

---

# USACCESS Program



## READY! Guide

Version 1.5

October 18, 2007

CM # : GSA-DI-0000164-1.4.0



## Revision Chart

Version	Description of Version	Date Completed
1.0	Create document	May 29, 2007
1.2	Revise with input from Deployment Working Group and Network Architect.	July 1, 2007
1.3	Significant additions include the following: <ul style="list-style-type: none"> <li>• Sample configuration diagrams</li> <li>• Power requirements</li> <li>• Activator role</li> <li>• Site Roles &amp; Processes                             <ul style="list-style-type: none"> <li>○ Credentialing Center POC</li> <li>○ Smartcard Receiving &amp; Handling Process</li> <li>○ Escort Process</li> </ul> </li> </ul>	July 15, 2007
1.4	Updated with lessons learned	July 29, 2007
1.5	Significant changes to IT Requirements include: <ul style="list-style-type: none"> <li>• Removed 5505 reference</li> <li>• Added Cisco 3002 VPN Router</li> <li>• Added Linksys 2008 Switch</li> <li>• Added diagrams for network connection requirements</li> </ul>	October 18, 2007

# Table of Contents

---

<b>1.0</b>	<b>Introduction .....</b>	<b>1</b>
1.1	Purpose .....	1
1.2	Scope .....	1
1.3	Plan Maintenance.....	1
1.4	Shared vs. Leased Credentialing Centers.....	2
<b>2.0</b>	<b>Site Facility Requirements .....</b>	<b>3</b>
2.1	Physical Site.....	3
2.1.1	Building Requirements.....	3
2.1.2	Room Requirements & Recommendations.....	3
2.1.3	Furniture Setup Requirements & Recommendations.....	4
<b>3.0</b>	<b>Power Requirements .....</b>	<b>8</b>
<b>4.0</b>	<b>Security Requirements .....</b>	<b>9</b>
<b>5.0</b>	<b>IT and Telecom Requirements .....</b>	<b>10</b>
5.1	IT Requirements.....	10
5.2	Recommended Installed Configuration .....	11
5.3	Possible Network Configuration Options .....	12
5.4	Telecom Requirements .....	12
<b>6.0</b>	<b>Roles &amp; Responsibilities .....</b>	<b>13</b>
6.1	Deployment Roles .....	13
6.1.1	MSO Deployment Manager.....	13
6.1.2	Agency Representative .....	13
6.1.3	Site Point of Contact (POC) .....	13
6.1.4	EDS Deployment Team .....	14
6.2	Operating Roles & Responsibilities .....	15
6.2.1	Credentialing Center POC .....	15
6.2.2	Registrars.....	15
6.2.3	Activators .....	15
<b>7.0</b>	<b>Site Processes.....</b>	<b>16</b>
7.1	USAccess PIV Card Receiving and Handling Process .....	16
7.2	Escort Process .....	16
<b>8.0</b>	<b>Infrastructure Reference .....</b>	<b>17</b>
8.1	System Security.....	18
8.2	Network Address Translation (NAT).....	18
8.3	Firewall .....	19

8.4	XML Gateway/Firewall.....	19
8.5	Web Application Scanning.....	19
8.6	Component Critical Files .....	19
8.7	Enrollment Station VPN.....	19
8.8	Highly Secure Device Level Authentication.....	20
8.9	Security Policy .....	20
8.10	Intrusion Prevention System (IPS).....	20
8.11	Anti-Virus.....	20
8.12	Centrally Managed Security .....	20
8.13	Endpoint Security Controller .....	21
8.14	Data Management.....	21
<b>Appendix A: Acronym List.....</b>		<b>22</b>

## List of Tables & Figures

---

Figure 2-1: Minimum Footprint of Registration Station .....	5
Figure 2-2: Alternative Footprint of Registration Station Registrar and Applicant sit side-by-side	6
Figure 2-3: Activation Station Can be used for self-service or attended Activation .....	7
Figure 8-1: USAccess Program Technical Infrastructure.....	18

## 1.0 Introduction

---

Homeland Security Presidential Directive 12 (HSPD-12), issued by President George W. Bush on August 27, 2004, established the requirement for a mandatory Government-wide standard for identifying Federal Government employees and contractors. As part of this presidential mandate, Government agencies must adopt and deploy a common identification system for both logical and physical access to Federally-controlled facilities and information systems by October 2006. The intent of the HSPD-12 mandate is to enhance security, increase efficiency and reduce identity fraud—while protecting personal privacy.

Following the HSPD-12 directive, the National Institute for Standards and Technology (NIST) developed the *Federal Information Processing Standard (FIPS) 201: Personal Identity Verification of Federal Employees and Contractors*. The FIPS 201 standard outlines the minimum requirements for issuing identity credentials and was used to establish an evaluation program to test products and services for HSPD-12 compliance.

Electronic Data Systems (EDS), in conjunction with Northrop Grumman Corporation (NG), has established a hosted, Managed Service solution offering Federal HSPD-12 services to Federal Government customers and contractors.

### 1.1 Purpose

The USAccess Program *READY!* Guide is intended to provide Agency personnel with the information they need to make decisions about where to locate their HSPD-12 Credentialing Centers that will contain Enrollment and Activation Stations.

### 1.2 Scope

All HSPD-12 Credentialing Centers must meet the requirements set forth in this document. Subjects addressed include building, room, furniture, telecom, IT and security requirements. Shared versus leased space is also addressed.

### 1.3 Plan Maintenance

This document has been reviewed against NIST Special Publications, Government security documents and other client specific security documents, and is commensurate with those requirements. This document will be periodically reviewed by responsible parties within the program and updated as necessary.

## 1.4 Shared vs. Leased Credentialing Centers

The USAccess Program offers an Agency the choice of either hosting a Credentialing Center that is shared with other participating Agencies or leasing a Credentialing Center. Shared Credentialing Centers include an Enrollment Station and a separate, standalone Activation Station that can be used for self-service (Cardholder-performed) or manned (assisted) activations. Agencies that choose to lease a Credentialing Center also receive an Enrollment Station and separate, standalone Activation Station. Additionally, Agencies may choose to purchase additional Activation Stations—either for use by sites with existing Credentialing Centers or sites with no other Program equipment.

