

Office of the Army Chief Information Officer/G-6

U.S. Army End-User Devices (EUD) Reference Architecture (RA)

8 January 2016

Version 2.0



CIO/G-6
ENABLING SUCCESS For Today and Tomorrow



CIOG6.ARMY.MIL

DISCLAIMER

The use of trade names in this document does not constitute an official endorsement or approval of the use of such commercial hardware or software. Do not cite this document for the purpose of advertisement.

DISPOSITION INSTRUCTIONS

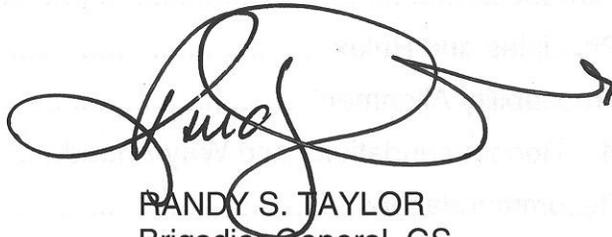
Destroy this document when no longer needed. Do not return it to the organization. Safeguard and destroy this document with consideration given to its classification or distribution statement requirements.

U.S. Army End-User Devices Reference Architecture Executive Summary

Today's Army is increasingly connected in many diverse ways. Mission requirements demand more connectivity among Army members throughout all operational and supporting activities. The need for devices to be portable and agile can strongly challenge connectivity, access and security, as well as the procurement and management of these technologies. In coming years, all devices will have to conform to the Joint Information Environment (JIE).

The U.S. Army End-User Devices (EUDs) Reference Architecture (RA) is the overarching and capstone document for EUDs. This RA provides guidance and direction for both classified and unclassified networks across the two computing configurations (thin and zero clients) in use and maintained by the U.S. Army for EUDs today and through 2021. Future versions of the EUD Reference Architecture will provide guidance for tactical systems and include annexes for thick client, thin client and zero client systems.

This RA uses a rules-based architecture, which organizes architecture data that are to be aligned against capabilities, gaps and outcomes with the principles and rules captured within the DoD Information Enterprise Architecture Version 2.0, LandWarNet 2020 and Beyond Enterprise Architecture, the JIE and future Army network objectives. It supports the Army's efforts to achieve a common operating environment for information technology.

A handwritten signature in black ink, appearing to read 'Randy S. Taylor', with a long horizontal stroke extending to the right and ending in an arrowhead.

RANDY S. TAYLOR
Brigadier General, GS
Director of Architecture, Operations,
Networks and Space

Table of Contents

U.S. Army End-User Devices Reference Architecture Executive Summary.....iii
Table of Contents.....iv
Chapter 1 Introduction..... 1
 1-1 Architecture Introduction 1
 1-2 Background..... 1
 1-3 Intended Audience 2
 1-4 Purpose..... 3
 1-5 Scope..... 3
 1-6 Problems, Issues and Concerns 4
 1-7 Limitations, Assumptions and Constraints 4
Chapter 2 Current and Objective State 5
 2-1 Current State..... 5
 2-2 Objective State..... 6
Chapter 3 Guiding Principles and Rules..... 7
 3-1 Introduction 7
 3-2 Principles and Rules 7
 3-3 Traceability Alignment..... 14
Chapter 4 Recommendations and Way Ahead 17
 4-1 Recommendations 17
 4-2 Way Ahead..... 17
Appendix A References..... 18
 A-1 Required References 18
 A-2 Related References 19
Appendix B Glossary of Acronyms 20
Appendix C Integrated Dictionary (AV-2)..... 22
Appendix D Technical Standards..... 27
Annex A – The Thin/Zero-Client Configuration.....A-1
Administrative Information..... Last Page

List of Figures

Figure 1. Reference Architecture Composition.....1
Figure 2. Current Architecture 5
Figure 3. Objective Architecture 6
Figure 4. Capability Taxonomy (CV-2a): Army Network Mapping of DoD IEA
Capabilities..... 15

List of Tables

Table 1. Principles and Rules Illustration 8
Table 2. Global Access Guiding Principle and Rules 9
Table 3. Secure Availability Guiding Principle and Rules 11
Table 4. Efficiency and Performance Guiding Principle and Rules 13
Table 5. Traceability Alignments 15

Chapter 1 Introduction

1-1 Architecture Introduction

The Army Network Campaign Plan (ANCP) provides the Chief Information Officer/G-6's (CIO/G-6) vision, mission and roles for the Army network. The ANCP, the DoD Information Enterprise Architecture (IEA) and the LandWarNet 2020 and Beyond Enterprise Architecture (LWN 2020 EA) inform the enterprise reference architectures (RAs) that support the Army's Enterprise Information Environment, Warfighting, Business and Defense Intelligence Mission Areas. The composition of the architectures and the context is shown in Figure 1.

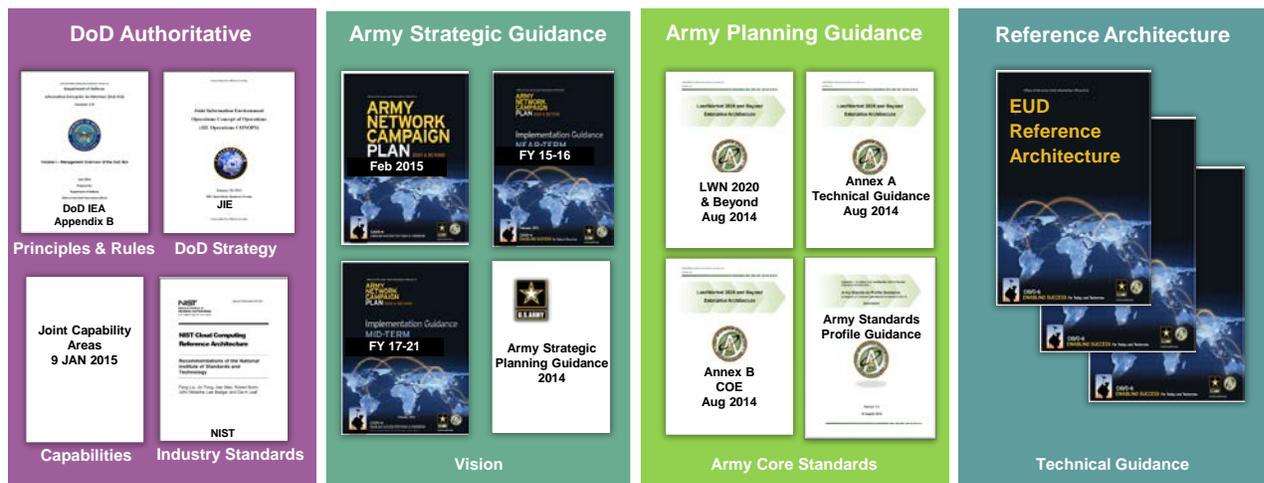


Figure 1. Reference Architecture Composition

This End-User Devices Reference Architecture provides guidance at the level of detail needed to support the development and evaluation of information technology (IT) architectures and their alignment with the ANCP.

1-2 Background

Recent trends in military communications are driving the Army toward more diverse end-user devices (EUDs) to perform more activities via Unified Capabilities (UC). UC are a suite of integrated voice, video and/or data services delivered ubiquitously across a secure and highly available network infrastructure, independent of technology, to increase mission effectiveness for the warfighter and business communities.¹ Concurrently, Army commanders are requesting EUDs based on their assessments of mission requirements, raising demand for the devices themselves as well as the connectivity necessary to enable their use. Meeting the demand comes at a cost. Eighty percent of network vulnerabilities exist at the end node.²

¹ DoD Instruction 8100.04, DoD Unified Capabilities (UC), 9 December 2010.

² Virtual End-User Environment (VEUE), Thin/Zero Client Computing, 5 April 2012.

In March 2013, the Secretary of the Army released Army Directive 2013-02 (Network 2020 and Beyond: The Way Ahead) with the intent to “change the way the Army will do business, the governance processes for managing network modernization, and the acquisition of information technology (IT) systems and equipment.” The directive mandates that the Army no longer purchase EUDs that cannot be supported due to insufficient bandwidth.

In response to the directive, the CIO/G-6 performed an alternatives assessment for secure EUDs; it produced the following high-level objectives to aid the Army in crafting a cohesive strategy for EUDs.

- (1) Optimize effectiveness, efficiency and security.
- (2) Minimize attack surface.
- (3) Rapidly restore EUDs to a known good state.
- (4) Centralize testing, certification and procurement.
- (5) Enforce application and configuration settings.
- (6) Consolidate management of enterprise licenses.
- (7) Establish a limited number of development platforms.
- (8) Adhere to established technical standards for interoperability.
- (9) Achieve a similar user experience across multiple devices.
- (10) Establish and enforce standards for implementation of uniform security patches and version updates to all EUDs.

The ANCP and its implementing documents provide the guidance upon which Army IT will be developed, deployed and operated. The CIO/G-6 uses enterprise reference architectures as the primary method to inform, guide and constrain the design and development of solution architectures. Rules supporting enterprise guiding principles are developed from existing architectural data, strategic objectives and senior leader guidance.

1-3 Intended Audience

The intended audience for this document includes the Office of the Assistant Secretary of the Army (Acquisition, Logistics and Technology) (ASA(ALT)), Program Executive Office Enterprise Information Systems (PEO EIS), U.S. Army Cyber Command (ARCYBER), Second Army, Signal Commands and the Defense Information Systems Agency (DISA). It also includes IT investment decision makers, architects, program managers, architecture developers, Army UC service providers and UC mission support personnel associated with the Enterprise Information Environment Mission Area (EIEMA), Warfighting Mission Area (WMA), Business Mission Area (BMA), Defense Intelligence Mission Area (DIMA) and Army network. This document should be referenced when developing enterprise and operational architecture solutions to ensure alignment with DoD guidance, architectures and strategies, and Joint initiatives. This RA can also be used to support IT investment review boards, validate procurement of solutions and assess conformance.

1-4 Purpose

The purpose of this document is to standardize architecture developed in support of procurement of Army EUD solutions for thin/zero-client configurations. Per the ANCP, Army end users interact with the Army network through EUDs, which are defined as IT hardware components that contain and execute human-machine interface (HMI) software. The guidance within this document is primarily provided as a set of business, operational and guiding principles and rules that address three general functions: global access, secure availability, and efficiency and performance.

1-5 Scope

This document supports Focused End State (FES) 2.7, Deliver Data Center Cloud Computing Environment (see the Army Chief of Staff's 20 February 2015 memorandum regarding Mission Command Network modernization). The Army's computing configurations for EUDs require support from each of the IT mission areas to function properly. This RA addresses both classified and unclassified networks, along with both government and commercial off-the-shelf (COTS) devices, with the latter often being more cost effective. It presents architectural rules to improve the Army's interoperability with DoD and ensure that it can leverage Joint Information Environment (JIE) capabilities as they emerge.

The Army Common Operating Environment (COE) 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 (CEs) (reference 4). Each CE has a minimum standard configuration that supports the Army's ability to quickly produce and deploy high-quality applications. It also reduces the complexity and costs of configuration, support and training. The principles and rules within this RA are intended to inform the configurations for EUDs in the Data Center, Cloud and Generating Force CEs. All other CEs are in the tactical domain, which will be addressed in the next version of this RA.

An EUD is composed of a physical device and the operating system software necessary for the device to function. A thin/zero client is a software service or application that runs on an EUD and is not essential to device function. The distinction is in data, applications and processing. This document covers two end-user environments.

(1) A thin-client configuration is a self-contained computing device that operates without locally stored data; data are accessed through the thin client and may be available in a cloud/server. The thin client has local applications and local processing; although a thin client may temporarily store data locally, it does not have permanent, locally stored data. The thin client may operate in a disconnected, intermittent or limited (DIL) connection mode, depending upon the configuration settings.

(2) A zero-client configuration is a self-contained network device with no or limited hard disk drive. It does not run a full operating system or store data; instead, the device merely initializes the network connection and handles input/output to a cloud/server. Zero clients must be connected to the network to operate and may operate in a DIL environment, but would have limited effectiveness. An example of a zero client is the Virtual Desktop Infrastructure.

1-6 Problems, Issues and Concerns

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 more secure, standardized and effective computing capabilities and network that enable mission command and meet strategic requirements at each post, camp and station. Today, the network lacks effective enterprise management to enable and secure all end-user computing devices. As an example, there is no method to uniformly update security patches, software and firmware on all end-user devices. As a result, many network vulnerabilities begin at the end node, for instance when users inadvertently allow malicious applications or changes to be introduced on their devices. Such security breaches can lead to exposure of sensitive data and cost a significant amount of time and money to resolve.

1-7 Limitations, Assumptions and Constraints

Topics beyond the scope of this RA include the following.

(1) Tactical forces (tactical infrastructure and tactical applications). The tactical portion of the network is not specifically addressed in this document. In general, the tactical network is below the Fixed Regional Hub Node and is provided by tactical equipment, such as the Warfighter Information Network-Tactical (WIN-T). Tactical guidance will be provided in the next version of this RA.

(2) Industrial control systems. These are generally commercial devices used for the control of industrial processing or manufacturing, or other administrative or logistical functions, such as a bar scanner or a temperature monitor. These systems are usually within the generating force, but may extend down to the operating force.

(3) Remote Continental United States (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.

This reference architecture is based on certain assumptions. Thin/zero-client computing has the potential for cost avoidance and some savings when implemented at locations with high user densities.

There also are certain constraints. Limited implementation on the Secret Internet Protocol Router Network (SIPRNet) and the Non-secure Internet Protocol Router Network (NIPRNet) will increase the time required to achieve the projected return on investment or may negate the return on investment.

Chapter 2 Current and Objective State

2-1 Current State

The current Army EUD architecture, shown in Figure 2, is a complex scenario that covers three environments (enterprise, institutional and tactical) in which IT must operate to fulfill Army requirements for EUDs. In the near term, network capacity for end users is set to expand through the Department of Defense Information Network (DoDIN) – formerly known as the Global Information Grid (GIG) – from a low of 10 gigabits per second (gbps) per installation to upward of 100 gbps per installation.

The DoD Mobile Classified Capabilities (DMCC) device uses a commercially developed smart phone hardened to National Security Agency (NSA) Commercial Solutions for Classified Mobility Access Capability Package specifications. It is an enterprise solution developed to protect Secret voice and data. DMCC solutions will displace 2G devices, the Secure Mobile Environment Portable Electronic Device, QSEC 2700s and Secure Sect-era phones. DMCC initial capabilities include secure voice and SIPR Defense Enterprise Email (DEE) via Outlook Web Access. Users will be able to view, but not download, email attachments until DISA incorporates the data-at-rest capability via incremental releases.

For unclassified mobile needs, Defense Mobile Unclassified Capabilities (DMUC) will implement Mobile Device Management and the Mobile Application Store (MAS). Mobile Device Management will be incrementally updated with additional capabilities.

