U.S. Department of Homeland Security

DHS ICE Office of the Chief Information Officer (OCIO)

287(g)

INTERCONNECTION SECURITY AGREEMENT BETWEEN U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT AND WASHINGTON COUNTY SHERIFF'S OFFICE FAYETTEVILLE, ARKANSAS

INFORMATION ASSURANCE DIVISION

FINAL

ICE IAD 2007-058

December 13, 2007

~~**FOR OFFICAL USE ONLY**~~

CONTENTS

EXHIBITS

1.0 INTRODUCTION

1.1 Purpose

This Interconnection Security Agreement (ISA) is required by Federal and Department of Homeland Security (DHS) policy and establishes individual and organizational security responsibilities for protection and handling of DHS Sensitive-but-Unclassified (SBU)/ For Official Use Only (FOUO) information. All specific requirements by both signatory organizations are also included in this ISA.

1.2 References

The authority for interconnectivity between information systems is based on the following federal guidance: Homeland Security Presidential Decision Directive 7; applicable National Institute of Standards and Technology (NIST) guidance (i.e., NIST Special Publication 800-47, *Security Guide for Interconnection Information Technology Systems*); Office of Management and

1.0 INTRODUCTION

1.1 Purpose

This Interconnection Security Agreement (ISA) is required by Federal and Department of Homeland Security (DHS) policy and establishes individual and organizational security responsibilities for protection and handling of DHS Sensitive-but-Unclassified (SBU)/ For Official Use Only (FOUO) information. All specific requirements by both signatory organizations are also included in this ISA.

1.2 References

The authority for interconnectivity between information systems is based on the following federal guidance: Homeland Security Presidential Decision Directive 7; applicable National Institute of Standards and Technology (NIST) guidance (i.e., NIST Special Publication 800-47, *Security Guide for Interconnection Information Technology Systems*); Office of Management and Budget Circular A-130, *Management of Federal Information Systems*, Appendix III, *Security of Federal Automated Information Resources*; applicable Immigration and Customs Enforcement (ICE) Information Assurance Division (IAD) guidance documents: DHS Information Technology (IT) Security Publication 4300A, *DHS Sensitive Systems Policy Publication*, DHS Management Directive 11042, *Safeguarding SBU/FOUO Information*; and other applicable DHS direction.

1.3 Scope

A T1 circuit will be used to access DHS and the Federal Bureau of Investigations (FBI) systems (Enforcement Case Tracking System (ENFORCE)/Automated Biometric Identification System (IDENT), and Integrated Automated Fingerprint Identification System (IAFIS), and HTTP/HTTPS/Exchange (DHS Intranet Web Portals), Central Index System (CIS), Computer Linked Applicatioin Information Management System (CLAIMS), Deportable Alient Control System (DACS), National File Tracking System (NFTS), and National Security Entry/Exit Registration System (NSEERS) to support the delegation of authority **to the Washington County Sheriff Office (WCSO)**. **Two data terminals** will be connected to this circuit. This is a new installation, and no previous data access has been at this site. **This is not an ICE controlled facility, but rather a county jail facility in Fayetteville, Arkansas**. This delegation of authority project has been approved by Assistant Secretary Clark on or around December 11, 2005.

1.4 Points of Contact

The established points of contact (POC) for all issues associated with this agreement are available in Exhibit 1:

Exhibit 1: Points of Contact

ICE Technical Point of Contact (TPOC)	**Name:** (b)(6), (b)(7)c **Phone: (202) 380** (b)(6), (b)(7)c **Fax: (504) 589**(b)(6), (b)(7)c **E-mail:** (b)(6), (b)(7)c
287(g) TPOC	**Name:** (b)(6), (b)(7)c **Phone: (479) 444-** (b)(6), (b)(7)c **Fax: (479) 444-**(b)(6), (b)(7)c **E-mail:** (b)(6), (b)(7)c
DHS ICE Office of Investigation Special Agent in Charge sponsor	(b)(6), (b)(7)c Office of Investigations ISSO Program Manager Executive Information Unit/ Modernization Office DHS ICE Office of Investigations 703-293- (b)(6), (b)(7)c (office) 202-498(b)(6), (b)(7)obile) (b)(6), (b)(7)c