Agencies that offer to host a shared Credentialing Center for use by all participating organizations may also request a GSA MSO-provided Registrar to operate the Enrollment Station for one year. Agencies that choose to lease a Credentialing Center also have the option to contract a Registrar (at an additional charge).

## 2.0 Site Facility Requirements

---

### 2.1 Physical Site

#### 2.1.1 Building Requirements

Potential locations for Credentialing Centers should be evaluated and selected based on the following set of specifications:

- The building is owned by the federal government or contains federally leased space.
- The building is accessible by public transportation, if available.
- The building meets federal requirements for disabled individuals under the Americans Disabilities Act requirements. This includes: parking, ramps, automatic entryway, elevators, etc.
- The building maintains at least a minimal level of physical security.

Additionally, **shared** Credentialing Centers should also:

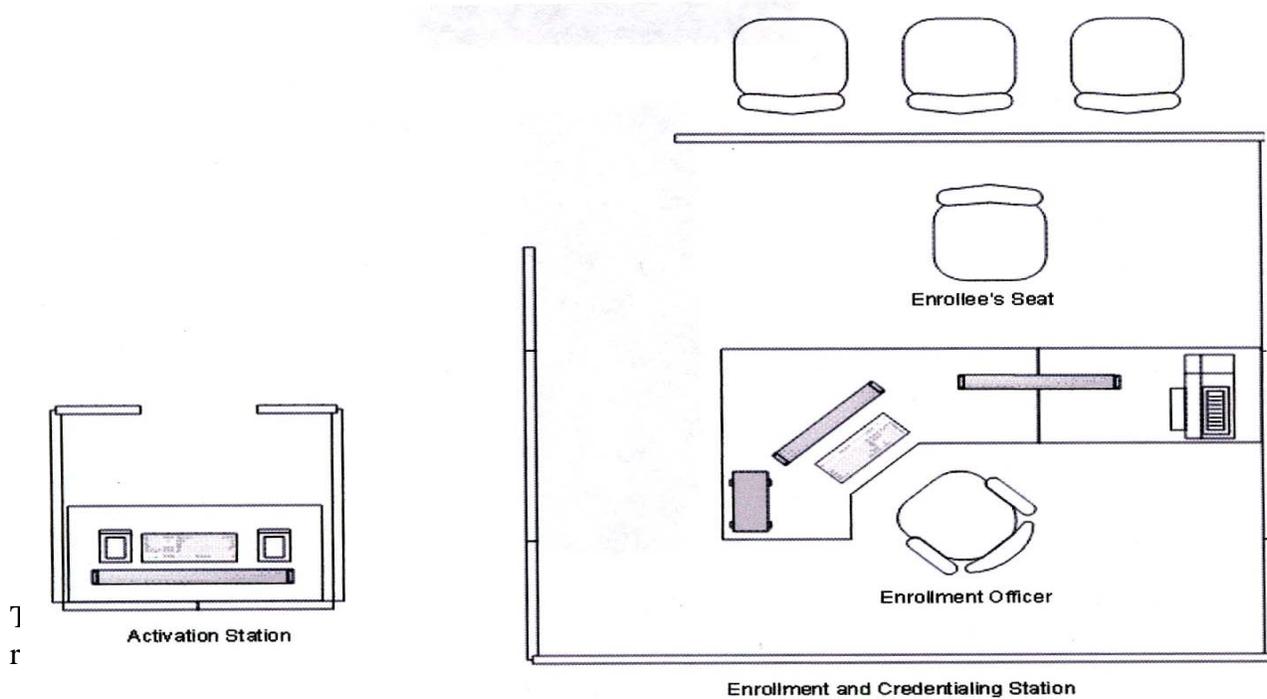
- Be centrally located among high concentrations of federal government employees and/or contractors, and
- Be able to accommodate the general public.

Once a building has been identified as a potential Credentialing Center, appropriate space inside the building should be identified. The following Room Requirements and Recommendations provide guidelines for the location within the building and build-out of a room for the Credentialing Center (if necessary).

#### 2.1.2 Room Requirements & Recommendations

An identified space within a potential Credentialing Center location should be evaluated for the following requirements before finalizing its location.

- The space is centrally located for easy access near a main entryway or elevator.
- The space has adequate, accurate and visible signage to help navigate from the main entrance(s).
- The recommended space is large enough that it can be configured to accommodate the Enrollment Station(s), furniture of Activation Station(s), privacy counters and/or barriers and a queuing/waiting area. Where possible, it is best to have the waiting area physically separated from the Enrollment workstations to allow for 1-to-1 privacy between a Registrar and an Applicant. An example of an approved setup that meets privacy requirements is shown below:



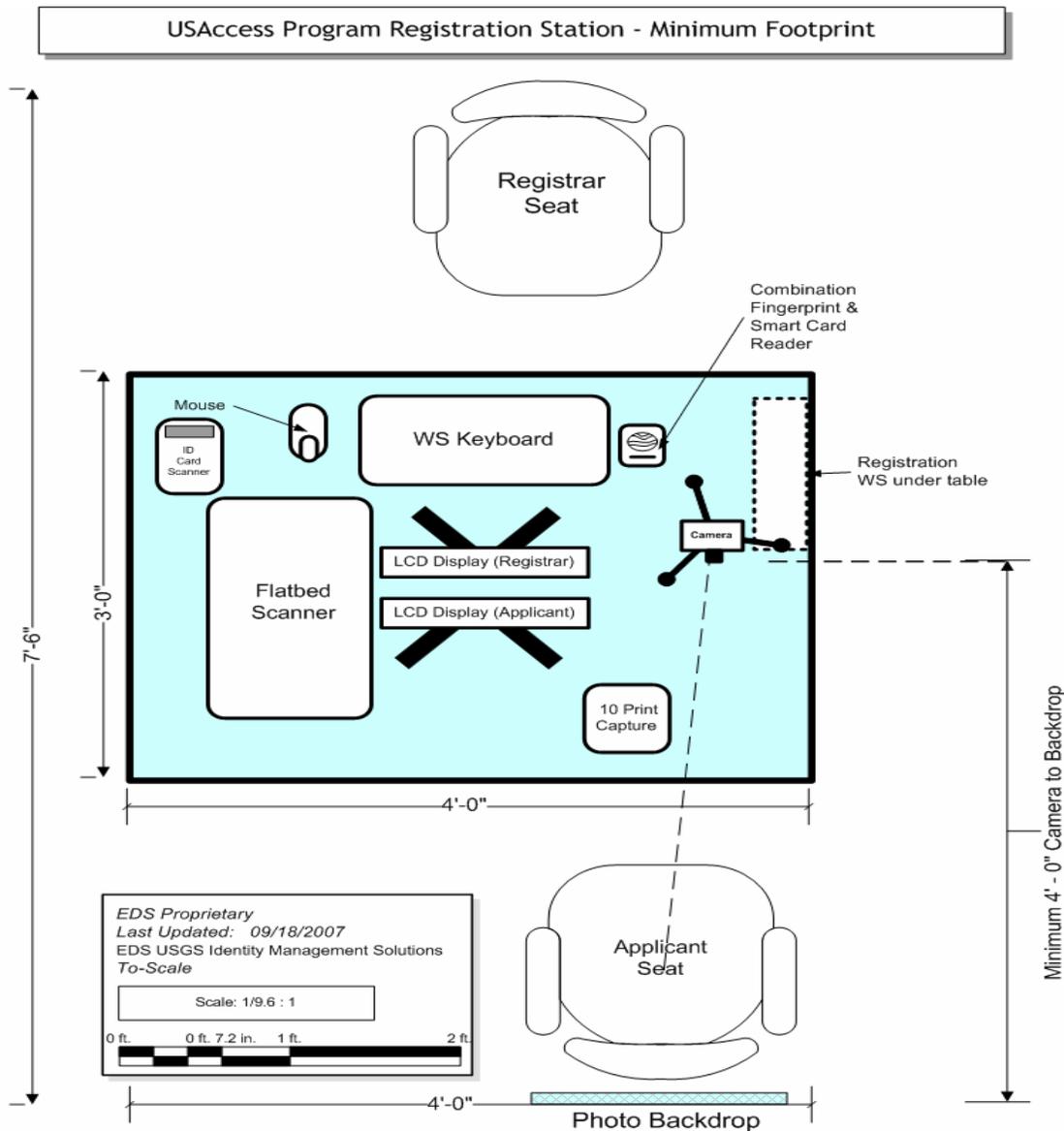
### 2.1.3 Furniture Setup Requirements & Recommendations

Ideally, each Credentialing Center should be equipped with a furniture setup that meets the following specification:

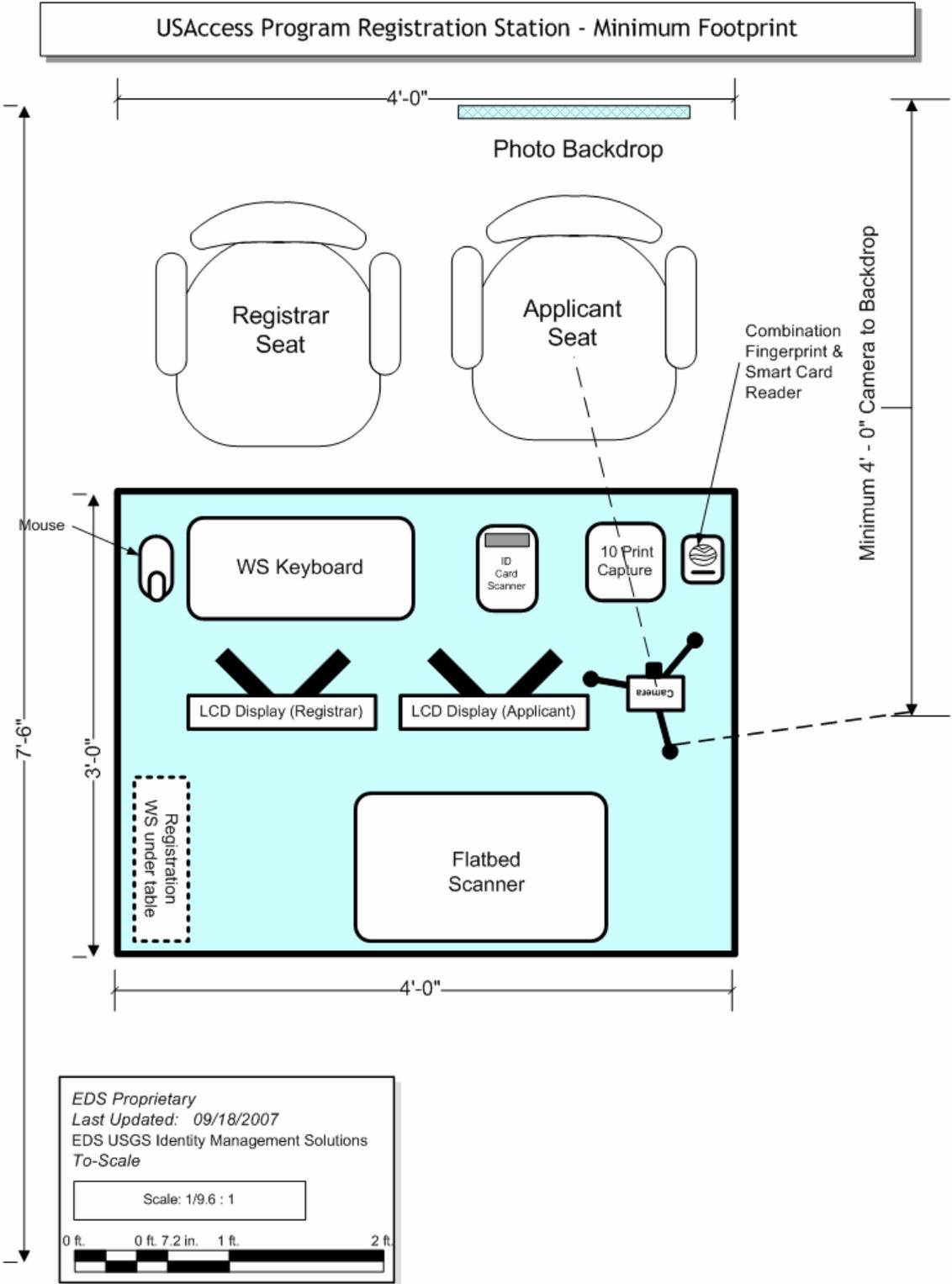
- For the Enrollment Station, a large desk/table capable of handling a PC, a monitor and several peripherals is needed. The desk/table may be modular (part of cubicle or wall structure) or standalone. The desk/table should be accessible by seated users from both ends. The Enrollment Station takes up approximately 48” x 33” of desk surface space and weighs about 50 pounds.
- The Enrollment Station requires a minimum of two chairs—one for the Registrar and one for the Applicant.
- In order to optimize photo quality, standard office lighting is required in the area of the Enrollment Station. However, overhead lighting that is too bright can adversely affect photo capture. In this case, supplemental, frontal lighting (such as a photo lamp) is recommended (but not provided by the USAccess Program).
- Additionally, a blue backdrop and stand should be provided. Allow added space behind the Applicant’s chair for a blue backdrop and stand.
- Excessive sunlight will have a negative effect on photo quality. Plan to place the Enrollment Station away from windows or shade the windows to block excessive sunlight.
- Whenever possible, a self-service Activation Station should be located near the Enrollment Station to allow Cardholders easy access to Registrars, or other trained personnel, in case of questions during self-service activation.