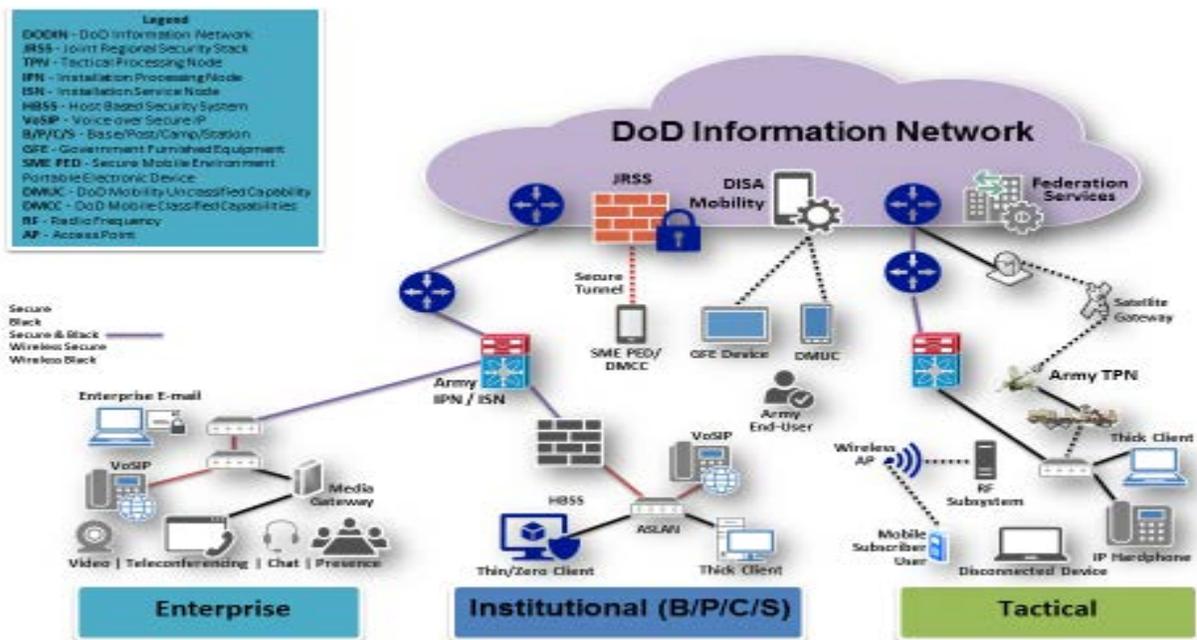


Figure 2. Current EUD Architecture

2-2 Objective State

Under the EUD objective architecture (Figure 3), users will see a more integrated suite of mobile devices, such as smart phones with more interactive voice capability that will interoperate with wired or wireless devices. As transmission changes to a combination of wired and wireless infrastructure, the Army will have a network that is always on and always available, and is less tactical, with limited single points of failure and more network diversity for Army EUDs. COTS devices will be leveraged, where appropriate, to reduce cost and provide the latest technologies to Army users.

Functional capabilities will be provided by the Installation Processing Node (IPN) data centers within the JIE architecture. An IPN is a fixed DoD data center serving a single DoD installation and local area (installations physically or logically behind the network boundary) with local services that cannot (technically or economically) be provided from a core data center (CDC). There will be only one IPN per DoD installation but each IPN may have multiple enclaves to accommodate unique installation needs (e.g., Joint bases).

Additionally, installation facilities will provide basic network and communication capabilities, which include the Installation Service Node (ISN). The ISN contains the localized equipment necessary to provide the minimum basic functionality to an installation should it become disconnected from the DoDIN. There is no application hosting or data processing in an ISN.

A more complete depiction of how the Army will use UC through EUDs is contained in the UC Reference Architecture (reference 10).

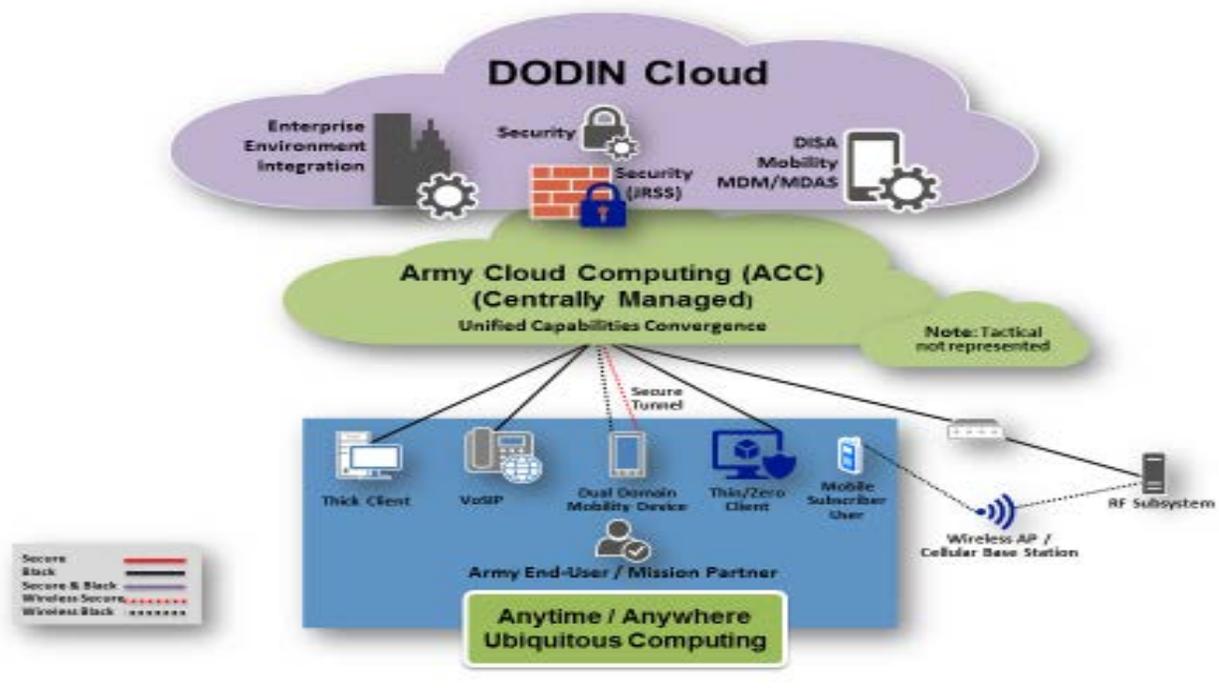


Figure 3. Objective Architecture

Chapter 3

Guiding Principles and Rules

3-1 Introduction

This chapter describes the principles and rules that inform, guide and constrain the design and implementation of a specific topic/technology. The principles in this chapter are aligned with the Army network. The architecture guidance and direction are organized according to the layered structure of the DoD Information Enterprise Architecture (IEA). The applicable references are identified in each principle. The tables in this chapter are organized as follows.

- Guiding Principles
- Capability Gaps
- Rules
- Desired Outcomes
- Considerations and Known Risk
- Mitigation

3-2 Principles and Rules

Guiding principles represent the top-level guidance for IT planning and decision making. They are high-level statements that apply to specific business and warfighting requirements. The Army guiding principles presented in Tables 2 through 4 were derived from DoD IEA Volume II B-1, listed below, and applied to the EUD architecture.

Table 1 illustrates how these rules will be presented within this document. The table is organized as follows.

- (1) An enterprise guiding principle derived from the DoD IEA is associated with a required DoD IEA capability.
- (2) Associated with each guiding principle is a reference to applicable Joint Capability Areas (JCAs) to show how the rules support the JCA. Gaps within current network capabilities that the Army wishes to achieve are then identified.
- (3) From the identified gaps, a set of rules that will produce the desired outcomes is listed.
- (4) If implementation of a rule warrants additional consideration because a known risk exists, this information will be provided to facilitate future risk mitigation and serve as documentation of the current challenges associated with the Army's EUD architecture.

Acronyms for DoD IEA v2.0 principles and business rules are as follows.

- CRP - Communications Readiness Principle
- CIRP - Computing Infrastructure Readiness Principle
- CIRR - Computing Infrastructure Readiness Rule

DSDR - Data & Services Deployment Business Rule

GP - Global Principle

SAP - Secured Availability Principle

SAR - Shared Availability Rule

Table 1. Principle and Rules Illustration

Guiding Principle <i>Guiding principle that is derived from the DoD Information Enterprise Architecture</i>	
Capability Gaps	
Identified gaps in a specific capability area.	
Architectural Rule(s) that mitigate Capability Gap	Desired Outcomes
Architectural rules that provide the constraints and guidance required to satisfy capability gaps and standards.	Specific outcomes that will be achieved with successful implementation of the rules.
Considerations and Known Risk	Mitigation
Identified considerations, risks and challenges associated with implementing the identified rules.	Identified considerations, risks and challenges associated with implementing the identified rules.

The general principles and rules applicable to Tables 2 through 4, which follow, are identified under three areas: global access, secure availability, and efficiency and performance.

Table 2. Global Access Guiding Principle and Rules

<p>EUD P1: Army EUDs use globally accessible services to provide global access to information, in accordance with LandWarNet (LWN) 2020 and Beyond EA and its annexes (A & B), to all authorized users. (Supports JCA 6.2.2.4)</p>	
<p>Capability Gap</p>	
<p>End users' experience is non-standard and inefficient.</p>	
<p>Architectural rules that mitigate capability gap</p>	<p>Desired Outcomes</p>
<p>EUD R1.1: Authorized Army EUD procurers and Army network providers will coordinate Army EUD requirements for operation at edge environments and consistency with Annexes A & B of LWN 2020 and Beyond EA to ensure compatibility and uninterrupted support to Army users. (Ref: CIRR-03, DoD IEA, v2.0, Vol. II, B-5)</p>	<p>The Army uses all types of clients that provide regionally aligned forces and unified action partners continuous advantages across all Joint operational phases by leveraging available capabilities and implementing the Army's Network 2020 and DoD's Joint Vision 2020 architectures.</p>
<p>EUD R1.2: Army end users will be able to obtain reliable network connectivity for their devices regardless of their point of attachment, network domain or community of interest. (Ref: CIRR-04, DoD IEA, v2.0, Vol. II, B-5)</p>	<p>The Army uses all types of clients that provide regionally aligned forces and unified action partners continuous advantages across all Joint operational phases by leveraging available capabilities and implementing the Army's Network 2020 and DoD's Joint Vision 2020 architectures.</p>
<p>EUD R1.3: Army network providers will ensure transparent near-real-time provisioning and allocation of shared resources to EUDs that are platform agnostic and location independent. (Ref: CIRP-03, DoD IEA, v2.0, Vol. II, B-5)</p>	<p>Computing services for all EUDs (thin/zero clients) are designed to meet mission requirements and will not adversely affect existing operations, systems or missions.</p>
<p>EUD R1.4: Responsible Army cybersecurity organizations will create policies and procedures to ensure that all authorized entities have access to critical data, services and applications from anywhere in an Army information environment, given the required network capacity. (Ref: Operational Rules-02, DoD IEA, v2.0, Vol. II, B-7)</p>	<p>Army EUDs can access business and warfighter services through a global cloud-based infrastructure.</p>

<p>EUD R1.5: Army acquisition will ensure that all EUDs that receive, process, store, display and/or transmit DoD information will be acquired, configured, operated, maintained and disposed of consistent with applicable DoD cybersecurity policies, standards and architectures. (Ref: DoDI 8500.01, 3.h. (1))</p>	<p>Cybersecurity features that are “designed in” at the device level are consistent, interoperable and the norm for Army end users. Implementation of these standards and disposal of devices maximize risk management.</p>
<p>EUD R1.6: Army EUD procurers and network and computing host providers will ensure that end users are able to derive a consistent user experience (that is, look, feel, content and utility), regardless of location or EUD, to the maximum extent possible. (Ref: LWN 2020 v2.0, 3.6.4., and Army Information Architecture (AIA) v4.1, p 17)</p>	<p>Mobile EUDs will retrieve and modify data as depicted in the AIA End State Information Sharing Framework. Factors that affect Soldier, civilian and mission-partner safety, health, workload and equipment ease of use are considered during the EUD life cycle.</p>
<p>Considerations and Known Risk</p>	<p>Mitigation</p>
<p>Mobility device development is driven primarily by the commercial marketplace and may create user expectations that are not feasible, acceptable or suitable for military application.</p>	<p>The Army continuously evaluates emerging technology and conducts analytical assessments to identify solutions that meet approved requirements and priorities. The Army constantly engages with industry to clearly communicate these needs.</p>
<p>Mobile devices have non-compliant (not DoD-approved) embedded Global Positioning Service (GPS) solutions.</p>	<p>Enforce public law and DoD implementation guidance related to GPS and position, navigation and timing (PNT).</p>
<p>Mobile devices can be deliberately or inadvertently connected to an incorrect security domain.</p>	<p>Develop markers and enforce audit log reviews for EUDs.</p>
<p>Detailed Common Operating Environment definition requires the integration of JIE, DoDIN, Army network, COE and Army Data Center Consolidation Plan operational, technical and management requirements. These requirements include provisions for EUDs.</p>	<p>COE-based standards and specifications will be published in the EUD technical architecture portion of the COE and reinforced by PEO EIS’s published plans.</p>

Table 3. Secure Availability Guiding Principle and Rules

<p>EUD P2: Army EUDs use DoD-approved computing infrastructure for secure access to authorized shared spaces and information assets. (Supports JCA 6.2.2.4.) (Ref: DoD Mobile Policy Security Requirements Guide Ver. 1, Rel. 2, 26 July 2013)</p>	
<p>Capability Gaps</p>	
<p>Access to Army networks and information is inconsistent. Controls and methods are ineffective at mitigating risk to information integrity and unauthorized access. No centralized life-cycle management of end-user devices throughout the Army.</p>	
<p>Architectural rules that mitigate capability gap</p>	<p>Desired Outcomes</p>
<p>EUD R2.1: Army cybersecurity organizations and network providers will ensure that authorized Army EUDs use a single common network identity or universal credentials that are recognized by all producers of information and services. (Ref: Operating Rule-01, DoD IEA, v2.0, Vol. II, B-7)</p>	<p>Authentication provides mitigation against unauthorized access, enables integrity that protects against unintentional or malicious change, and supports availability of data for Army mission partners and users.</p>
<p>EUD R2.2: Devices used through the Army network will tailor the “view” presented to each user based on his/her role(s) within the limitations of his/her EUD. (Ref: LWN and Beyond 2020 EA)</p>	<p>Access control is granted utilizing dynamic, rule-based or attribute-based access control, if available. EUDs that facilitate access to Army/DoD information shall authenticate all entities, as specified in the Identity and Access Management RA, prior to granting access.</p>
<p>EUD R2.3: Army cybersecurity professionals must have the ability to reconfigure, optimize, defend and recover data in an automated manner, when possible, remotely or with minimum “hands on” physical access. Attempts made to reconfigure, defend and recover should produce an incident audit trail. (Ref: DoDI 8500.01, 3.b.(3))</p>	<p>Self-aware EUDs coupled with self-healing networks will maintain secure and robust access for Army personnel. Routine tasks are effectively executed with limited resources.</p>
<p>EUD R2.4: EUD procurers will register EUDs in the Army Portfolio Management Solution (APMS) to record investment data, and register the application data in the Army Data Center Consolidation Plan Tracking Tool.</p>	<p>EUDs are registered to enable life-cycle performance, schedule and cost oversight.</p>