2.0 INTERCONNECTION STATEMENT OF AGREEMENT

The intent of this ISA is to provide DHS ICE agents, contractors, and **WCSO** with exclusive ICE access to those systems listed in Exhibit 2. This ISA encompasses the connection of the DHS wide area network via a T1 to the Joint Enforcement Operations **Facility located at the WCSO 1155 Clydesdale Drive, Fayetteville, Arkansas 72701**. Personnel will utilize these systems to process aliens and conduct investigations.

The access to DHS and FBI systems (refer to Exhibit 2) from **WCSO** will be a network connection between the DHS Wide Area Network (WAN) and the ICE DHS local area network (LAN), which consists of T1 network connection via DHS ICE.

ICE-provided equipment is owned by DHS and **WCSO** has the responsibility to secure the location of the equipment. Both organizations are authorized to perform on-site verification to the extent necessary to confirm compliance with this agreement.

2.1 WCSO LAN Staff Responsibilities

The **WCSO** LAN staff responsibilities include:

- Limiting workstation logon access only to cleared and authorized users of specific DHS and FBI.

2.2 ICE Office of the Chief Information Infrastructure Engineering Staff Responsibilities

ICE Infrastructure Engineering Staff responsibilities include:

- Setting up User accounts to support 287(g) activities
- Providing a user group Internet Protocol (IP) list (and updates) to the DHS ICE Infrastructure Engineering Firewall Staff
- Enabling stringent Identification and Authorization enforcement, using DHS Password/system inactivity standards (e.g., Windows password protected screen saver) as described in Section 3.7
- Establishing of end-to-end session and login encryption between each workstation and the DHS firewall.
- Utilizing the ICE image which includes hardened operating system, rigorous patch/Service Patch, and anti-virus management

The approval of this ISA does not include the ability for outside agency to establish user accounts. DHS ICE security policies and procedures must be followed for clearances and written authorization by DHS.

System administration and maintenance of ICE-owned networking devices and workstations are the sole responsibility of the ICE OCIO staff, including the Firewall Staff, Enterprise Operations Center (EOC) (routers and switches), and others as necessary and appropriate.

Auditing of user connectivity through the firewall and Internet browsing via the DHS portal will be performed in accordance with DHS policies and procedures.

Exhibit 2: Systems/Applications to Access

Acronym	System
IDENT	Automated Biometric Identification System
ENFORCE	Enforcement Case Tracking System
IAFIS	Integrated Automated Fingerprint Identification System
HTTP/HTTPS/Exchange	DHS Intranet Web Portals
CIS	Central Index System
CLAIMS	Computer Linked Application Information Management System

Acronym	System
DACS	Deportable Alien Control System
NFTS	National File Tracking System
NSEERS	National Security Entry/Exit Registration System

3.0 SYSTEM SECURITY CONSIDERATIONS

3.1 Formal Security Policy

All other government agencies (OGA), contractors, and DHS must comply with existing Federal security and privacy laws and regulations in order to protect Federal systems and data. Additionally, ICE in the protection of DHS systems and data, will utilize DHS and ICE IAD documents, listed in section 1.2. OGAs and contractors shall comply with their own internal agency security policies as well as the higher-level requirements applicable to their operations. Additionally, OGAs and contractors agree to requirements set forth by ICE. Circuits associated with this ISA are required by DHS 4300A to enforce and maintain FIPS 140-2 level encryption.

3.2 General Information/Data Description

The biometric data of IAFIS will transport through the Criminal Justice Information System (CJIS) Gateway/CJIS WAN. This data will include fingerprint image data. The interconnection will utilize FIPS 140-2 compliant encryption technologies provided through Transport Level Security (TLS) 1.0. Biographic, biometric (in the form of ten fingerprints), and search result data will be transmitted to IDENT. Illegal or criminal aliens encountered by OGAs will be checked against DHS records and processed for removal from the U.S. or prosecuted in U.S. District Court, as appropriate.