- Barriers should be placed in a manner that shields screens from the view of waiting Applicants or from other Credentialing Stations. This is only necessary if the room configuration does not allow for such privacy to occur naturally.
- A safe or secure cabinet must be located with each of the Credentialing Centers. The safe (or cabinet) is used to store new credentials prior to issuing them to the Cardholders and subsequent activation.

The MSO has procurement vehicles in place for purchasing the necessary furniture. For a general idea of possible station setups, see the examples below for Enrollment Stations and Activation Stations including the minimum footprint of each.

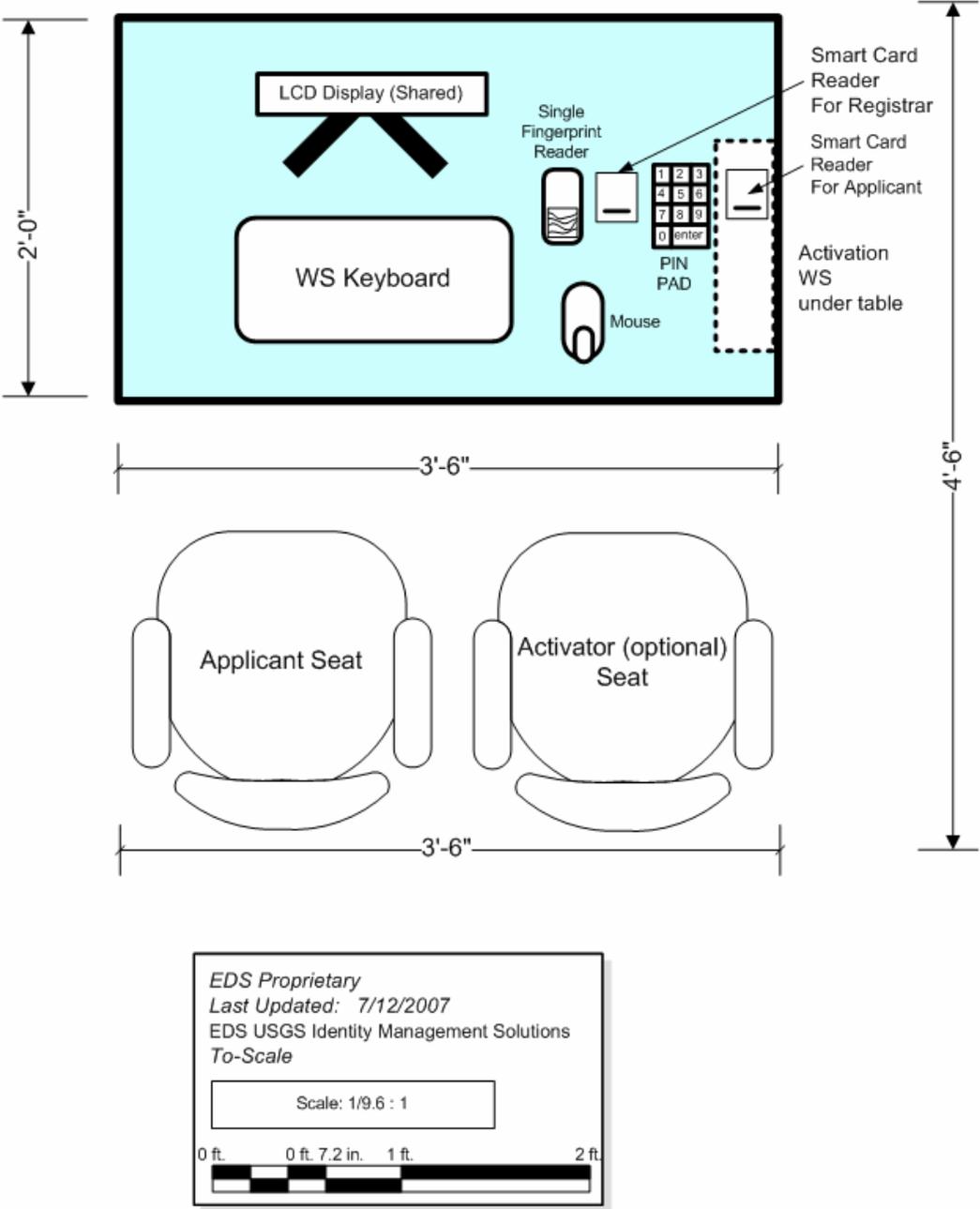


**Figure 2-1: Minimum Footprint of Registration Station**



**Figure 2-2: Alternative Footprint of Registration Station  
Registrar and Applicant sit side-by-side**

**USAccess Program Attended Activation Station  
(Allows for self-activation or manned activation)**



**Figure 2-3: Activation Station  
Can be used for self-service or attended Activation**

### 3.0 Power Requirements

---

Enrollment Stations, Activation Stations and the VPN communications equipment require standard 120 Volt AC power.