<p>EUD R2.5: Army cybersecurity professionals and EUD procurers will ensure that mobile devices that store data use appropriate encryption with the wipe keys upon shutdown or as the situation demands.</p>	<p>Data-at-rest encryption standards are implemented on EUDs; devices are designed with functions to automatically wipe data when the application closes or shuts down, or as required by the user.</p>
<p>Considerations and Known Risk</p>	<p>Mitigation</p>
<p>Lack of status information for all EUDs in the Army can lead to misallocation of scarce resources and security breaches.</p>	<p>Enforcement of existing and emerging information technology asset management will help to ensure asset visibility, as well increase interoperability.</p>

Table 4. Efficiency and Performance Guiding Principle and Rules

<p>EUD P3: EUDs must be designed, procured and supplied in a manner consistent with DoD and Army policies to support interoperability and efficient use of resources. (Supports JCA 6.2.2.4)</p>	
<p>Capability Gaps</p> <p>Missed opportunities to equip end users with next-generation solutions provided by commercial off-the-shelf (COTS) technologies. Duplication of efforts for testing, certification and configuration management. Development and use of redundant data, services and other solutions.</p>	
<p>Architectural rules that mitigate capability gap</p>	<p>Desired Outcomes</p>
<p>EUD R3.1: Army acquisition professionals will establish and implement a mission assurance capability that promotes COTS solutions while addressing hardware, software and supplier assurance through assessments or certifications of end-user devices. (Ref: SAR-05, DoD IEA, v2.0, Vol. II, B-3)</p>	<p>The Army acquires COTS solutions (e.g., desktop, laptop, tablet, smart phone, personal digital assistant, mobile phone) that meet DoD and Army standards, such as National Information Assurance Acquisition Policy and NSA requirements, through the commercial solutions for classified process. The results are lower cost and greater interoperability, with the appropriate management of risk and vulnerabilities.</p>
<p>EUD R3.2: Army end users use existing enterprise data, services and EUD interfaces whenever possible, practical and appropriate instead of recreating those assets. (Ref: DSDR 11, DoD IEA, v2.0, Vol. II, B-3)</p>	<p>For classified EUDs, the Army’s approach is to partner with agencies, such as the NSA, in order to obtain secure government-furnished equipment (GFE). For unclassified EUDs, the Army’s approach is to partner with agencies, such as DISA, through pilots to reduce program risk.</p>
<p>Considerations and Known Risk</p>	<p>Mitigation</p>
<p>Rapid changes within technology development, market needs and delivery employment methods could place DoD and the Army in disadvantaged positions.</p>	<p>Publication and use of the COE will help measure and forecast change. Continue leveraging shared DoD technology expertise and purchasing power for mobile and end-user equipment.</p>
<p>Many EUDs that generate position, navigation and timing (PNT) data to provide situational awareness both directly and indirectly are vulnerable to jamming and spoofing.</p>	<p>Those EUDs must use a DoD-approved PNT application or device.</p>

3-3 Traceability Alignment

Alignment with the JIE, DoD IEA and Army Network

The JIE is envisioned as a secure environment, comprised of shared information technology infrastructure, enterprise services and a single security architecture, to achieve full-spectrum superiority, greater mission effectiveness, increased security and IT efficiencies. Operation and management of the JIE occurs in accordance with the Unified Command Plan (UCP), using enforceable standards, specifications and common tactics, techniques and procedures (TTPs). As described in DoD IEA v2.0 (reference 1), the three major facets are:

- (1) User/operation requirements (govern): processes and models, standards and policy, and monitoring compliance.
- (2) Enable capabilities: operate, defend.
- (3) End-user capabilities: connect, access, share.

The Army's framework for managing network modernization, as stated in the ANCP (reference 5), is the Army network portfolio, which addresses JCA 6, Communications and Computers (Reference 14). The portfolio is composed of three Army network domains: Enterprise Services, Network Operations and Security, and Network Capacity.

Enterprise Services Domain: This domain provides authorized users awareness of and access to all DoD information and DoD-wide information services. It is responsible for core enterprise services, information and data management, and services management capabilities.

Network Operations and Security Domain: This domain provides a secure, seamless and continuous network environment with protected critical data and information for the Total Force. This is achieved through capabilities within the overarching areas of operating and defending the network.

Network Capacity Domain: This domain oversees the portfolio of investments intended to increase network transport bandwidth and processing and storage capacity. It is responsible for transport, computing, storage and end-user services (which include EUDs).

The general alignment between the DoD IEA and the Army network is depicted in Figure 4 and Table 5. This viewpoint shows a crosswalk from DoD IEA capabilities to delivered Army domains.

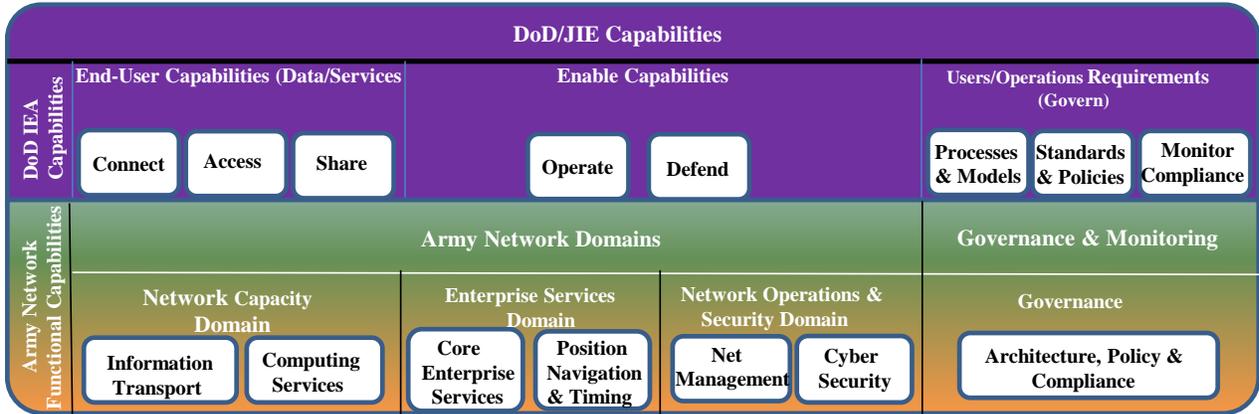


Figure 4. Capability Taxonomy (CV-2a): Army Network General Alignment to DoD IEA

Table 5. Traceability Alignments

Principle	Rule	Traceability Reference	Number	Name
EUD P1	EUD R1.1 – R1.6	DoD IEA, v2.0, Vol. II, B-1	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.
		Army Network Capability	n/a	Army EUDs use the globally accessible services to provide all authorized users access to information through the Army network.
EUD P2	EUD R2.1 – R2.4	DoD IEA, v2.0, Vol. II, B-4	CIRP-01	Computing infrastructure must support all Army missions and provide the edge effective, on-demand, secure access to shared spaces and information assets across functional, security, national and interagency domains.
EUD P2	EUD R2.1 – R2.4	Army Network Capability	n/a	Network Capacity EUDs: The ability of an authorized user to send, receive and process data.

Principle	Rule	Traceability Reference	Number	Name
EUD P3	EUD R3.1 – R3.2	DoD IEA, v2.0, Vol. II, B-3	SAP-02	The globalization of information technology, particularly the international nature of hardware and software development (including the supply chain), and the rise of global providers of IT and communications services present a very new and unique security challenge. DoDIN resources must be designed, managed, protected and defended to meet this challenge.
		Army Network Capability	n/a	Network Capacity EUDs: The ability of an authorized user to send, receive and process data.

Chapter 4

Recommendations and Way Ahead

EUDs are evolving from costly legacy hardware-based devices to devices that perform more activities via UC. UC is the integration of voice, video and/or data services delivered ubiquitously across a secure and highly available network infrastructure, independent of technology, to increase mission effectiveness for the warfighter and business communities.

4-1 Recommendations

The demand for these devices in units is rising as the need for constant connectivity grows. DoD and the Army have been directed to implement more efficient approaches to architect end-user desktop and mobile device environments. Army EUD efforts will align with the Army network strategy. The Army will continue to pursue the use of COTS devices to decrease the cost of delivering the most current technologies available. EUD architects will coordinate with Headquarters, Department of the Army and CIO/G-6 during planning and development of the EUD architecture.

4-2 Way Ahead

In accordance with the ANCP near-term guidance, the Army will:

- (1) Develop an EUD strategy to define requirements for a common EUD environment, which shall include recommendations from the COTS IT working group.
- (2) Establish the technical parameters necessary to enable enterprise-level agreements with providers of mobile data service.
- (3) Identify and begin implementing adjustments to the installation and deployable network infrastructure components necessary to support the mobile aspect of the EUD strategy.
- (4) Standardize procurement of infrastructure and EUD solutions (e.g., thin/zero clients).
- (5) Assist organizations with implementation of a standard suite of EUD systems, resulting in significant cost savings and the ability to collaborate across the force.

The CIO/G-6 Army Architecture Integration Center will work with stakeholders to accomplish the following.

- (1) Participate in and support applicable EUD integrated development teams.
- (2) Develop requirements for EUD RA v3.0 to address identified issues and concerns. The next version will incorporate changes based on updates and new guidance from DoD and the Army, and will address the tactical portion of the network.
- (3) Ensure that EUD RA v3.0 supports Army EUD development and implementation activities.

Appendix A References

Documents and links may have been updated since the release date of this appendix; readers should refer to the applicable updated document or link for the latest information.

A-1 Required References

1. DoD Information Enterprise Architecture Version 2.0, July 2012.
http://DODcio.defense.gov/Portals/0/Documents/DIEA/DOD%20IEA%20v2.0_Volume%20Description%20Document_Final_20120730.pdf.
2. Memorandum, Secretary of the Army, 20 February 2013, subject: Information Technology Management Reform (ITMR) Implementation Plan.
[https://army.deps.mil/army/cmds/HQDA_CIOG6_Temp/Shared%20Documents/Information%20Technology%20Management%20Reform%20\(ITMR\)%20Implementation%20Plan.pdf](https://army.deps.mil/army/cmds/HQDA_CIOG6_Temp/Shared%20Documents/Information%20Technology%20Management%20Reform%20(ITMR)%20Implementation%20Plan.pdf).
CAC Required.
3. LandWarNet 2020 and Beyond Enterprise Architecture Version 2.0, 1 August 2014.
<http://ciog6.army.mil/Architecture/tabid/146/Default.aspx>.
4. Annex B: Definitions and Guidance for the Common Operating Environment, Version 2.0, 1 August 2014. <http://ciog6.army.mil/Architecture/tabid/146/Default.asp>.
5. Army Network Campaign Plan 2020 and Beyond, February 2015.
<http://ciog6.army.mil/AboutCIO/Mission/ANCP/tabid/237/Default.aspx>
6. Army Network Campaign Plan Implementation Guidance, Near Term (2015-2016), February 2015. <http://ciog6.army.mil/AboutCIO/Mission/ANCP/tabid/237/Default.aspx>
7. Army Network Campaign Plan Implementation Guidance, Mid Term (2017-2021), Version 1.2, February 2015.
<http://ciog6.army.mil/AboutCIO/Mission/ANCP/tabid/237/Default.aspx>.
8. Army Information Architecture (AIA), Version 4.1, 5 June 2013.
<http://ciog6.army.mil/Architecture/tabid/146/Default.aspx>.
9. U.S. Army Identity and Access Management Enterprise Reference Architecture, Version 4.0, 29 September 2014.
<http://ciog6.army.mil/Architecture/tabid/146/Default.aspx>.
10. U.S. Army Enterprise Cloud Computing Reference Architecture, Version 1.0, 29 September 2014. <http://ciog6.army.mil/Architecture/tabid/146/Default.aspx>.
11. U.S. Army Enterprise Service Management Reference Architecture, Version 1.0, 20 May 2015. <http://ciog6.army.mil/Architecture/tabid/146/Default.aspx>.
12. U.S. Army Unified Capabilities Reference Architecture, Version 2.0, 24 June 2015.
<http://ciog6.army.mil/Architecture/tabid/146/Default.aspx>.
13. U.S. Army Network Operations Reference Architecture, Version 1.0, 6 March 2014.
<http://ciog6.army.mil/Architecture/tabid/146/Default.aspx>.
14. U.S. Army Network Security Enterprise Reference Architecture, Version 2.0, 29 September 2014. <http://ciog6.army.mil/Architecture/tabid/146/Default.aspx>.

15. U.S. Army End-User Devices Reference Architecture, Version 1.0, 29 September 2014. <http://ciog6.army.mil/Architecture/tabid/146/Default.aspx>.
16. Joint Chiefs of Staff Joint Capability Areas, 9 January 2015. https://intellipedia.intelink.gov/wiki/Joint_Capability_Areas. CAC required.
17. Joint Tactical Radio Software Communications Architecture (JTR SCA), Version 1.0, 7 November 2012. <https://wmaafip.csd.disa.mil/Project/Details?ald=6&prjld=179&prjVld=U179&Encrypt=8C9C7C2C01D32A413A956D41DCE147EBE8D02A80>.

A-2 Related References

1. Army Regulation (AR) 25-13, Telecommunications and Unified Capabilities, 25 March 2013. http://armypubs.army.mil/epubs/pdf/r25_13.pdf.
2. Department of Defense Enterprise-wide Access to Network and Collaboration Services (EANCS), Version 1.0, December 2009. http://DODcio.defense.gov/Portals/0/Documents/DIEA/EANCS%20RA_Final_v1_20091221.pdf.
3. DoD Active Directory Optimization Reference Architecture, 15 December 2010. http://DODcio.defense.gov/Portals/0/Documents/DIEA/ADORA_Final_v1_20101215.pdf.
4. DoD Information Enterprise Architecture Core Data Center Reference Architecture, Version 1.0, 18 September 2012. http://DODcio.defense.gov/Portals/0/Documents/DIEA/CDC%20RA%20v1_0_Final_Releaseable%20Version.pdf.
5. DoD Joint Information Environment Enterprise Architecture (DoD JIE EA), Version 1.0, December 2012. https://army.deps.mil/army/cmds/hqda_ciog6/ZX/ZBS/SIG%20Internal%20Library/DOD-%20JIE-EA%20v1%200.pdf. CAC required.
6. DoD Instruction 8500.01, Cybersecurity, 14 March 2014. http://dtic.mil/whs/directives/corres/pdf/850001_2014.pdf.
7. AR 25-2, Information Management Information Assurance, Raid Action Revision, 23 March 2009. http://armypubs.army.mil/epubs/pdf/r25_2.pdf.
8. National Institute of Standards and Technology (NIST) Special Publication 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems, February 2010. <http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf>.
9. Memorandum, Chief of Staff of the Army, 20 February 2015, subject: Mission Command Network Modernization Way Ahead. https://army.deps.mil/army/cmds/hqda_ciog6/ZX/ZBS/SIG%20Internal%20Library/MCN%20Modernization%20CSA%20Signed%2020%20Feb%02015.pdf

Appendix B Glossary of Acronyms

The following acronyms are applicable within this document.