3.3 Services Offered

The client workstation will utilize Transmission Control Protocol (TCP)/Internet Protocol (IP) for accessing systems. The systems are identified in Exhibit 2.

Technical detail is provided in the high-level illustration in Exhibit 3 and the business case requirements table maintained by the IAD staff.

3.4 Data Sensitivity

The data passed to the 287(g) agents, via the DHS WAN connection, will be considered SBU/FOUO sensitivity level 2.

3.5 User Community

The user community will be restricted to staff having an appropriate background investigation, and authorized by the ICE POC, based on DHS 4300A. By DHS Sensitive Systems Policy, non-DHS staff is permitted "read/write" access to DHS and FBI systems. DHS 4300A security policy 4.1.1e states that, "Only U.S. citizens shall be granted access to DHS systems processing sensitive information. An exception to the U.S. citizenship requirement may be granted by the

Component Head or designee with the concurrence of the Office of Security and the DHS CIO or their designees."

3.6 Information Exchange Security

The information accessed by the 287(g) site shall be considered sensitivity level is 2. The information must be protected in accordance with DHS 4300A Sensitive Systems Policy and marked, stored, and disposed of in accordance with DHS MD 11042.1.

3.7 DHS Rules of Behavior

Each connected workstation will use and maintain the latest ICE-approved hard disk image/ configuration in compliance with DHS ICE 4300A Sensitive System Policy Rules of Behavior.

Each agency shall protect the information shared under this agreement. Each agency shall implement the following security controls:

a) **Anti-Virus**—Workstations will include the ICE-approved anti-virus software with current definitions.

b) **Clearance** DHS will restrict system access to authorized DHS ICE Special Agents or employees and 287(g) personnel who must be U.S. citizens with favorable background investigations who require this information in the course of official DHS ICE duties.

c) **Data Storage**– 287(g) personnel are not permitted to replicate or store any system information in a separate database or in any other electronic format, unless approved by the system owner.

d) **Disabled Sessions**– –Workstations shall be configured to automatically disable inactive sessions after no more than 20 minutes of inactivity. Authentication must be required to re-establish the session, either through unlocking a screensaver or logging onto the workstation.

e) **Passwords** All 287(g) personnel are to go to the 287(g) Project Management Officer at your site. The Officer will set up the process for 287(g) training including acquiring User IDs and passwords. For subsequent password changes during the course of the year, 287(g) personnel should go to the local Password and Issuance and Control System (PICS) officer at the Special Agent in Charge (SAC) office or at the Detention and Removal Office's Field Office Director (FOD). The 287(g) TPOC must also submit password changes to the ICE Help Desk at 1-888-347-7762 or via the Internet at http;//remedyweb.ice.dhs.gov/help. 287(g) users must utilize the following policy for passwords. Passwords must:

- Be at least eight characters in length
- Contain a combination of alphabetic, numeric, special characters and not contain any dictionary word, e.i. (!@#S%)
- Contain no more than two identical consecutive characters in any position from previous password
- Not be the same as the previous eight passwords
- Contain a combination of upper and lower case alphabetic letters

- Not be shared among users under any circumstances (including DHS ICE, WCSO and non-ICE personnel)

All 287(g) personnel accessing data must complete a DHS/ICE 287(g) Access Request Form covering each system. The 287(g) users then must submit the 287(g) Access Request Form to the local PICS Officer at the SAC or FOD. If possible, please hand deliver the completed 287(g) Access Request Form to the local PICS Officer. If it must be sent via e-mail, please note the following: Due to the inclusion of Social Security Number information on the 287(g) Access Request Form, this form must be compressed and encrypted using WinZip or equivalent software and then emailed. The password for this form must be delivered in a separate email. Coordination of fax transfer should be made prior to that transfer.

f) **Printing** Any output of 287(g) information to media other than the screen is prohibited.

g) **Privacy**—In accordance with Federal Information Processing Standards, 287(g) may not disclose information obtained from the system to a third party, without written permission from ICE. Personally Identifiable Information (PII) must be controlled and safeguarded according to federal guidelines. This data is to only be used for those having an authorized purpose only and must be destroyed after 90 days.

h) **System Modifications**—System access from the facility is read/write unless approved in writing by the Information System Security Officer.