All of the equipment for a single Enrollment Station requires a minimum of 3.3 amps of power

All of the equipment for a single Activation Station requires a minimum of 2.1 amps of power.

Each VPN device requires a minimum of 1.8 amps of power.

Given that a standard 120 Volt AC 20 amp circuit should not be loaded to more than 80% (16amps) of its capacity (20 amps), it is recommended that there be at least one dedicated 20 amp 120 Volt AC circuit for each group of no more than 2 Enrollment Stations with 2 Activation Stations and 1 Site VPN. See below for an example:

Enrollment Station	3.3 amps	x 2	=	6.6 amps
Activation Station	2.1 amps	x 2	=	4.2 amps
Site VPN Concentrator	1.8 amps	x 1	=	<u>1.8 amps</u>
		Total	=	12.6 amps

This would also allow for the addition of one additional Enrollment or Activation Station later if needed.

## 4.0 Security Requirements

---

The following minimum security requirements apply to all Credentialing Centers, whether Shared or Leased:

- A safe or a secured cabinet must be utilized to secure the USAccess PIV Cards until activated.
- The Credentialing Center must be locked when not occupied.
- The space containing the Credentialing Center must safeguard against accidental disclosure of sensitive information and equipment tampering.
- USAccess Credentialing Center equipment may not be tampered with, added to, or changed in any way.
- Enrollment Stations, Activation Stations and Credentialing Center VPN routers may not be moved. Requests to move, add or change Credentialing Center equipment must be made through the USAccess Help Desk.
- Only trained Registrars should have access to the Credentialing Center equipment. This does not include the Activation Stations which may be accessed by Cardholders (for self-activation), or Activators and Cardholders (for manned activation).

## 5.0 IT and Telecom Requirements

---

### 5.1 IT Requirements

A Credentialing Center consists of at least one each of the following components:

- Cisco 3002 VPN Router or a different router with similar functionality which is FIPS 140-2 validated.
- Linksys 2008 Switch
- Enrollment Station
- Activation Station

*The Cisco 3002 VPN Router is NIST (FIPS 140-2) certified. There is a planned upgrade to a replacement VPN Router, which will be implemented upon testing and certification.*

The network requirements for standing up a USAccess Credentialing Center are as follows:

- One physical (non-wireless) Internet/LAN connection must be provided for each VPN device.
- A WAN IP address must be established for each VPN device. The IP address must be communicated to the USAccess Implementation Engineer, via the SET! Worksheet, prior to the deployment of the Credentialing Center.
- The Enrollment Stations and Activation Stations are remotely managed. Periodically, anti-virus definitions, operating system patches and EDS Assured Identity™ updates will be sent to the workstations to ensure security and performance are maintained.
- Administrative access is exclusive to the remote administrators at the USAccess Program Network Operations Center (NOC). The remote administrators will also run regular audit and production reports.
- No third-party software or hardware may be added to the Enrollment Workstations. Software is installed on all the stations that prevent the installation of any additional software or drivers.
- No data is stored on the local workstations.. If an enrollment cannot be completed for any reason, no data is stored.
- Outside of local network connectivity and performance, no support will be expected from local network administrators. All support requests will be handled by the USAccess Help Desk.
- The architecture calls for IPSEC over SSL Port 443 VPN transport only between the Credentialing Center workstations (Enrollment and Activation Stations) and the Service Infrastructure Provider (SIP). Communication is always initiated from the Enrollment and Activation Stations and must be allowed through any outbound firewalls or network

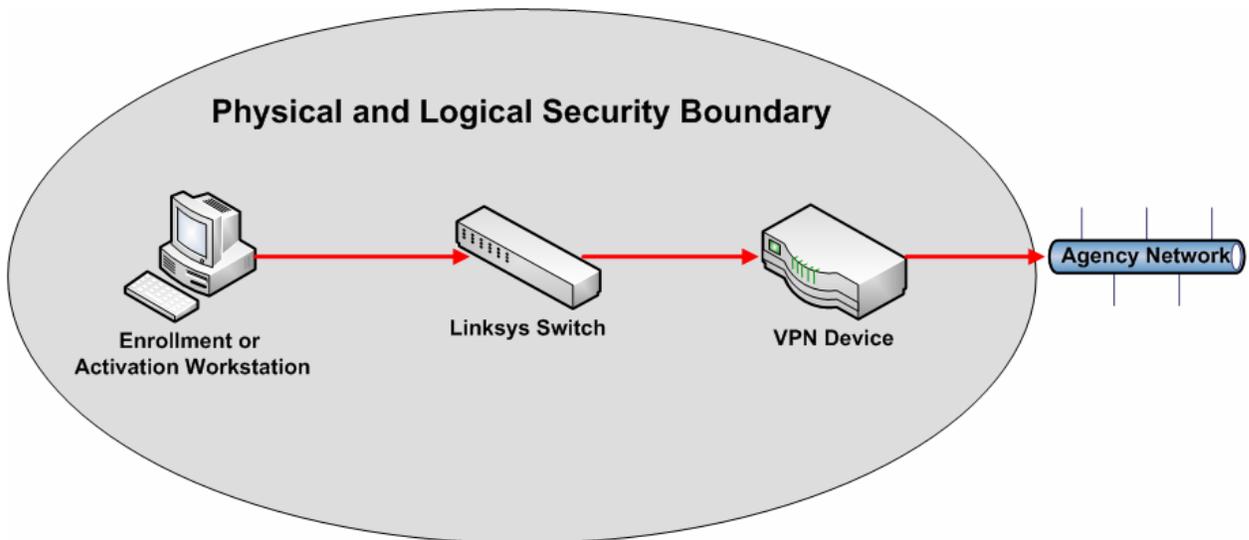
security devices from the VPN device(s). In addition, the workstations run endpoint security agents with a centrally managed, host-based firewall with tight control of both ingress (none) and egress (IDMS, realm controller, etc.). From a network perspective, the workstations are clients initiating a TCP 443 (IPSEC) connection to the outside world.