Acronym	Description
AAIC	Army Architecture Integration Center
ADCCP	Army Data Center Consolidation Plan
AENC	Army Enterprise Network Council
AGM	Army Golden Master
ANCP	Army Network Campaign Plan
ARCYBER	U.S. Army Cyber Command
ASA(ALT)	Assistant Secretary of the Army (Acquisition, Logistics and Technology)
BMA	Business Mission Area
CAC	Common Access Card
CDC	Core Data Center
CIO/G-6	Chief Information Officer/G-6
CIRP	Computing Infrastructure Readiness Principle
CIRR	Computing Infrastructure Readiness Business Rule
CMO	Army Chief Management Officer
COE	Common Operating Environment
CONUS	Continental United States
CRP	Communications Readiness Principle
DIL	Disconnect, Intermittent, Limited
DIMA	Defense Intelligence Mission Area
DISA	Defense Information Systems Agency
DMCC	Department of Defense Mobile Classified Capabilities
DMUC	Department of Defense Mobile Unclassified Capabilities
DNS	Domain Name System
DoD	Department of Defense
DoDIN	Department of Defense Information Network
DSDR	Data & Services Deployment Business Rules
EA	Enterprise Architecture
EIEMA	Enterprise Information Environment Mission Area
EUD	End-User Device
FSO	Field Security Operations
GFE	Government-Furnished Equipment
GP	Global Principle
HMI	Human-Machine Interface

UNCLASSIFIED

Acronym	Description
HQDA	Headquarters, Department of the Army
I3C2	Installation, Information, Infrastructure, Communications and Capabilities
ICAN	Installation Campus Area Network
IdAM	Identity and Access Management
IEA	Information Enterprise Architecture
IPN	Installation Processing Node
ISN	Installation Service Node
ITMR	IT Management Review
JCA	Joint Capability Area
JIE	Joint Information Environment
MAS	Mobile Application Store
MDM	Mobile Device Management
NETCOM	Network Enterprise Technology Command
NIAAP	National Information Assurance Acquisition Policy
NIPRNet	Non-secure Internet Protocol Router Network
NIST	National Institute of Standards & Technology
NSA	National Security Agency
OPR	Operational Rule
PEO EIS	Program Executive Office Enterprise Information Systems
PKI	Public Key Infrastructure
PNT	Position, Navigation and Timing
QoS	Quality of Service
RA	Reference Architecture
SAP	Secured Availability Principle
SAR	Secured Availability Business Rule
SIPRNet	Secret Internet Protocol Router Network
SLA	Service Level Agreement
SME PED	Secure Mobile Environment Personal Electronic Device
TLA	Top Level Architecture
TPN	Tactical Processing Node
TRADOC	U.S. Army Training and Doctrine Command
UC	Unified Capabilities
VPN	Virtual Private Network
WIN-T	Warfighter Information Network-Tactical
WMA	Warfighting Mission Area

Appendix C Integrated Dictionary (AV-2)

The following terminology captured in All Viewpoint (AV)-2 is applicable within this document.

Acronym	Description	Reference
Assured Services Local Area Network (ASLAN).	ASLANs are required to support Department of Defense Internet Protocol (DoD IP)-based voice services. ASLANs must have 99.997 percent availability, to include scheduled maintenance, and no single point of failure that can cause an outage of more than 96 percent of IP telephony subscribers.	http://ciog6.army.mil/Architecture/t/abid/146/Default.aspx
DoD X.509 Certificate Policy	The unified policy under which an unclassified certification authority (CA) operated by a DoD component is established and operates to issue and manage digital PKI credentials.	http://iase.disa.mil/pki-pke/downloads/unclass-dod_cp_v10-5.pdf
End-User Device	A device that provides a human-machine interface, most specifically when connected to a network.	http://ciog6.army.mil/Architecture/t/abid/146/Default.aspx
End-User Services	The specific set of computing devices that enable end users to access information, applications and services locally and via the network.	JCA, 9 January 2015 http://dcmo.defense.gov/products-and-services/business-enterprise-architecture/9.0/reports/bealist_jointcapabilityarea_na.htm
Installation Processing Node (IPN)	A fixed (i.e., not designed to be relocated or transported) data center serving a single installation and local area (installations physically or logically behind the network boundary) with local services that cannot (technically or economically) be provided from a core data center.	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afi33-115/afi33-115.pdf

Acronym	Description	Reference
Installation Service Node (ISN)	A facility containing the localized equipment necessary to provide the minimum basic functionality to an installation should it become disconnected from the Global Information Grid (DoDIN). There is no application hosting or data processing in an ISN. Potential services include read-only Active Directory (AD) servers, Domain Name System (DNS) servers, Assured Compliance Assessment Solution (ACAS) servers, Host-Based Security System (HBSS) servers and print servers. In addition, ISNs may host UC capabilities that must remain on the installation to enable emergency services when the connection to the DoDIN is interrupted.	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afi33-115/afi33-115.pdf
IP-Based Networking Services	This service group provides for the seamless transmission of information (voice, video or data) by using the set of communication protocols for the Internet and other similar networks.	CV-7, DoD IEA v2.0, 201207 http://dodcio.defense.gov/Portals/0/Documents/DIEA/DoD%20IEA%20v2.0_Volume%20I_Description%20Document_Final_20120730.pdf
Media Gateway (MG)	A media gateway is any device, such as a circuit switch, soft switch and/or packet switch, IP gateway or channel bank that converts data from the format required for one type of network to the format required for another.	DoD Unified Capabilities Framework 2013 http://www.disa.mil/network-services/UCCO/~media/Files/DISA/Services/UCCO/UCR2013/UC_Framework_2013_Combined.pdf
Mobile/Handheld	A form-factor device that includes the use of handheld, mobile, cellular, tablets, etc., which may be used in austere, tactical environments.	http://ciog6.army.mil/Architecture/tabid/146/Default.aspx

Acronym	Description	Reference
Online Certificate Status Protocol	An Internet protocol used for obtaining the revocation status of an X.509 digital certificate. It is an alternative to certificate revocation lists (CRL) used as part of the Public Key Infrastructure (PKI).	http://jtc.fhu.disa.mil/projects/pki/documents/DoD_ocsp_mtp_v1_0_july_2003.pdf
Public Key Infrastructure (PKI)	An enterprise-wide service (that is, data integrity, user identification and authentication, user non-repudiation, data confidentiality, encryption and digital signature) that supports digital signatures and other public key-based security mechanisms for DoD functional enterprise programs, including generation, production, distribution, control and accounting of public key certificates. PKI provides the means to bind public keys to their owners and helps in the distribution of reliable public keys in large heterogeneous networks. Public keys are bound to their owners by public key certificates. These certificates contain information such as the owner's name and the associated public key, and are issued by a reliable certification authority.	DA PAM 25-1-1 26 September 2014 http://www.apd.army.mil/pdf/files/p25_1_1.pdf
Service Level Agreement (SLA)	Part of a service contract where the level of service is formally defined, including references to the contracted delivery time (of the service) or performance.	http://ciog6.army.mil/Architecture/abid/146/Default.aspx
Tactical/Mobile Processing Node (TPN)	Tactical/Mobile Processing Nodes will provide services similar to a Core Data Center, but are optimized for the tactical or deployed environment. Depending upon the circumstances, TPNs may connect to the DoDIN through DoD Satellite Gateways.	http://www.armed-services.senate.gov/imo/media/doc/Takai_02-26-14.pdf

Acronym	Description	Reference
Thick Client	A thick-client configuration (local data, applications and processing) is a self-contained computing device, which has resident applications and processes stored on the hard drive, enabling local manipulation of locally stored data. A thick-client device can operate in a connected or disconnected, intermittent and limited connection mode.	Government EUD SME
Thin Client	A thin-client configuration (local applications and processing, remote data) is a self-contained computing device that operates without locally stored data; data are accessed from the thin client and may be available in a cloud/server. Thin client has local applications and local processing, but does not have locally stored data. Thin client may operate in a disconnected, intermittent and limited connection mode, depending upon the configuration settings.	Government EUD SME
Unified Capabilities	The ability to seamlessly integrate voice, video and data applications and services for mobile and fixed communications so that they are delivered ubiquitously across a secure and highly available single-protocol network infrastructure.	CIO Lexicon DoDI 8100.04 http://www.dtic.mil/whs/directives/corres/pdf/810004p.pdf
Video Teleconferencing Services	Two-way electronic voice and video communication between two or more locations. May be fully interactive voice or two-way voice and one-way video; includes full-motion video, compressed video, and sometimes freeze-frame (still) video.	DA PAM 25-1-1 26 September 2014 http://www.apd.army.mil/pdf/files/p25_1_1.pdf

Acronym	Description	Reference
Wired Communication Services	This service enables the transmission of data over a wire-based communication technology, typically telephone lines, cables and fiber-optic communication.	http://ciog6.army.mil/Architecture/abid/146/Default.aspx
Wireless Communication Services	This service provides communications via radio frequency, microwave or infrared short range, transferring information without the use of wires.	http://ciog6.army.mil/Architecture/abid/146/Default.aspx
Zero Client	A zero-client configuration (no local data, applications or processing) is a self-contained network device with no or limited hard disk drive. It does not run a full operating system; instead, the device merely initializes the network connection and handles in/output to a cloud/server. Zero clients must be connected to the network to operate; they will not operate in a disconnected, intermittent and limited connection mode. An example of zero client is the Virtual Desktop Infrastructure.	Government EUD SME

Appendix D Technical Standards

The Standards Profile (StdV-1), Standards Forecast (StdV-2) and the Non-Defense Information Technology Standards and Profile Registry (DISR) are not in this document due to their changing nature.

The standards can be found in an addendum at the following location:
<http://ciog6.army.mil/Architecture/tabid/146/Default.aspx>.

1
2
3
4
5
6

U.S. Army End-User Devices (EUD) Reference Architecture (RA)

Annex A – The Thin/Zero-Client Configuration

8 January 2016

Version 2.0



CIO/G-6
ENABLING SUCCESS For Today and Tomorrow



DISCLAIMER

The use of trade names in this document does not constitute an official endorsement or approval of the use of such commercial hardware or software. Do not cite this document for the purpose of advertisement.

DISPOSITION INSTRUCTIONS

Destroy this document when no longer needed. Do not return it to the organization. Safeguard and destroy this document with consideration given to its classification or distribution statement requirements.

Table of Contents

Annex A, Chapter 1 Introduction A-1

1-1 Background A-1

1-2 Intended Audience A-1

1-3 Purpose A-1

1-4 Scope A-3

Annex A, Chapter 2 Thin/Zero-Client Computing A-5

2-1 Relationship between Thin/Zero-Client Computing and Other DoD/Army Enterprise IT Efforts A-5

2-2 Thin/Zero-Client Computing Components A-8

Annex A, Chapter 3 Thin/Zero-Client Computing Principles and Rules A-11

3-1 Thin/Zero-Client Computing Capabilities Principles & Business Rules A-11

3-2 Capability 1: Deliver an Army Thin/Zero-Client Computing Solution A-12

3-3 Capability 2: Enhance Security and Information Assurance A-23

3-4 Capability 3: Enhance Maintenance and Support A-32

3-5 Capability 4: Maximize Usability and Flexibility A-35

3-6 Capability 5: Improve Performance Quality and Reliability A-36

3-7 Capability 6: Enhance Business Processes A-40

Administrative Information Last Page

List of Figures

Figure A-1. High-Level Operational Concept GraphicA-2

Figure A-2. Thin/zero-client computing objectives to standardize and centralize the computing environment.....A-3

Figure A-3. Organizations and Architectural RelationshipA-5

Figure A-4. Thin/Zero-Client Computing Requirements Alignment to DoD IEA.....A-8

Figure A-5. Thin/Zero-Client Computing Alignment with JIE Capabilities.....A-10

List of Tables

Table A-1. Deliver Army Thin/Zero-Client Computing Solution Principles and Business Rules Mapped to DoD IEAA-13

Table A-2. Enhance Security and Information Assurance Principles and Business Rules Mapped to DoD IEA.....A-23

Table A-3. Enhance Maintenance and Support Principles and Business Rules Mapped to DoD IEAA-32

Table A-4. Maximize Usability and Flexibility Principles and Business Rules Mapped to DoD IEAA-35

Table A-5. Improve Performance Quality and Reliability Principles and Business Rules Mapped to DoD IEA.....A-36

Table A-6. Enhance Business Processes Principles and Business Rules Mapped to DoD IEAA-40

Annex A, Chapter 1 Introduction

1-1 Background

The Army relies heavily on personal computing devices. 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 that 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 for IT requirements, leaving leadership with an inaccurate view of the 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 were analyzed to capture lessons learned in order to establish Army-wide standardized solutions for thin/zero-client computing, and are reflected in this annex.

1-2 Intended Audience

The primary intended audience for this reference architecture (RA) is the Assistant Secretary of the Army (Acquisition, Logistics and Technology) (ASA (ALT)), Program Executive Officers (PEOs), Program Managers (PMs), and operational and solutions architects and engineers engaged in the planning and execution of delivering thin/zero-client solutions. Other stakeholders include:

- DoD Chief Information Officer (CIO)

- Defense Information Systems Agency (DISA)

- Army Chief Management Officer (CMO) – Office of Business Transformation

- Army CIO/G-6

- Army Deputy Chief of Staff, G-3/5/7

- U.S. Army Training and Doctrine Command (TRADOC)

- U.S. Army Cyber Command

- Second Army

- Network Enterprise Technology Command (NETCOM)

- 7th Signal Command (Theater)

1-3 Purpose

The purpose is to deliver thin/zero-client computing solutions to provide Army users centrally managed IT capabilities. Thin/zero-client computing employs a computing architecture in which applications, data, processing and storage are hosted on an installation infrastructure, as shown in Figure A-1. This operational concept graphic represents the thin/zero-client computing “to be” configuration for Continental United States (CONUS) thin/zero-client computing solutions. The graphic depicts three major

aspects: the end-user environment, the network environment and the data center environment.