3.8 Incident Reporting

Any information regarding security incidents as defined by DHS and ICE security policies in references listed in Section 1.2 will be reported to the ICE Help Desk at (888) 347-7762.

3.9 Audit Trail Responsibilities

Auditing of the systems' transactions will be the responsibility of DHS/FBI system owners.

3.10 Security Parameters

DHS ICE has the responsibility to protect against possible intrusions to the ICE connections to the DHS WAN. 287(g) personnel will allow ICE to perform vulnerability assessments on this connection in order to verify established/continued access security as set forth by this ISA.

3.11 Training and Awareness

The DHS ICE Office of Investigation Special Agent in Charge sponsor shall ensure that DHS and 287(g) personnel, with access to DHS ICE systems, have documented participation in mandatory ICE Computer Security Awareness Training. These sessions shall be taken initially and annually.

3.12 Specific Equipment Restrictions

Government Furnished Equipment that are on the 287(g) Network shall be configured and maintained to current ICE Image Lab standards. Special purpose circuits, routers, servers, and workstations will be configured and maintained in compliance with current, mandatory security polices.

All equipment with access to host 287(g) sites must be located in a secured area not accessible to the public and must be restricted to cleared and authorized staff.

3.13 Dial-Up Connectivity

N/a.

3.14 Security Documentation

ICE System Security Plans and other Certification and Accreditation documentation will be updated and provided to the ICE IAD as appropriate for systems accessed. 287(g) managerial and technical security policies and procedures may be requested and reviewed by the DHS ICE IAD on a periodic basis.

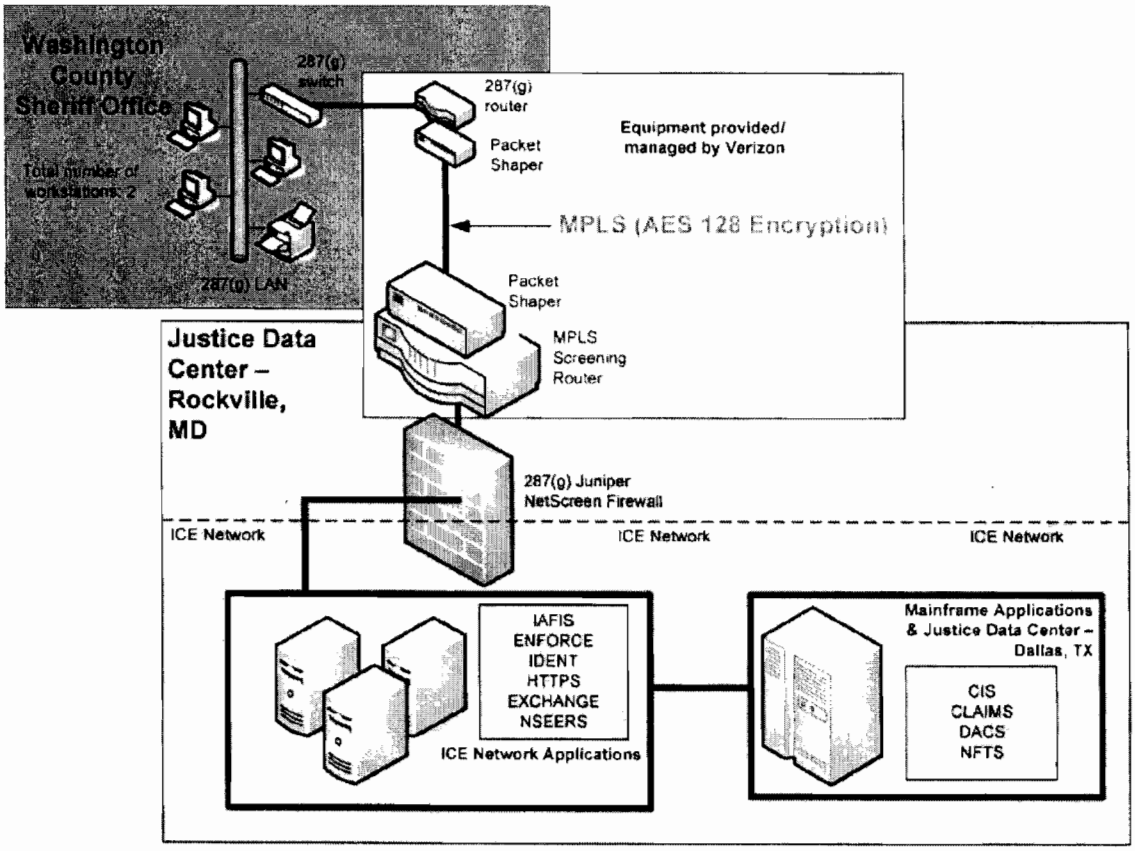
3.15 Site or System Certification and Accreditation