- The architecture is designed to isolate the Credentialing Center devices from all other devices on the host site’s network (if applicable). Proximity of the Credentialing Center VPN device(s) to the edge device (switch or router) may be an issue for some older networks. If you prefer to use your current address space, you must allow the VPN device to connect outside the firewall(s). If the VPN device is to reside behind a firewall, port 443 must be opened outbound.
- Optionally, a separate circuit (i.e. DSL, T-1, etc.) may be used. Recommended bandwidth for this option is 1.5mbps up and down. Although a line provisioned less than 1.5mbps will work, it may increase processing time for enrollments. The minimum bandwidth is 168Kbps per pair of workstations (1 Enrollment Station and 1 Activation Station).

Upload speed is important as the Registrars will be sending 1-3MB of data for each enrollment processed. The USAccess Program does not provide a dedicated circuit.

## 5.2 Recommended Installed Configuration

The ideal configuration, as defined by the C&A documentation, is that all deployed terminals are directly connected to the Linksys switch, and that the Linksys switch is directly connected to the VPN device. All of these components should exist within the same physical boundary (i.e. within the same room, behind locked doors). The diagram below illustrates the C&A configuration for installing Credentialing Center equipment on an existing agency’s network.



### 5.3 Possible Network Configuration Options

Configuration	Characteristics/Requirements
Installed on Agency WAN	<ul style="list-style-type: none"> <li>• Site must provide an IP address, which is configured in to the VPN device prior to deployment</li> <li>• Port 443 must be opened to outbound communications</li> <li>• If site utilizes a non-stateful firewall, ports 1024 and above must be opened to receive incoming traffic</li> <li>• Proxies and internet monitoring tools (such as Web Sense and Web Inspector) may interfere with workstation authentication and must be changed to permit traffic flow across Port 443.</li> </ul>
Dedicated circuit (DSL, SDSL, T1, etc.)	<ul style="list-style-type: none"> <li>• Site must obtain IP address from network provider and provide it to Deployment Team prior to deployment</li> <li>• Recommend symmetrical networks whenever possible to provide best performance</li> </ul>

### 5.4 Telecom Requirements

At least a single telephone line must be installed in each room. Each line must have a local contact number and voicemail setup for the Registrars. This number must be relayed back to the Implementation Engineer for reference.

## 6.0 Roles & Responsibilities

---

### 6.1 Deployment Roles

The following entities play key roles in the Deployment of Credentialing Centers to Agency Sites.

#### 6.1.1 MSO Deployment Manager

The GSA Managed Service Office is primarily responsible for the following:

- Defining the Program deployment strategy
- Guiding the participating agencies in choosing sites
- Providing policy guidance to the Agencies and to its partners
- Approving sites for deployment
- Participating in GO! Calls

#### 6.1.2 Agency Representative

An Agency Representative is responsible for:

- Participating the program Deployment Working Group meetings
- Identify sites to receive Credentialing Centers. Identify the number of Enrollment/Activation Stations to be deployed to each site and whether a particular site will be a “Shared” or “Leased” (aka, “Dedicated” Center).
- Providing complete Site POC information
- Participating in the GO! Call

#### 6.1.3 Site Point of Contact (POC)

A Site POC is responsible for:

- Reviewing the *READY!* Guide and asking questions to assure understanding.
- Providing the *READY!* Guide to anyone within their organization who might play a role in the successful deployment to their site.

- Providing accurate information, via the SET! Worksheet, to the EDS Deployment Team representative
- Providing additional points of contact information for appropriate site personnel, such as network engineers, facilities managers and security personnel
- Facilitating all site preparation activities for the site
- Engaging the other functional staff at their sites and confirming tasks are completed
- Participating in the GO! Call

### **6.1.4 EDS Deployment Team**

The EDS Deployment Team consists of the EDS Deployment Manager, several Implementation Engineers, staging warehouse technicians, and a field services personnel, and is responsible for:

- Participating in the program Deployment Working Group meetings.
- Working with the Agency Representatives and Site POCs to prepare the identified sites to receive their USAccess Credentialing Center equipment
- Creating and maintaining the various tools and documents used to facilitate the deployment process:
  - The USAccess Deployment Process
  - The Site Code Database
  - READY! Guide
  - SET! Worksheet
  - GO! Call process
  - Site Certification Sign-off sheet
- Facilitating the GO! Calls
- Delivering, installing and configuring Credentialing Center equipment to the sites.
- Certifying the site Credentialing Centers for operation.
- Providing two-days of on-site system support during the start-up phase.

## 6.2 Operating Roles & Responsibilities

### 6.2.1 Credentialing Center POC

Each site must identify a Credentialing Center POC for that site. This person is responsible for the day-to-day operations of the Credentialing Center and acts as the ongoing site POC to the USAccess Program Help Desk and the GSA MSO. The Help Desk will maintain a list of contact information for site POCs for use in notifying them of system updates and outages. Additionally, the Help Desk will notify the site POC if his/her Credentialing Center is unexplainably not open for business during normal operating hours (i.e., if an Applicant arrives for his/her appointment and the Credentialing Center is closed).

Each Credentialing Center POC should also identify a backup POC for times when he/she is not available to perform this role.

### 6.2.2 Registrars

Registrars operate the Enrollment Stations. Therefore, they must be trained and certified to perform this role. Agencies have the option of either providing their own Registrars or requesting one through the USAccess Program. Classroom and web-based training is available for Agency personnel and contractors to train them on use of the USAccess Program enrollment system and performing the Registrar role.