The initial Army enterprise thin/zero-client computing configuration will be installation-centric with regional/remote access from DoD/Army facilities for both classified Secure Internet Protocol Router Network (SIPRNet) and unclassified Non-secure Internet Protocol Router Network (NIPRNet) data through the Department of Defense Information Network (DoDIN), and remote access from untrusted networks (Internet, cloud) at home/hotel.

Thin/zero-client users will be provisioned to meet all 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 for all users. Installations' data centers will further enable services with the virtualization of operating systems, applications and profiles.

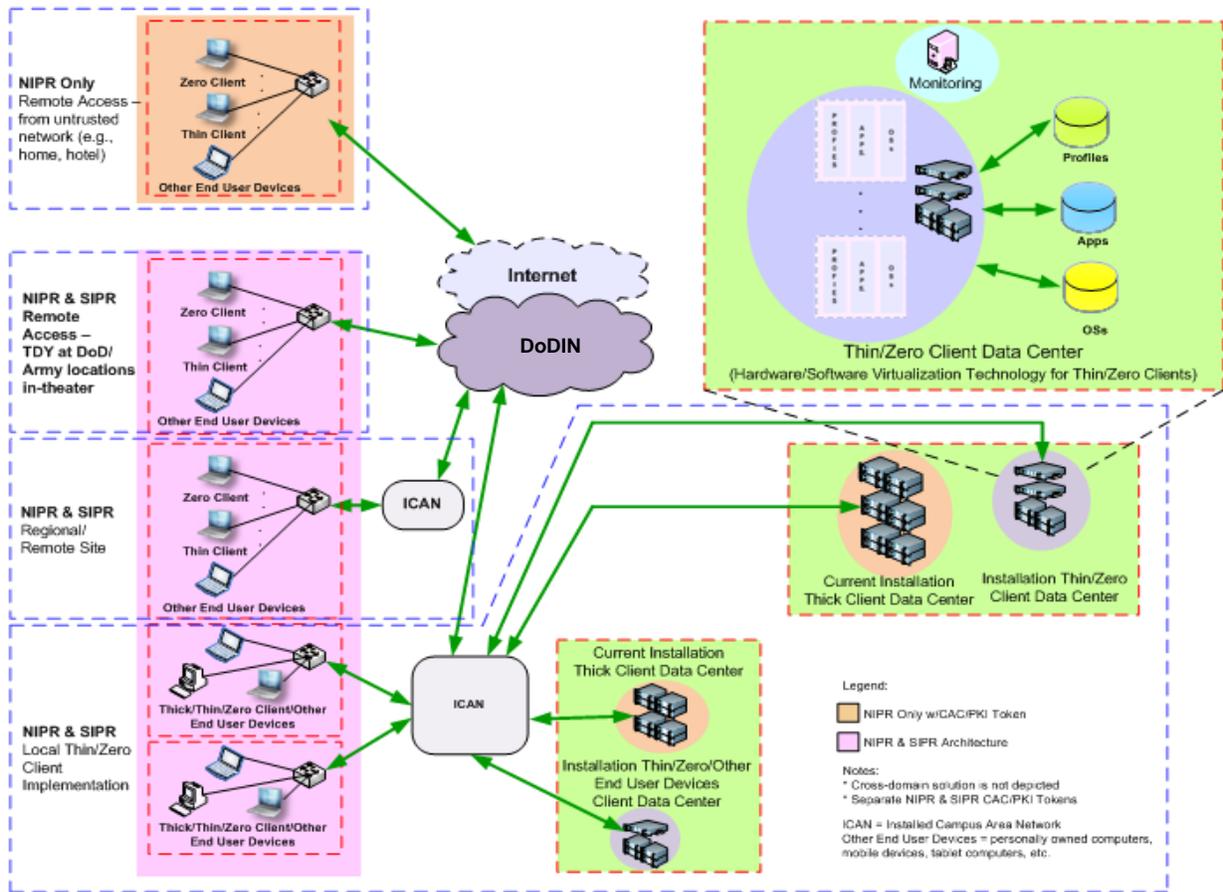


Figure A-1. Thin/zero-client High-Level Operational Concept Graphic

Figure A-2 below depicts the Army thin/zero-client computing objectives to standardize and centralize the computing environment. The goals are to increase mission effectiveness, security and IT asset visibility. The objectives also describe opportunities for cost efficiencies generated by 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 restoration • 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
<p>These capabilities provide the opportunity for cost efficiencies through</p> <ul style="list-style-type: none"> • Efficient operation & maintenance (O&M) through reduced touch labor • Reduced tech refresh • Enterprise application/license identification and rationalization • Elimination of outdated software 		

Figure A-2. Thin/zero-client computing objectives to standardize and centralize the computing environment

1-4 Scope

This annex applies to the thin/zero-client computing implementations in key locations that support the Generating Force computing environment (e.g., end-user devices, servers, applications, storage). The approach leverages 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 occur on the NIPRNet and the SIPRNet. Prioritization by leadership and funding availability will determine when sites receive thin/zero-client capability. Implementation plans must be aligned with the Active Directory forest way ahead and other ongoing initiatives to ensure appropriate operation.

Thin/Zero-Client Computing Model – Data Center (Back End). Today, back-end solutions fall into one of two basic categories.

(1) Virtual desktops provide server-based operating system and applications that are accessed by thin-client users as though they are remote computers. Optimally, all processing is done on the server and only keystrokes and screen refreshes pass over

the network. Virtualization simplifies software versioning and patch management, and enables centralized control of which applications the user is allowed to access on the workstation. These technologies are evolving, and the Army anticipates that, over time, more solutions will meet the requirements of this architecture.

(2) Streaming applications stream the server-based operating system (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.

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 system functions 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.

Annex A, Chapter 2 Thin/Zero-Client Computing

The Army Thin/Zero-Client Computing Annex defines the attributes required to implement this technology. It describes thin/zero client computing in the context of the DoD IEA, and is intended to guide the implementation of a standardized computing environment. This annex will serve as the primary guidance for Army organizations and programs in developing thin/zero client computing solution architectures. When implemented to the standards described in Appendix D of this RA, thin/zero-client computing contributes to strengthening the network security posture and, for larger user densities, reducing overall information technology operating costs over time. Figure A-3 below, Organizations and Architectural Relationships, depicts the reference architecture hierarchy, from DoD/JIE architectures to the Army Enterprise Architecture policy and guidance to PEO/PM-driven segment and solution architectures.

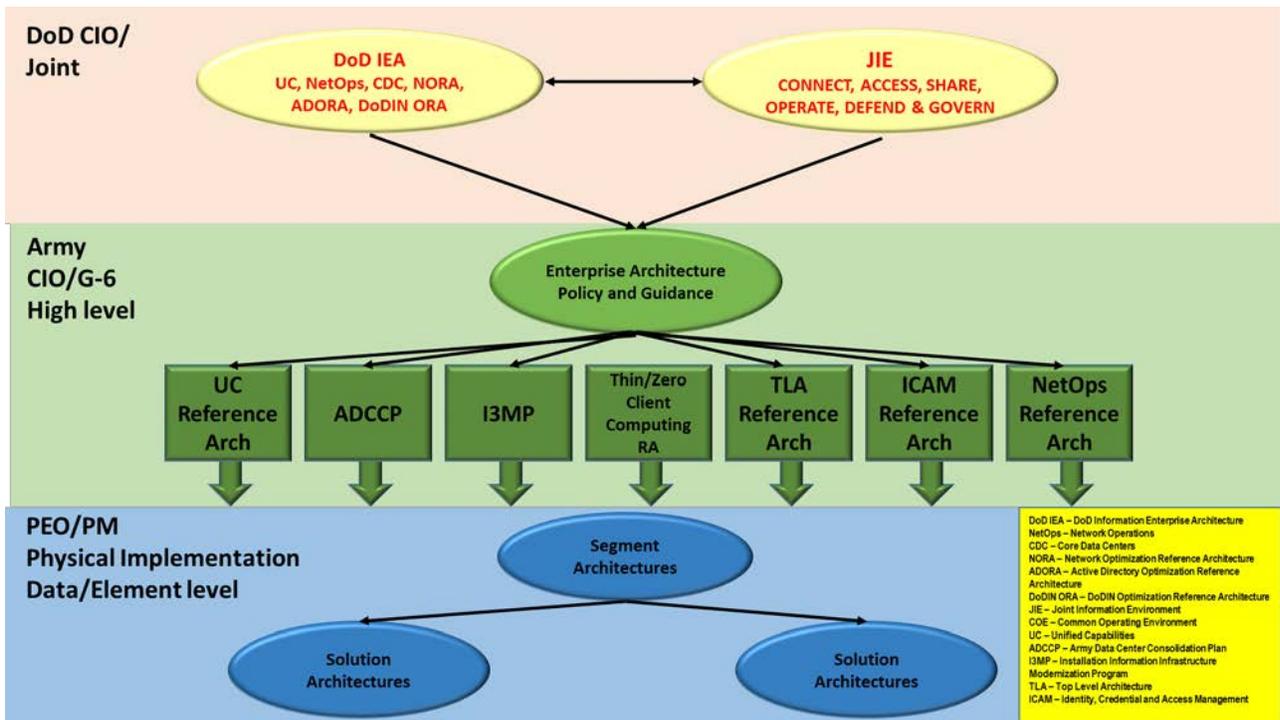


Figure A-3. Organizations and Architectural Relationships

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. These relationships are briefly described below.

DoD Information Enterprise Architecture (IEA), Version 2.0. The DoD IEA provides a clear, concise description of what the information enterprise must be and how its

elements should work together to accomplish transformation and deliver efficient, cost-effective information and services via the Joint Information Environment (JIE). 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. It describes the future vision for the information environment based on merging operational needs with the concepts previously embedded in separate net-centric strategies. The EUD RA is aligned with the DoD IEA, as shown in paragraph 2-2 (Thin/Zero-Client Computing Components), and within the principles and rules provided in Tables A-1 through A-6.

DoD Core Data Center Reference Architecture (CDC RA), Version 1.0. DoD CDC RA Version 1.0 provides direction in the form of principles, business rules, standards and architectural patterns. They are divided into five functional areas: facility infrastructure, computing infrastructure, security/information assurance, capability delivery and standardized operations and processes. Requirements are aligned with the JIE capability and security architectural guidance. The DoD CDC RA's organization of capabilities and specific requirements guides and informs the EUD RA, as shown in Figure A-4 (Thin/Zero-Client Computing Requirements Alignment to DoD IEA).

Common Operating Environment (COE). The Army Common Operating Environment 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 quick production and deployment of high-quality applications, simpler configuration, support and training, and lower costs.

Unified Capabilities (UC). Army Unified Capabilities are a secure suite of collaboration, real-time communications and supporting services, including email, 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.

Identity and Access Management (IdAM). IdAM is a critical service that must be integrated and synchronized with the delivery of thin/zero-client computing solutions. It comprises the following infrastructure and services: Public Key Infrastructure (PKI), Common Access Card (CAC) services, SIPR token services, claims-based authentication, enterprise authentication services, attribute-based access control, policy decision services and directory services. The DoD Enterprise Identity Attribute Service (EIAS) distributes DoD person, persona and personnel attributes to applications and services in a controlled, consistent and secure manner. The information provided via EIAS, which is managed by the Defense Manpower Data Center, can be used to confirm an individual's identity and affiliation to DoD for the purpose of enabling attribute-based access control. The hardware and software provided to the end user for thin/zero-client computing must enable the IdAM services listed above to meet Army security requirements.

Network Security. The Army maintains a security enclave boundary known as the Top Level Architecture (TLA). The TLA is the overarching architecture across the Army enterprise that integrates with the DoD Information Enterprise Architecture and serves as the interface to Installation Processing Nodes (IPN) and the Installation Campus Area Network (ICAN). The ICAN is the network interface connecting thin/zero-client computing end users to back-end applications and data resources. Security Technical Implementation Guides (STIGs) and National Security Agency Guides are the configuration standards for DoD information assurance (IA) and IA-enabled devices/systems. Since 1998, DISA Field Security Operations (FSO) have played a critical role in enhancing the posture of DoD's security systems by providing the STIGs, which contain technical guidance to "lock down" information systems/software that might otherwise be vulnerable to a malicious computer attack. DISA FSO are in the process of moving the STIGs toward the use of the National Institute of Standards & Technology Security Content Automation Protocol in order to automate STIG compliance reporting. Solution providers for Army thin/zero-client computing implementation on installations must ensure that these STIGs are incorporated into their solution architecture.

Army Data Center Consolidation Plan (ADCCP). The ADCCP consolidates Army data centers in order to cut operating costs and improve energy efficiency. The CIO/G-6 ADCCP team is designating as data centers the Installation Processing Nodes that will not be closed or regionally consolidated. IPNs will host installation-level data. Virtualization efforts, such as thin/zero-client computing, will also contribute to ADCCP objectives by standardizing the Army's hardware and software architecture. 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 informational, visit <https://www.us.army.mil/suite/page/643748>.

Installation Information Infrastructure - Communications and Capabilities (I3C2). The Installation Campus Area Network, provisioned through I3C2 as a part of the installation information infrastructure architecture, is critical to the success of thin/zero-client computing. A bandwidth analysis must 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.

Network Operations. Network operations establish, operate, manage, protect and defend the LandWarNet. They consist of three core functions: network and enterprise service management; cybersecurity and computer network defense; and information dissemination management and content staging. 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. Network operations provide commanders and users at all levels end-to-end network and information system visibility, protection and prioritization 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. Thin/zero-client computing implementation must be

designed to accommodate the suite of network operations tools being deployed by the Army and DoD.

2-2 Thin/Zero-Client Computing Components

Operational Model Overview. The Army’s thin/zero-client computing requirements are the basis for providing Army stakeholders enterprise-level technical direction for implementation of a standardized computing environment. These Army requirements are derived from the approved requirements document. Figure A-4, below, depicts DoD IEA and Core Data Center high-level requirements, and the alignment of Army thin/zero-client computing requirements.