This new connectivity between ICE and the non DHS facility will be included in the System Interconnection/Information Sharing section of the DHS WAN System Security Plan during periodic updates.

4.0 TOPOLOGICAL DRAWING

The network connectivity between the ICE and the **WCSO** is shown in Exhibit 3.

Exhibit 3: ICE-to-WCSO Connectivity



5.0 SIGNATORY AUTHORITY

Access from the ICE facility to required systems cannot occur until both signature authorities sign the ISA.

The ISA is valid for 3 years after the last date of latest signature below. This is considered a living document, to be reviewed annually and modified as circumstances warrant. This agreement may not be unilaterally modified and all changes to the ISA must be reviewed and may necessitate a new ISA or an ISA Addendum.

Luke McCormack ICE Chief Information Officer Designated Accrediting Authority	**Chief Deputy** (b)(6), (b)(7)c Designated Accrediting Authority
	(b)(6), (b)(7)c 11-28-2007
(Signature and Date)	**(Signature and Date)**

Orig: (b)(6), (b)(7)c

cc:
ICE IAD
WCSO DAA
WCSO POC
ICE ISSO
ENFORCE POC
IDENT POC
IAFIS, NCIC, NIIS POC
ICE OCIO
ICE IAD
ICE Infrastructure Engineering
ICE Architecture
ICE SOC Manager

Office of Investigations

U.S. Department of Homeland Security
One Tower Lane, Suite 1600
Oakbrook Terrace, Illinois 60181

U.S. Immigration and Customs Enforcement

December 14, 2007

MEMORANDUM FOR: Marcy M. Forman
Director
Office of Investiga (b)(6), (b)(7)c

FROM: (b)(6), (b)(7)c
Special Agent in C
Chicago, Illinois

SUBJECT: Waukegan, Illinois Police Request for 287(g) Delegation of Authority Training

U.S. Immigration and Customs Enforcement (ICE) Headquarters received a request for 287(g) Delegation of Authority training from (b)(6), (b)(7)c for the Waukegan, Illinois Police Department, requesting 287(g) Delegation of Authority training for a minimum of two Waukegan Police Officers. In his letter, (b)(6), (b)(7)c expressed his desire to move forward with ICE in an effort to identify criminal aliens who pose a risk to the citizens of his community. ICE HQ requested that SAC Chicago initiate a field survey of the Waukegan Police Department for consideration of acceptance into the 287(g) program.

SAC Chicago is currently available to support the Waukegan Police upon their receipt of training. (b)(6), (b)(7)c has requested 15 officers be trained in the program, but would be willing to fill up to 30 slots in a training class if it is held locally. Although two other departments in the Chicago metropolitan area are awaiting consideration for participation in the program, no other law enforcement agencies in the AOR are approved participants in the 287(g) program. Therefore, it is believe that SAC Chicago would be able to handle the increased workload should Waukegan be approved. However, if additional departments in the Chicago metropolitan area are approved for the 287(g) program, resource issues may have to be re-addressed to deal with the increased responsibilities.