All Registrars, whether Agency or USAccess Program provided, must have a USAccess PIV Card to log into and operate the Enrollment Station.

### 6.2.3 Activators

Activation Stations are configured to be able to perform either self-service (Cardholder only) or manned activations (Cardholder and an Activator). Agencies should be prepared to have a trained, certified Activator(s) available to perform manned activations—as well as assist Cardholders who are having difficulties with self-service activations. Registrars may be able to perform as Activators, but due to the large number of people that must be enrolled in a short period of time, Agency Points of Contact (POC) should not depend on Registrars to handle all activations.

## 7.0 Site Processes

---

### 7.1 USAccess PIV Card Receiving and Handling Process

Even though the USAccess PIV Cards do not contain any electronically stored personal information at the time they are shipped from the manufacturer, they are still considered controlled media. As such, a “chain of trust” must be maintained from the time it is received on site until the time it is turned over to the Cardholder for activation.

Each site must define and document a process for receiving and handling the USAccess PIV Cards after they are received from the manufacturer. This process should take into consideration any site specific receiving processes.

**At no time prior to the activation of the USAccess PIV Cards should they be left unsecured or unattended.** A hand-receipt and/or logging process should be implemented to track any internal transfers of the USAccess PIV Cards (i.e., from loading dock personnel to Primary Card Receiving POC).

During the Site Preparation Process, the site POC will be asked to provide a Primary Card Receiving POC, a Secondary Card Receiving POC and their contact information. This information will be provided to the USAccess PIV Card production facility for use as the “Ship To” name and phone number for USAccess PIV Cards being shipped to the site.

### 7.2 Escort Process

Depending on site specific visitor policies, a Credentialing Center POC may also have to devise a process to provide access to non-Agency personnel using the Credentialing Center to register or activate their USAccess PIV Cards. For instance, the POC may choose to print out a list of all Applicants with appointments for that day and provide the list to the front desk to allow scheduled Applicants access to the Credentialing Center.

## 8.0 Infrastructure Reference

---

The backend of the USAccess Program infrastructure is designed into zones and layers. This approach—in coordination with firewalls—limits interaction between system components to required interactions.

All accounts on any backend systems are provisioned only with necessary privileges. All accounts and associated privileges follow security standard operation procedures and are required to be audited periodically. All systems employ IPS, IDS, anti-virus and firewalls to assist in ensuring they remain secured at all times. Additionally, system components utilize Odyssey software to implement further security of the components.

FIPS 140-2 level 1, 2 and 3 certified cryptographic modules are used to store all cryptographic keys. All cryptographic operations are executed using FIPS compliant algorithms and key sizes. The system uses an nCipher nShield for NetHSM, which is FIPS 140-2 level 3 compliant.

Figure 8-1 illustrates a high-level component overview of the USAccess Program infrastructure.

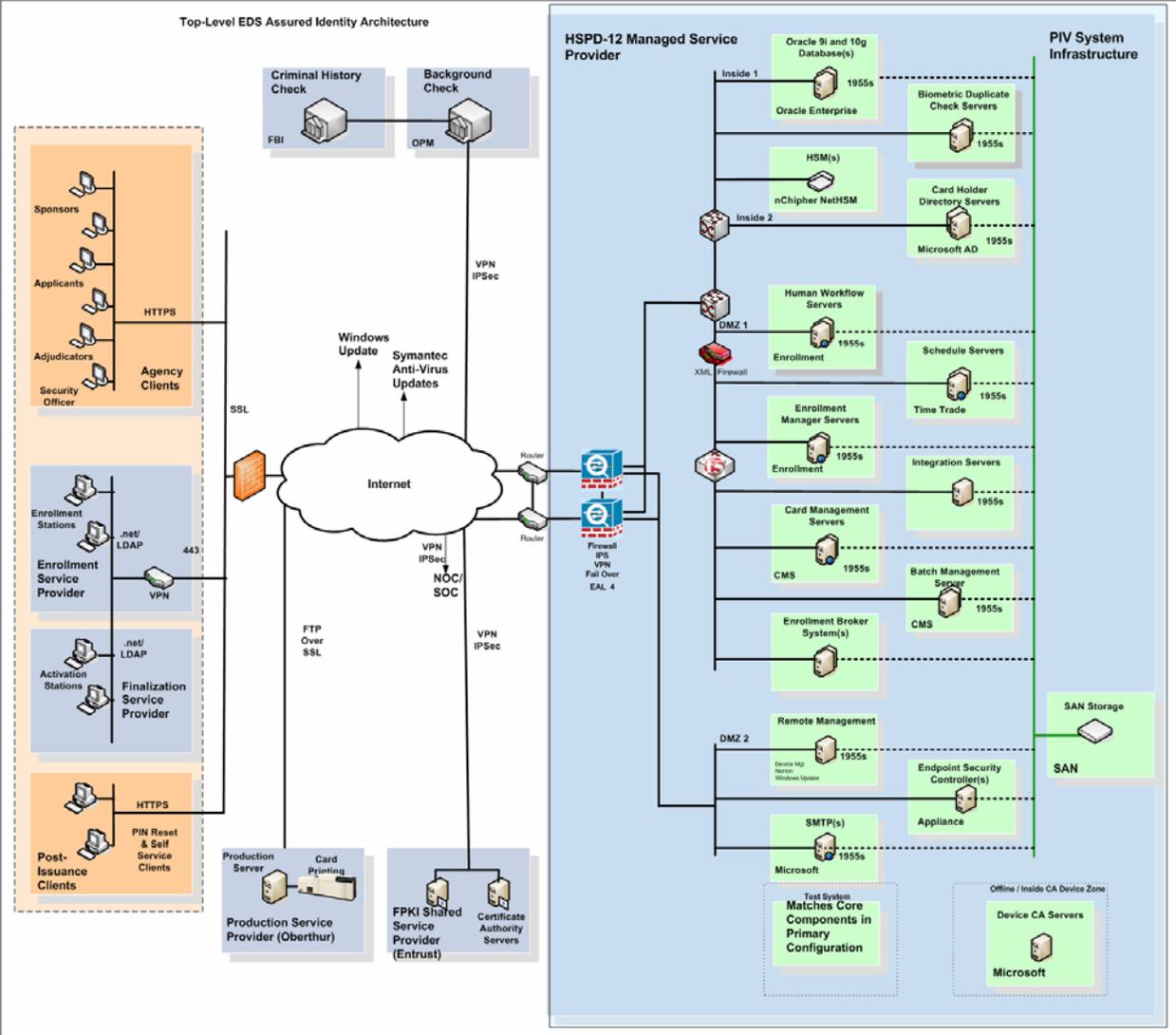


Figure 8-1: USAccess Program Technical Infrastructure

### 8.1 System Security

The Enrollment Stations and Activation Stations are configured to establish a tunnel using 256-bit symmetric keys and the AES encryption algorithm.