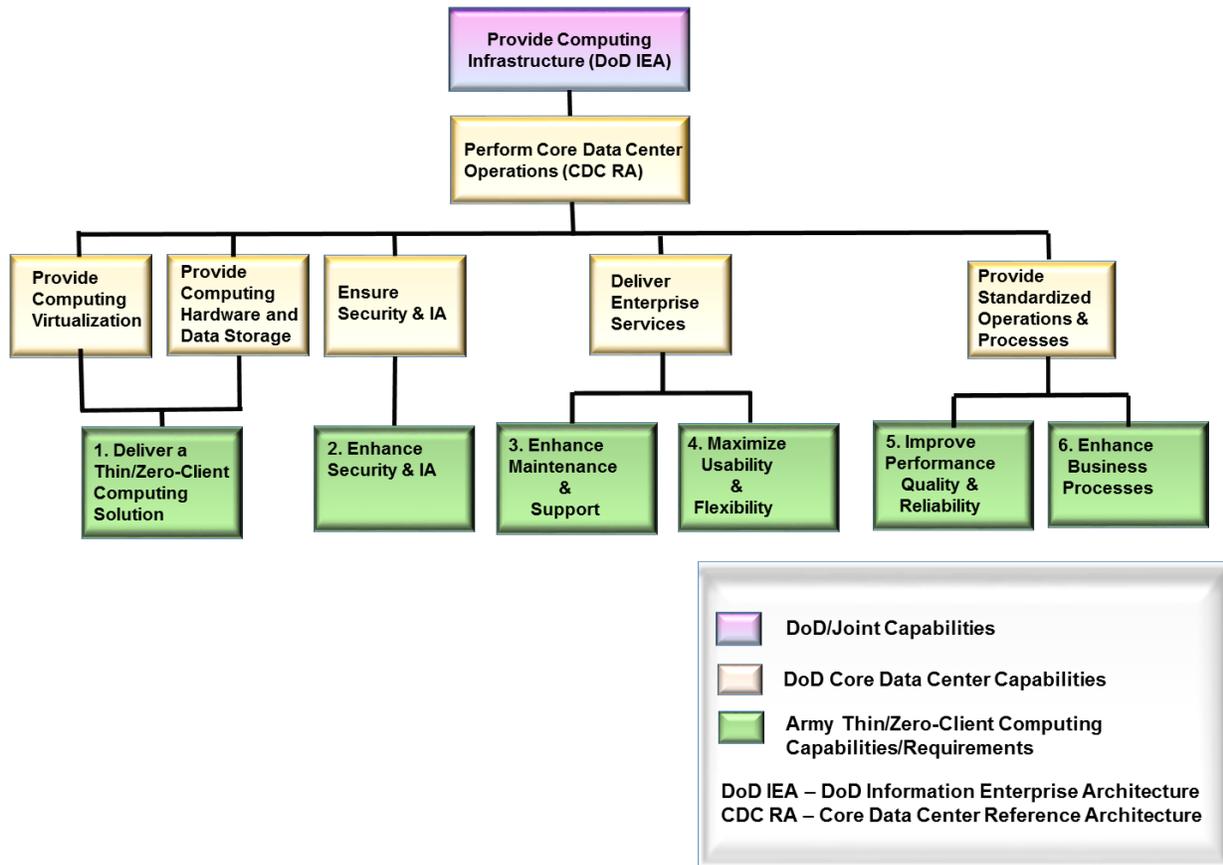


Figure A-4. Thin/zero-client Computing Requirements Alignment to DoD IEA

Operational Activities Model Overview. The Operational Activities Model describes the operations that are normally conducted in the course of achieving Army thin/zero-client computing mission or business goals, and the operational activities that are being conducted. The model will be used to:

UNCLASSIFIED

(1) Clearly delineate lines of responsibility for Army thin/zero-client computing activities.

(2) Uncover unnecessary operational activity redundancy.

(3) Make decisions about streamlining, combining or omitting activities.

(4) Define or flag issues, opportunities or operational activities and the interactions that need further analysis.

(5) Provide the foundation necessary for depicting activity sequencing and timing in the principles and business rules, as described in Tables 1-6.

Virtualization - Joint Information Environment (JIE). Alignment to a common set of virtualized services and functions, provided through a joint information infrastructure, will provide greater effectiveness and efficiency in executing the vision for the Army enterprise. Thin/zero-client computing enables the Army user through the establishment and control of processes, procedures and enterprise solutions that enhance:

(1) Connecting to the enterprise network anywhere, using the various end-user devices available to Army personnel and mission partners.

(2) Accessing information, services and other information assets, when needed, using various end-user devices available to Army personnel and mission partners.

(3) Sharing information and services throughout the Army enterprise, and providing global visibility and availability of information, services and other information assets.

(4) Optimization of the end-user capabilities described above by creating governance processes, policies and standards that ensure:

(a) Effective management of network performance and dynamic allocation of enterprise resources.

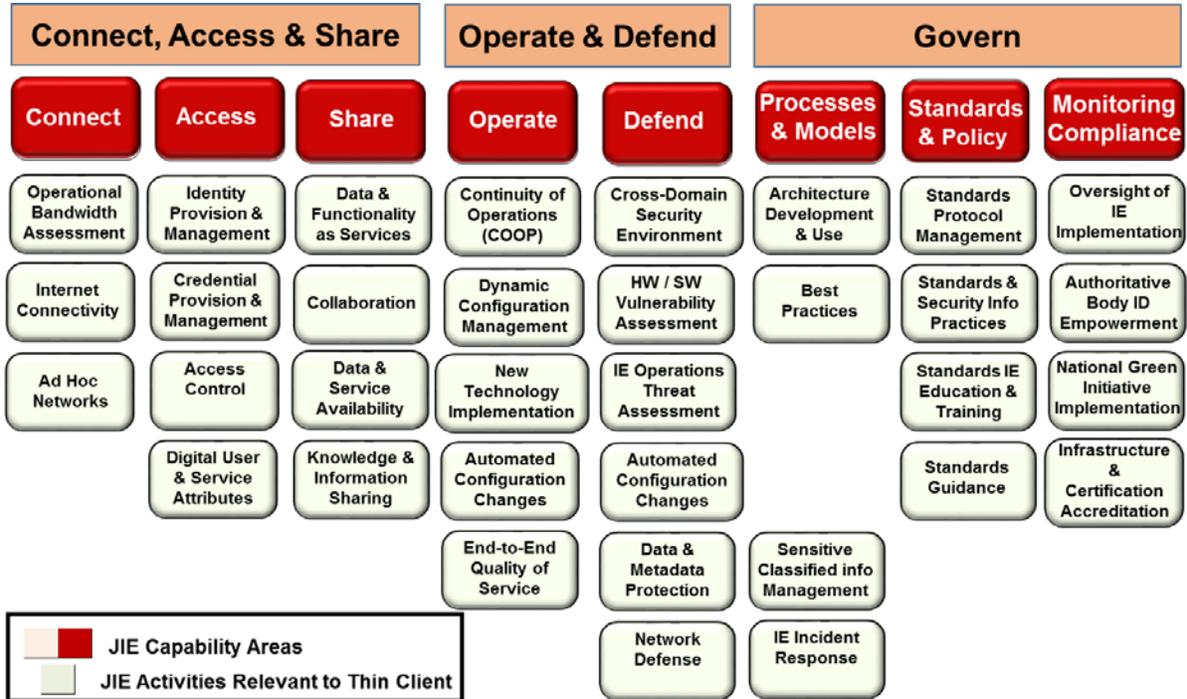
(b) Common access control for all users and devices throughout the Army enterprise.

(c) Cross-domain security and proactive network defense.

(d) Data security.

(e) Effective development and use of architecture.

The thin/zero-client activities relevant to JIE capabilities are depicted in Figure A-5, below. These activities will be updated as the JIE effort matures over time.



Reference: DoD IEA Volume 2, Version 2, dated July 2012

Figure A-5. Thin/zero-client Computing Alignment with JIE Capabilities

Annex A, Chapter 3 Thin/Zero-Client Computing Principles and Rules

3-1 Thin/Zero-Client Computing Capabilities Principles & Business Rules

Tables A-1 through A-6, below, reflect the alignment of Army CIO/G-6 high-level principles and business rules to DoD IEA Global Principles/Rules, as published in DoD IEA, Volume 2. They further associate Army principles and business rules with supporting technical positions and patterns to guide and constrain subsequent architectures. The tables represent the following major operational activities derived from the Thin/Zero-Client Computing Requirements Document.

- (1) Deliver a thin/zero-client solution.
- (2) Enhance security and information assurance.
- (3) Enhance maintenance and support.
- (4) Maximize usability and flexibility.
- (5) Improve performance quality and reliability.
- (6) Enhance business processes.

These rules and technical standards will guide thin/zero-client computing solution architecture technologies. The thin/zero-client computing technical positions and standards can be organized into certain patterns, as listed below. These patterns provide the framework for the technical standards presented in Appendix D (Technical Standards).

- (1) Virtualization of resources (e.g., operating systems, hardware, storage and central processing unit capacities).
- (2) Application formats and protocols.
- (3) Operating systems.
- (4) Storage.
- (5) Databases.
- (6) Information assurance.
- (7) Network perimeter protection (e.g., firewalls, intrusion detection/prevention).
- (8) Network interfaces (e.g., Internet Protocol routers, local area network switches).
- (9) Transport network (e.g., synchronous optical networking).
- (10) Virtual private networks (VPNs) (e.g., virtual local area networks, Internet Protocol/Multi-Protocol Label Switching, Border Gateway Protocol).
- (11) Quality of service (QoS).
- (12) Network management/operations.

3-2 Capability 1: Deliver an Army Thin/Zero Client Computing Solution

DoD IEA Principles and Business Rules Abbreviations.

GP – Global Principles

SIP – Shared Infrastructure Principles

SIR – Shared Infrastructure Business Rules

CIRP – Computing Infrastructure Readiness Principles

CIRR – Computing Infrastructure Readiness Business Rules

SAR – Shared Availability Rules

DoD IEA 2.0 capabilities and principle/business rules drive the Army principles, business rules and technical positions shown in Table A-1 below.

Table A-1. Deliver 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: DoDIN infrastructure resources shall be discoverable and available both to meet the dynamic demand of all mission requirements and to support DoDIN monitoring and management.	P1: Thin/zero-client computing will be designed to deliver computing services to all end users (thick, thin, zero) in order to meet mission requirements, and will not adversely affect existing operations, systems or missions.	R1.1: Thin/zero-client computing will virtualize server, storage and networking resources by placing computing devices, operating systems and applications on servers in the data center, using an open, standards-based architecture in accordance with DoD, Joint & Army requirements.	Thin-client back-end solutions fall into one of these categories: a) Terminal services, e.g., Microsoft remote desktop service b) Streaming operating system/applications c) Virtual desktops All operating systems, hardware, CPU capacities, storage and application resources of thin/zero-client computing servers and clients will be: available and discoverable (e.g., Universal Description, Discovery and Integration); and managed and monitored dynamically, using open technical standards (e.g., Open Virtualization Format or Simple Network Management Protocol).
		P1: Thin/zero-client computing will be designed to deliver computing services to all end users (thick, thin, zero) in order to meet mission requirements, and will not adversely affect existing operations, systems or missions.	R1.2: The thin/zero-client computing enterprise solution will be scalable to support 100% of SIPRNet users and 80% of NIPRNet users.	U.S. Army Unified Capabilities Reference Architecture, Version 2.0, 24 June 2015. http://ciog6.army.mil/Architecture/tabid/146/Default.aspx

UNCLASSIFIED

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>P1: Thin/zero-client computing will be designed to deliver computing services to all end users (thick, thin, zero) in order to meet mission requirements, and will not adversely affect existing operations, systems or missions.</p>	<p>R1.3: Power users (power usage is characterized by video, heavy graphics and/or complex, rapid screen rolling, as in large Excel spreadsheets, etc.) must be provisioned to support mission requirement (e.g., streaming media, Defense Collaboration Services, bi-directional audio and video, etc.) by providing proper engineering configuration for acceptable performance or determining criteria for remaining on a thick-client solution.</p>	

UNCLASSIFIED

DoD IEA 2.0 Capabilities	DoD IEA 2.0 Principle/Business Rules	Army Thin/Zero-Client Computing Principles (PR)	Business Rules (BR)	Technical Positions
Information Sharing with Mission Partners	Operational Rule 09: Edge users have direct information-sharing capabilities with peers outside their immediate organization, with central processing for their mission and strategic assets per their mission requirements.	P1: Thin/zero-client computing will be designed to deliver computing services to all end users (thick, thin, zero) in order to meet mission requirements, and will not adversely affect existing operations, systems or missions.	R1.4: Thin/zero-client computing will deliver core user applications to the end user at the same (or improved) level of performance and usability as the level provided by the status quo thick-client computing environment. These capabilities will include the ability to support video, data and audio. (QoS).	Thin/zero-client computing enhances performance and usability of client-server computing environments through dynamic sharing of resources on an on-demand basis, using open and market-based standards without being locked into specific resources (e.g., operating systems, hardware, software, storage, CPU capacities) of certain vendors that are statically allocated in non-interoperable environments.
		P1: Thin/zero-client computing will be designed to deliver computing services to all end users (thick, thin, zero) in order to meet mission requirements, and will not adversely affect existing operations, systems or missions.	R1.5: Thin/zero-client computing will be supported with a network infrastructure that is capable of migrating all system users' data and providing users 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 the client and server.

UNCLASSIFIED

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 discovered and accessed for virtual management and control across the DoDIN.	P1: Thin/zero-client computing will be designed to deliver computing services to all end users (thick, thin, zero) to meet mission requirements, and will not adversely affect existing operations, systems or missions.	R1.6: Provide the capability for remote users operating on thick, thin/zero or other clients on trusted or untrusted networks to access data and applications, and meet DoD/Army security requirements.	Thin/zero-client computing resources (e.g., operating systems, hardware, CPU capacities, storage and application software) of clients and servers will be discoverable, using open and common standards and repositories (e.g., UDDI) in open, standards-based (e.g., American National Standards Institute X.509, Framework for Implementing Files Systems 201, CAC, DoD Instruction 8520.03), secured environments.
Data & Functionality as Services	GP 01: DoD CIO-governed resources are conceived, designed, operated and managed to address the mission needs of the department.	P1: Thin/zero-client computing will be designed to deliver computing services to all end users (thick, thin, zero) in order to meet mission requirements, and will not adversely affect existing operations, systems or missions.	R1.7: Thin/zero-client computing will support all standard software included in the Army Golden Master (AGM) Program baseline and all validated above-baseline software required by the mission.	Market-based thin/zero-client computing technical standards (e.g., virtualization software) related to the operating systems, hardware, CPU capacities, storage and applications of servers and clients that will be part of the AGM are needed to enhance reliability, security, interoperability and economies of scale through virtualization of computing environments.

UNCLASSIFIED

DoD IEA 2.0 Capabilities	DoD IEA 2.0 Principle/Business Rules	Army Thin/Zero-Client Computing Principles (PR)	Business Rules (BR)	Technical Positions
		P1: Thin/zero-client computing will be designed to deliver computing services to all end users (thick, thin, zero) in order to meet mission requirements, and will not adversely affect existing operations, systems or missions.	R1.8: Provide and allocate sufficient random access memory (RAM) to enable user productivity at the same level as provided by the status quo thick-client computing environment.	The PM will determine system requirements to meet performance criteria.
		P1: Thin/zero-client computing will be designed to deliver computing services to all end users (thick, thin, zero) in order to meet mission requirements, and will not adversely affect existing operations, systems or missions.	R1.9: Support approved peripherals attached locally to the client device (e.g., via USB), to include printers, CAC/token readers, scanners and multifunction devices.	All thin-client solutions must support common applications, including: -CAC/token authentication to Active Directory (login) -CAC-enabled web server login, email signature and encryption -Defense Travel System
		P1: Thin/zero-client computing will be designed to deliver computing services for all end users (thick, thin, zero) to meet mission requirements, and will not adversely affect existing operations, systems or missions.	R1.10: Support networked services, to include printers, scanners, multifunction devices and data storage.	

