 2009.
28. Army CIO/G-6 Approved Reference Architectures are posted at:
<http://ciog6.army.mil/Architecture/tabid/146/Default.aspx>