### 8.2 Network Address Translation (NAT)

The Enrollment Stations and Activation Stations do not use Network Address Translation. The Credentialing Center operates in its own, segregated VPN zone. The VPN provides DHCP services that issue IP addresses that are viable network destinations accessible from the system DMZ or “inside” network zones.

## 8.3 Firewall

The backend system utilizes a Cisco ASA5540 Firewall, which is certified at EAL 4. Firewalls are configured to only allow specific traffic between identified network nodes that are required to communicate—and deny all other attempts from unspecified network nodes to communicate with other network nodes that are not approved. Further, the nodes are limited to communicating on ports with protocols that are implicitly specified. All other ports and protocols will be denied.

## 8.4 XML Gateway/Firewall

All web services transactions are filtered through the XML gateway. The XML gateway is configured to analyze the XML packages for malicious code and web service attacks (SOAP and attack vectors). Only values within the XML package that are deemed appropriate and benign are allowed for further processing. Additionally, the software generating the XML packages filters fields for acceptable values prior to processing the package.

## 8.5 Web Application Scanning

Web applications and services are scanned on a monthly basis. The Managed Service Provider networking team will utilize scanning tools such as nmap and similar detection tools. Once made aware of a vulnerability, efforts to mitigate the vulnerability are initiated through Change Management and the system is updated accordingly.

## 8.6 Component Critical Files

Each system component operates the Odyssey Software. This product monitors the component's resources and sensitive files. In the event that a critical file or security breach occurs (or a file is illegitimately modified), a security alert will be sent out notifying administrators—in addition to locking down the component and preventing further system tampering.

## 8.7 Enrollment Station VPN

Enrollment Stations and Activation Stations are attached to a Cisco 3002 Firewall/VPN Client or a different router with similar functionality via a Linksys 2008 switch. This client communicates over SSL port 443 and is configured to establish a tunnel using 256-bit symmetric keys and the AES encryption algorithm. The Cisco 3002 connects to a backend VPN concentrator. The workstations are assigned intra-system routable IP addresses for centralized management (patch and configuration updates) as well as to communicate with the endpoint security controller.

## 8.8 Highly Secure Device Level Authentication

Each system component will have a Juniper endpoint security agent running on it. These agents interact with a centrally managed endpoint security Juniper Infranet Controller device that authenticates and authorizes specific actions within the system. The authentication will be X.509 certificate based and the certificates will be issued from a system trusted Certificate Authority. The authentication methodology is 802.1x compatible.

## 8.9 Security Policy

All security elements combined in coordination with the overall security policy will prevent system components from:

- Accessing the internet (unrestricted),
- Loading unapproved software and
- Using the enrollment component for other than its intended purpose.

Personnel security training includes the acknowledgement and acceptance of their trusted role and undesired actions such as these are expressly disallowed (subsequently logged and audited periodically). Further, system components are technologically prevented from performing such actions.

## 8.10 Intrusion Prevention System (IPS)

All system components are locked down by the Juniper Odyssey clients. This product provides host-based checking in real-time whenever the host connects to the network. It also prevents well-known intrusion methods employed by would-be hackers to exploit the vulnerabilities of the system in order to gain access to it.

## 8.11 Anti-Virus

All system components run the Symantec anti-virus agents. These agents are centrally managed by a server configured to manage the agents. The server checks the subscription service for updates to virus definitions. Once definitions are updated, the server automatically deploys the updates to all the agents associated with the server.

## 8.12 Centrally Managed Security

All security policies, patches, updates, DAT files and configurations are pushed to components and are administered through a secure central service.

## 8.13 Endpoint Security Controller

The system uses a Juniper Infranet Controller (a hardened, purpose-built network appliance) to manage all system components outfitted with endpoint security agents. The Juniper implements 802.1x security methodology (device authentication) in addition to managing privilege and access of device components on the network. The Juniper Infranet Controller can manage up to 3,000 security agent connections.

## 8.14 Data Management

Data is never stored on the USAccess Workstations. No partial enrollments are permitted—if an enrollment cannot be completed for any reason, no data will be saved to the IDMS.

## Appendix A: Acronym List

Acronym	Description
AC	Alternating Current
ACL	Access Control List
AES	Advanced Encryption Standard
DAT File	Data File
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
EAL	Evaluation Assurance Level
EDS	Electronic Data Systems Corporation
FIPS	Federal Information Processing Standard
FOIA	Freedom of Information Act
GSA	General Services Administration
HSPD-12	Homeland Security Presidential Directive 12
IDMS	Identity Management System
IDS	Intrusion Detection System
IP	Internet Protocol
IPS	Intrusion Prevention System
IPSEC	IP Security
ISSO	Information System Security Officer
IT	Information
MSO	Managed Services Office
MSS	Managed Support System
NAT	Network Address Translation
NG	Northrop Grumman Corporation
NIST	National Institute for Standards and Technology
NOC	Network Operations Center
NSA	National Security Agency
PC	Personal Computer
PIV	Personal Identity Verification
POC	Point of Contact
SIP	Service Infrastructure Provider
SOAP	Simple Object Access Protocol

Acronym	Description
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
VPN	Virtual Private Network
WS	Work Station
XML	Extensible Markup Language