UNCLASSIFIED

DoD IEA 2.0 Capabilities	DoD IEA 2.0 Principle/Business Rules	Army Thin/Zero-Client Computing Principles (PR)	Business Rules (BR)	Technical Positions
Hardware/Software Vulnerability Assessments and Information Environment Operational Threat Assessments	SAR 05: DoDIN assets must establish and implement a mission assurance capability that addresses hardware, software and supplier assurance through engineering and vulnerability assessments.	P2: The capability will not adversely affect existing operations, systems or missions.	R2.1: 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., virtualization software) and will provide interoperability between heterogeneous operating systems, hardware, software and storage networks via virtualization, which will facilitate the graceful migration of existing systems to new ones.

UNCLASSIFIED

DoD IEA 2.0 Capabilities	DoD IEA 2.0 Principle/Business Rules	Army Thin/Zero-Client Computing Principles (PR)	Business Rules (BR)	Technical Positions
Identity & Provisioning 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 access control rules and quality of protection requirements for all individuals, organizations, chief information officers (CIOs), automated services and devices.	P3: Thin/zero-client computing will provide controlled user access to the NIPRNet and SIPRNet to meet mission requirements.	R3.1: Thin/zero-client computing solutions will comply with Army IdAM requirements for controlled access to NIPRNet and SIPRNet. For more information see the IdAM RA.	A market-based thin/zero-client computing storage virtualization standard will be part of AGM. It will have a firewall and intrusion detection/prevention system in SIPRNet/NIPRNet environments, and will allocate storage dynamically according to demand.
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 DoDIN configuration processes.	P4: Enable the Army regional construct (e.g., Regional Cyber Centers) to quickly deploy new capabilities while centrally managing controls and configurations.	R4.1: Configuration management of the system shall allow change requests for each system to be channeled through standard Command structures.	

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	<p>Operational Rule 24: Develop common standards and policies that serve as enforcement mechanisms to ensure interoperability.</p> <p>Operational Rule 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>	P5: Thin/zero-client computing planning and implementation must synchronize with other Army/DoD/federal IT initiatives to ensure interoperability, compatibility and compliance.	R5.1: 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., virtualization software).

Delivery of Thin/Zero-Client Computing Capability Facts and Assumptions.

- (1) Mission success is the first priority.
- (2) 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.
- (3) The Army will operate in an enterprise environment in accordance with DoD IEA guiding principles.
- (4) The thin/zero-client computing capability will maximize utilization of ongoing Army virtualization efforts.
- (5) The Installation Campus Area Network will enable the thin/zero-client computing capability.
- (6) Virtualization will contribute to interoperability as common infrastructure, repositories and registries and standard security solutions are achieved.

Delivery of Thin/Zero-Client Computing Capability Constraints.

(1) The traditional thick-client common peripherals (e.g., DVD, compact disc, digital scanner, etc.) must be provided separately as standalone units, as required by the mission. (Note: The Army must adhere to the USB moratorium, and must replace legacy printers with parallel technology.)

(2) The Army must provide training to all users.

(3) 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 operating system.

(4) Local processing power necessitates more intensive monitoring to prevent users' 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 when connected to the network.

(5) The thin/zero-client computing capability must be compatible and operate within Army network operations tool functionality (i.e., discovery, monitoring, management, etc.).

(6) Thin/zero-client solutions outside of the post, camp and station must use a proxy in the Demilitarized Zone.

(7) Thin/zero-client solutions that implement a terminal server infrastructure must support Remote Desktop Protocol or the Independent Computing Architecture protocol to allow connection to a terminal server.

(8) If the thin-client device is running on the Microsoft operating system, it must emulate the desktop Army Golden Master as listed for the Windows Baseline Software Configuration.

(9) Thin-client solutions must comply with Executive Order 13423, Electronic Product Environmental Asset Tool requirements. Reference Section 2h. For more information, visit: <http://www.epa.gov/oaintrnt/practices/eo13423.htm>. (TA 2010-001, 10 Sep 10, p9, 4.3-a.)

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

Delivery of Thin/Zero Client Computing Capabilities 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 offline 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 Continuity of Operations Plan (COOP) and disaster recovery (DR) 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 and computing environment.

Risk Area: Testing. Testing of the objective solution outside the government computing environment would be inadequate.

Mitigation: Ensure that 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 implementation.

Mitigation: The Army develops and implements strategic messages as solutions are developed to communicate the importance of thin/zero-client computing to end users.

Risk Area: Inadequate Performance for Power Users. Power usage is characterized by video, 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 have with a thick-client solution.

Mitigation: Create a criteria baseline, based on end users' mission requirements, to determine whether they are candidates for migration from thick-client to thin/zero-client computing. Test power-user requirements to determine the parameters for users classified as power users versus others.

3-3 Capability 2: Enhance Security and Information Assurance

Table A-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 DoDIN 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 and non-governmental organizations, and academic, research and business partners.	P6: The Army will ensure compliance with DoD Directives and accreditation requirements through the implementation of an effective defense in-depth strategy and enforcement of cybersecurity strategies that provide protection, detection, reaction and restoration (PDRR) capabilities.	R6.1: Meet the information assurance controls and requirements specified in DoD Directive 8500.01, DoD Instruction 8500.02 and Army Regulation (AR) 25-2, based on Mission Assurance Category level and sensitivity level.	Virtual environments created by thin/zero-client computing will be based on market standards that provide server-based centralized configuration control of operating systems, hardware and software. Thin/zero-client computing security will use IdAM RA technical standards.

UNCLASSIFIED

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>P6: The Army will ensure compliance with DoD Directives and accreditation requirements through the implementation of an effective defense-in-depth strategy and enforcement of cybersecurity strategies that provide PDRR capabilities.</p>	<p>R6.2: For connecting to the SIPRNet, multi-level security, cross-domain solutions (CDS) adhere to requirements outlined at http://www.disa.mil/Cybersecurity/Cross-Domain-Enterprise-Services and allow single-level, secure, cross-domain connectivity (e.g., NIPRNet to the Defense Research and Engineering Network).</p>	<p>DISA's Cross-Doman Enterprise Services (CDES) provide support to Combatant Commands, Services and agencies by implementing, fielding and providing life-cycle support for cross-domain solution technologies that provide secure interoperable capabilities throughout DoD. In addition, thin/zero-client computing will adhere to CDS SIPRNet cybersecurity requirements.</p>
		<p>P6: The Army will ensure compliance with DoD Directives and accreditation requirements through the implementation of an effective defense-in-depth strategy and enforcement of cybersecurity strategies that provide PDRR capabilities.</p>	<p>R6.3: Comply with Army data-at-rest requirements and all applicable DoD and Army security policies and regulations.</p>	
		<p>P6: The Army will ensure compliance with DoD Directives and accreditation requirements through the implementation of an effective defense-in-depth strategy and enforcement of cybersecurity strategies that provide PDRR capabilities.</p>	<p>R6.4: Communications security handling procedures related to thin/zero clients must meet the requirements of AR 380-40 (Safeguarding and Controlling Communications Security Material (U, restricted distribution)).</p>	

UNCLASSIFIED

DoD IEA 2.0 Capabilities	DoD IEA 2.0 Principle/Business Rules	Army Thin/Zero-Client Computing Principles (PR)	Business Rules (BR)	Technical Positions
Oversight of Information Enterprise (IE) Implementation	Operational Rule 23: Develop enterprise acquisition and certification to ensure that purchased and acquired IE components are interoperable and universally certified.	P7: Be accredited through the DoD Risk Management Framework.	R7.1: The capability solution will comply with the applicable Army and DoD Approved Products Lists.	Thin/zero-client computing products will comply with open and market-based technical standards that are part of the Army and DoD Approved Products Lists.
		P7: Be accredited through the DoD Risk Management Framework.	R7.2: Operate using only software with an approved Certificate of Networkiness (CON) and vendor patch update support.	Thin/zero-client computing market-based virtualization technical standards (as a part of AGM) and open, standards-based cybersecurity (under DISA) will facilitate operations within the Army and DoD IA Frameworks, including validation through a standard security engineering process.
Identity Provisioning & Management	SAR 07: All DoD information services and applications must uniquely and persistently digitally identify and authenticate users and devices. 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, automated services and devices.	P7: Be accredited through the DoD Risk Management Framework.	R7.3: Provide the capability to block restricted users from storing data on a client device. It shall have the capability for the operating system 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 cybersecurity policy.	

UNCLASSIFIED

DoD IEA 2.0 Capabilities	DoD IEA 2.0 Principle/Business Rules	Army Thin/Zero-Client Computing Principles (PR)	Business Rules (BR)	Technical Positions
Cybersecurity Policy Compliance & Standard Engineering Practices in Accordance with System-of-Systems Engineering (SoSE) Guidelines	SAR 09: DoD programs must demonstrate that the network, data assets, services, applications and device settings that control or enable cybersecurity functionality have been established, documented and validated through a standard security engineering process.	P7: Be accredited through the DoD Risk Management Framework.	R7.4: 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 cybersecurity (under DISA) will ensure that operations within the Army and DoD IA Frameworks include validation through a standard security engineering process.
		P7: Be accredited through the DoD Risk Management Framework.	R7.5: The solution will restrict access to the virtualization management system to authorized administrators.	

UNCLASSIFIED

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 Guidance	SAR 02: DoDIN 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.	P7: Be accredited through the DoD Risk Management Framework.	R7.6: 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 implementation of client-server-based computing architecture, where all virtualization services are controlled from the centralized servers located in 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 to meet 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.	P7: Be accredited through the DoD Risk Management Framework.	R7.7: 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 cybersecurity technical standards will support CDS, protecting data in transit and at rest according to their confidentiality level, Mission Assurance category and level of exposure.

UNCLASSIFIED

DoD IEA 2.0 Capabilities	DoD IEA 2.0 Principle/Business Rules	Army Thin/Zero-Client Computing Principles (PR)	Business Rules (BR)	Technical Positions
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.	P7: Be accredited through the DoD Risk Management Framework.	R7.8: The capability will support CAC/Public Key Infrastructure (PKI) and Secure Token via an interface internal or external to the client device.	Thin/zero-client computing cybersecurity architecture will support IdAM RA technical standards, to include CAC/PKI and Secure Token, via an interface internal or external to the client device. Core standards.
Infrastructure Certification & Accreditation	SAR 09: DoD programs must demonstrate that their network, data assets, services, applications and device settings that control or enable cybersecurity functionality have been established, documented and validated through a standard security engineering process.	P8: Ensure that network, data connections and end-user devices are compliant with cybersecurity requirements and have been validated through a standard security engineering process.	R8.1: Ensure and document engineering acceptance documents' security configurations in addition to AGM security guidelines in accordance with STIGs and NSA security guidelines.	Thin/zero-client computing market-based virtualization technical standards (as a part of AGM) and open standards-based cybersecurity (under DISA) will facilitate Army and DoD certification and accreditation (C&A).

UNCLASSIFIED

DoD IEA 2.0 Capabilities	DoD IEA 2.0 Principle/Business Rules	Army Thin/Zero-Client Computing Principles (PR)	Business Rules (BR)	Technical Positions
Identity Provisioning & Management	SAR 07: All DoD information services and applications must uniquely and persistently digitally identify and authenticate users and devices. 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.	P9: End users and devices must be uniquely and persistently digitally identified and authenticated in accordance with Army cybersecurity policies and IdAM RA requirements.	R9.1: Support required PKI, SIPR token or current approved authentication method middleware.	Thin/zero-client computing cybersecurity architecture supports IdAM RA technical standards.
		P9: End users and devices must be uniquely and persistently digitally identified and authenticated in accordance with Army cybersecurity policies and IdAM RA requirements.	R9.2: Support authentication to the NIPRNet and SIPRNet.	DoDI 8520.03 establishes and defines sensitivity level for the purpose of determining appropriate authentication methods and mechanisms.
		P9: End users and devices must be uniquely and persistently digitally identified and authenticated in accordance with Army cybersecurity policies and IdAM RA requirements.	R9.3: Provide the capability for a user to sign and encrypt email.	

UNCLASSIFIED

DoD IEA 2.0 Capabilities	DoD IEA 2.0 Principle/Business Rules	Army Thin/Zero-Client Computing Principles (PR)	Business Rules (BR)	Technical Positions
		P9: End users and devices must be uniquely and persistently digitally identified and authenticated in accordance with Army cybersecurity policies and IdAM RA requirements.	R9.4: Support access to websites by authenticating via PKI, SIPR token or other current approved authentication methods.	Core Standards: CAC PKI. Alternate non-CAC PKI.
		P9: End users and devices must be uniquely and persistently digitally identified and authenticated in accordance with Army cybersecurity policies and IdAM RA requirements.	R9.5: Support digital signatures and provide the capability for users to digitally sign and encrypt documents.	
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 or organizational level (e.g., DoD Component), then at the service or application level.	P10: 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).	R10.1: Provide the capability to correct the unauthorized transmission of classified data to a lower-classified network (spillage).	Thin/zero-client-computing cybersecurity technical standards (e.g., IdAM 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 or organizational level). Thin/zero-client computing cybersecurity technical standards (e.g., IdAM RA technical standards) support cross-domain solutions' correcting the unauthorized transmission of classified data to a lower-classified network (spillage).

Enhance Security and Information Assurance Facts and Assumptions.

- (1) Eighty percent of network security compromises occur at the client device.
- (2) Thin/zero-client computing will facilitate a more secure network for the Army by providing Information Assurance Vulnerability Alert (IAVA) patch consistency, containment (of spillage), data recovery and streamlined network management and operations (defend, detect and react).
- (3) Thin/zero-client computing will comply with federal, DoD and Army Regulations (e.g., mandated Host-Based Security System use).
- (4) Thin/zero-client computing will increase the potential impact of system compromise because each user shares computing resources; therefore, infiltration of a single user's system is equivalent to system-wide infiltration.

Enhance Security and Information Assurance Constraints.

- (1) Personnel providing accreditation of cybersecurity systems' procurement/fielding and cybersecurity support shall meet training and certification requirements identified in DoD Instruction 8500.2 and DoD 8570.01-M.
- (2) In environments where a protective distribution system is required to protect cabling, provisions must be taken to comply with published requirements (see National Security Telecommunications and Information Systems Security Instruction No. 7003, Protected Distribution System, 13 December 1996, <http://www.networkintegritysystems.com/nstissi-7003/>; and AR 380-27, Control of Compromising Emanation, 22 July 2014, https://armypubs.us.army.mil/epubs/DR_pubs/DR_c/pdf/r380_27.pdf).
- (3) Network ports, protocols and services (PPS) must be approved by the Theater Network Operations and Security Center.
- (4) Network ports for NIPRNet and SIPRNet must be allowed by DISA. Check <http://iase.disa.mil/policy-guidance/Lists/Ports%20and%20Protocols/AllItems.aspx> for the category assurance list and port status.
- (5) Local processing power necessitates more-intensive monitoring to prevent users' circumventing security controls. A thin client must not operate its full-capacity operating system.

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 network operations tools and management processes.

3-4 Capability 3: Enhance Maintenance and Support

Table A-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.	P11: Thin/zero-client computing platforms, applications and services will interoperate with other similar Army and DoD systems, and decrease cost and complexity of operations.	R11.1: The capability will be suitable for operation and maintenance (O&M) via existing Army O&M policies and processes.	Established technical standards (e.g., OVF, SNMP) will facilitate operation of thin/zero-client computing data assets, services, applications and device settings that control or enable cybersecurity functionality.
		P11: 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.	R11.2: Enable at least as efficient O&M as the status quo (thick-client computing environment).	Cost-benefit analysis that supports the specific implementation.

UNCLASSIFIED

DoD IEA 2.0 Capabilities	DoD IEA 2.0 Principle/Business Rules	Army Thin/Zero-Client Computing Principles (PR)	Business Rules (BR)	Technical Positions
Dynamic Configuration Management	CIRR 06: Shared computing and data storage resources can be discovered and accessed for virtual management and control across the DoDIN.	P11: Thin/zero-client computing platforms, applications and services will interoperate with other similar Army and DoD systems, and decrease cost and complexity of operations.	R11.3: Thin/zero-client computing will allow for the efficient use of data storage capacity, and leveraging of vendor tools to implement, manage, support and sustain service levels.	Thin/zero-client computing virtualizes computing infrastructure resources (e.g., storage, CPU capacities, operating systems, hardware, software), including storage, using market-based standards (e.g., virtualization software). All thin/zero-client computing resources, including storage, can be discovered using technical standards (e.g., UDDI) and can be accessed using cybersecurity and other procedures.
		P11: Thin/zero-client computing platforms, applications and services will interoperate with other similar Army and DoD systems, and decrease cost and complexity of operations.	R11.4: Thin/zero-client computing will establish virtual application libraries, allowing Army-wide release management of applications and synchronization among libraries.	
		P11: Thin/zero-client computing platforms, applications and services will interoperate with other similar Army and DoD systems, and decrease cost and complexity of operations.	R11.5: Support the use of thin-client devices with a longer life cycle than status quo thick clients.	

DoD IEA 2.0 Capabilities	DoD IEA 2.0 Principle/Business Rules	Army Thin/Zero-Client Computing Principles (PR)	Business Rules (BR)	Technical Positions
		P11: Thin/zero-client computing platforms, applications and services will interoperate with other similar Army and DoD systems, and decrease cost and complexity of operations.	R11.6: Enable central management and programming of technical refresh (life-cycle replacement) of end-user computing equipment.	
		P11: Thin/zero-client computing platforms, applications and services will interoperate with other similar Army and DoD systems, and decrease cost and complexity of operations.	R11.7: Configuration management of the capability shall allow change requests for each system to be channeled through standard Command structures.	

Enhance Maintenance and Support Facts and Assumptions.

- (1) Implementation of thin/zero-client computing will simplify patch, IAVA and application (load set) management.
- (2) The implementation of thin/zero-client computing will enable the addition and upgrade of applications with less overall administrative effort.
- (3) The implementation of thin/zero-client computing will reduce software and software licenses.
- (4) The implementation of thin/zero-client computing will simplify end-user device management and administration.

Enhance Maintenance and Support Constraints. Any back-end solution using Microsoft Windows Server software shall use the AGM to the maximum extent possible.

Enhance Maintenance and Support Risks.

Risk Area: Platform diversity increases O&M complexity.

Mitigation: Centralized management of thin/zero-client computing implementation will decrease platform diversity and O&M complexity.

3-5 Capability 4: Maximize Usability and Flexibility

Table A-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 DoD is a strategic goal. All parts of the DoDIN 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. DoD achieves infrastructure interoperability through definition and enforcement of standards and interface profile, and implementation guidance.	P12: 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.	R12.1: Deliver a single Army standard desktop environment to thin-client users, agnostic of the user's client hardware.	See Appendix D of this RA.
Standard Protocol Management	Operational Rule 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.	P12: 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.	R12.2: 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 operating systems, hardware and software used by Army and DoD systems.
Standard Protocol Management	Operational Rule 24: Develop common standards and policies that serve as enforcement mechanisms to ensure interoperability.	P12: 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.	R12.3: Support clients running Microsoft Windows in accordance with Army policy.	Virtual environments created by thin/zero-client computing, based on market standards, facilitate support for existing operating systems used by the Army and DoD, and will be included in the Army Golden Master Program.

Maximize Usability and Flexibility Facts and Assumptions. Thin/zero-client hardware solutions will be hardware agnostic.

Maximize Usability and Flexibility Constraints.

(1) The solutions provider will limit the number of architecture solutions to one per installation.

(2) Solutions must be scalable to 100 percent of the SIPRNet population in the Army and 80 percent of NIPRNet users.

(3) Solutions for thin/zero client will be limited to a minimal number across the Army enterprise.

3-6 Capability 5: Improve Performance Quality and Reliability

Table A-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.	P13: 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.	R13.1: 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 implementation of a client/server-based computing architecture in which all virtualization services (e.g., operating systems, hardware and software) are controlled from the centralized servers located in data centers. Servers/data centers can be geographically distributed, facilitating disaster recovery and continuity of operations for the virtual environment.

UNCLASSIFIED

DoD IEA 2.0 Capabilities	DoD IEA 2.0 Principle/Business Rules	Army Thin/Zero-Client Computing Principles (PR)	Business Rules (BR)	Technical Positions
Continuity of Operations	SIP 01: DoDIN 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.	P14: The client architecture (software and hardware) must be highly available to eliminate single points of failure.	R14.1: The quality of service will be capable of availability and uptime of 99.99%.	Thin/zero-client computing technical standards facilitate implementation of a client/server-based computing architecture in which all virtualization services (e.g., operating systems, hardware and software) are controlled from the centralized servers located in data centers. 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: DoDIN 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.	P14: The client architecture (software and hardware) must be highly available to eliminate single points of failure.	R14.2: 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.	

UNCLASSIFIED

DoD IEA 2.0 Capabilities	DoD IEA 2.0 Principle/Business Rules	Army Thin/Zero-Client Computing Principles (PR)	Business Rules (BR)	Technical Positions
Continuity of Operations	SIP 01: DoDIN 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.	P15: Comply with published DoD and Army guidelines for service, disaster recovery and storage of mission data.	R15.1: The capability shall be able to support disaster recovery (DR) and COOP plans for mission-critical infrastructure and information, based on Mission Assurance Category and sensitivity level.	<p>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.</p> <p>COOP plans for consideration:</p> <p>Alternate Site Plan(s) - A plan to recover technology services at another location. Hardware and software are controlled from the centralized servers located in data centers, where servers/data centers can be geographically distributed, facilitating disaster recovery and COOP for the virtual environment.</p> <p>Data Center Recovery - A plan to restore the data center at its current location.</p> <p>Vital Records Management - A plan to secure and retrieve information.</p> <p>Security - A plan to secure information from internal and external threats.</p>

UNCLASSIFIED

DoD IEA 2.0 Capabilities	DoD IEA 2.0 Principle/Business Rules	Army Thin/Zero-Client Computing Principles (PR)	Business Rules (BR)	Technical Positions
	DoD CDC RA Table 4, Rule 6: IT services and applications hosted in the computing services provider environment must include robust systems management and monitoring.	P15: Comply with published DoD and Army guidelines for service, disaster recovery and storage of mission data.	R15.2: 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>TIA 942-2012 Telecommunications Infrastructure Standard for Data Centers. http://www.freestd.us/soft4/4437943.htm</p> <p>Universal System Restore software rebuilds complete partitions, regardless of the platform.</p> <p>Thin/zero-client computing technical standards facilitate implementation of a client/server-based computing architecture in which all virtualization services (e.g., operating systems, hardware and software) are controlled from the centralized servers located in data centers. 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>
	DoD CDC Table 4, Rule 7: Data centers that provide enterprise hosting as a managed service for applications must, at a minimum, provide cybersecurity backup, continuity of operations and disaster recovery services.	P15: Comply with published DoD and Army guidelines for service, disaster recovery and storage of mission data.	R15.3: The implementer will ensure that the selected vendors provide a system warranty when fielding the system.	<p>TIA 942-2012 Telecommunications Infrastructure Standard for Data Centers. http://www.freestd.us/soft4/4437943.htm</p> <p>Thin/zero-client computing technical standards facilitate implementing a client/server-based computing architecture in which all virtualization services (e.g., operating systems, hardware and software) are controlled from the centralized servers located in data centers. Servers/data centers can be geographically distributed, facilitating disaster recovery and COOP for the virtual environment.</p>

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.

Improve Performance Quality and Reliability Constraints.

(1) Defense Collaboration Services (DCS) require bi-directional audio and video. If not available, thin/zero-client computing must provide the proper engineering configuration for acceptable performance.

(2) Some power users may continue to require thick clients to support streaming media and the need for high availability of applications and data in degraded communications environments.

Improve Performance Quality and Reliability Risks.

Risk Area: Performance quality will be affected with limited scalability. The challenge for the solution provider is the balance between optimizing resources with scalability in order 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.

3-7 Capability 6: Enhance Business Processes

Table A-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 discovered and accessed for virtual management and control across the DoDIN.	P16: Thin/zero-client computing implementation will enhance the Army's ability to discover and access LandWarNet assets through virtual management and control across the enterprise.	R16.1: The capability will increase Headquarters, Department of the Army (HQDA) visibility of computing assets and software licenses.	Thin/zero-client computing virtualizes computing infrastructure resources (e.g., storage, CPU capacities, operating systems, hardware and software).
		P16: Thin/zero-client computing implementation will enhance the Army's ability to discover and access LandWarNet assets through virtual management and control across the enterprise.	R16.2: Change requests for implementation of thin/zero-client computing requirements or solutions shall be governed by the Army Business Council (ABC) approval process.	

UNCLASSIFIED

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>P17: 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.</p>	<p>R17.1: 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.</p>	
		<p>P18: Thin/zero-client computing implementation funding requirements, to include O&M for tech refresh, will be submitted to the CIO/G-6 in accordance with the PPBE process.</p>	<p>R18.1: The PM shall develop a technology refresh strategy, identify to the CIO/G-6 the programmed funding required to support it, and provide technical refresh as required.</p>	

UNCLASSIFIED

DoD IEA 2.0 Capabilities	DoD IEA 2.0 Principle/Business Rules	Army Thin/Zero-Client Computing Principles (PR)	Business Rules (BR)	Technical Positions
		P18: Thin/zero-client computing implementation funding requirements, to include O&M for tech refresh, will be submitted to the CIO/G-6 in accordance with the PPBE process.	R18.2: The PM shall be responsible for developing technical, engineering, architectural, operational, implementation, transition, acquisition and sustainment documentation, as indicated by regulation and other statutory guidance.	
		P18: Thin/zero-client computing implementation funding requirements, to include O&M for tech refresh, will be submitted to the CIO/G-6 in accordance with the PPBE process.	R18.3: The capability will have fully developed tactics, techniques and procedures for system use, implementation, integration, operation and maintenance prior to system installation and fielding.	

Enhance Business Process Requirements Facts and Assumptions.

- (1) The Thin/Zero-Client Computing Requirements Document will be approved by the Army Business Council Three-Star Board.
- (2) An ASA(ALT) Program Manager will design and Second Army will implement the thin/zero-client computing enterprise service solution.
- (3) The PM will develop the acquisition strategy and establish cost, schedule and performance metrics.
- (4) The Cost Review Board will review the PM plan and develop the Army Cost Position.
- (5) The Deputy for Acquisition and Systems Management will review the thin/zero-client computing acquisition strategy and cost position for readiness to proceed to the Army Systems Acquisition Review Council.
- (6) The SIPRNet thin/zero-client implementation has been validated as critical. The NIPRNet implementation, which is within the scope of this RA, has been validated as competing with other priorities.

Enhance Business Process Requirements Constraints.

- (1) Information Technology Infrastructure Library (ITIL) processes will be considered in the development of business processes and implementation.
- (2) Second Army will assist the PM in the selection of thin-client technologies; and standardize the solutions, including proper sizing, risk mitigation and security standards, to reduce vendor dependencies that are acceptable to AEN operations.
- (3) Software and hardware (e.g., commercial off-the-shelf equipment, routers, switches, phones, etc.) must be ordered through Army Computer Hardware, Enterprise Software and Solutions (CHESS) in order to standardize equipment, improve interoperability and reduce cost.
- (4) Requirements for all non-CHESS equipment must be approved via a waiver with a rationale/justification that explains the extenuating circumstances or unique configurations.
- (5) Implementation of thin/zero-client computing capabilities on an Army post/camp/station with IT services provided by a local Network Enterprise Center must follow TA 2010- 001 Technical Guidance. (TA 2010-001, 10 September 2010.)
- (6) Individual organizations must coordinate with their headquarters (i.e., G-6/S-6, Second Army) to implement the SIPRNet and NIPRNet thin-client infrastructure and acquisition strategy. (TA 2010-001, 10 September 2010.)
- (7) 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 September 2010, pg. 7, g.)

(8) Deviations from the standard enterprise thin-client configurations/guidance will be submitted to Second Army through Command channels. Following analysis to determine interoperability, security and O&M impacts, Second Army will submit its recommendations to the Army Business Council for approval.

(9) The thin-client solution must follow the DoD acquisition process, to include provisions addressing cybersecurity throughout the acquisition life cycle. (TA 2010-001, 10 September 2010, pg. 11, 4.4i; DoDD 5000.1, Defense Acquisition System.)

(10) Application owners are responsible for transitioning current applications that must be supported in a zero/thin-client environment, to include mobile EUDs.

Enhance Business Process Requirements Risk.

Risk Area: Lack of clarity in the performance work statement creates lack of synchronization with modifications, which causes a schedule slip and cost overruns.

Mitigation: Establish a PM and contracting agency, and build adequate time into the overall execution plan for contracting actions.

Solutions for thin/zero-client will be limited to a minimal number across the Army enterprise.

Administrative Information

Approval Authority. HQDA CIO/G-6.

Distribution and Use Restrictions. This document is intended for use by U.S. Government agencies and their Contractors doing business with the U.S. Army.

Document Custodian. The Custodian for this document is CIO/G-6, SAIS-AEA, usarmy.pentagon.hqda-cio-g-6.list.architecture@mail.mil.

-----Nothing follows-----