The Field Office Director has confirmed that the Waukegan Police Department is not a contract facility; however, DRO anticipates being able to handle the expected increase in aliens each month that Waukegan believes will be processed through the 287(g) program.

Should the Assistant Secretary choose to approve or disapprove the request, the 287(g) Program Manager will draft a letter to the requesting agency with her response.

Approved: _____ Disapproved: _____

Needs more discussion: _____

Office of Investigations
U.S. Department of Homeland Securit
425 I Street, NW
Washington, DC 20536

U.S. Immigration and Customs Enforcement

(b)(6), (b)(7)c

420 Robert V. Sabonjian Place
Waukegan, Illinois 6085

Dear (b)(6), (b)(7)c

Thank you for your interest in the 287(g) delegation of immigration authority program. The 287(g) Program Management Office and the Office of the Assistant Secretary for U. S. Immigration and Customs Enforcement (ICE) are in receipt of your request for training for the Waukegan Police Department.

On August 2, 2007, the Program Manager for 287(g) Delegation of Authority at ICE Headquarters forwarded your request to the Special Agent in Charge (SAC) Chicago, IL, and the Field Officer Director (FOD) of Detention and Removal, Chicago. Local representatives from these two divisions will be in contact with you soon to conduct a preliminary assessment and determine whether the 287(g) program is the appropriate application to address your local law enforcement challenges.

The local ICE point of contact regarding the 287(g) program is (b)(6), (b)(7)c (b)(6) who can be reached at 630-574-(b)(2)Low

Sincerely,

Roland Jones
Acting State and Local Coordinator
Investigative Services Division

U.S. Immigration and Customs Enforcement

287(g) Program

Office of the Chief Information Officer

IT Site Survey Report

Washington County Sheriff's Office, AR

FINAL

Version 1.0

Site Survey/Checklist

Site Name: Washington County Sheriff's Office

Survey Date: 04-17-07

Assessment Conducted by: (b)(6), (b)(7)c

Riggs

The main purpose of the document is to assist the survey team with assessing both the IT and Facility infrastructures. Within this document is a checklist of areas that need to be assessed including facility areas such as Physical access, HVAC, Electrical. IT areas will consist of cable plant, LAN and WAN components.

Site Information
Washington County Sheriff's Office
1155 Clydesdale Drive
Fayetteville, AR 72701

- Site POC: Major (b)(6), (b)(7)c Commander. (479)444 (b)(6), (b)(7)c
- Site POC: (b)(6), (b)(7)c Sheriff's Deputy IT POC (479)444- (b)(6), (b)(7)c
- Site POC: (b)(6), (b)(7)c , Chief Deputy (479)444(b)(6), (b)(7)c

Official Site Code:
Unofficial Site Code: __

ICE Team

Jesus M. Garcia	ITFO – 287G (956) 346	(b)(2)Low
Jamie Wright	ICE 287G (202)305-	
Dale Riggs	Contractor (202) 246	

ISSUES

The site is the Washington County Sheriffs Office and Detention Facility. It is located at 1155 Clydesdale Drive, Fayetteville, Arkansas. This facility is fairly new and up to date with IT Technology. After touring the facility and looking at the number of detainees processed by the facility it was recommended that Washington County will be well served if they were to obtain two full IAFIS workstations :

1. Interview Room in Processing/Holding Area, two (IAFIS)

The Interview Room designated to support two IAFIS workstation has no CAT 5 drops currently in place. The current plan is for the site to install all new CAT 5 cabling to connect the IAFIS workstations to the ICE Network via T1 connection. OCIO will add one twenty-four port switch to accommodate the two IAFIS Processing Workstations and provide flexibility for future expansion of the site.

Equipment and Storage:

Is there a loading dock to load /unload equipment	YES ☐	NO ☒
If no, how the equipment can be delivered to the site? Equipment will be delivered to the intake area door		
Are there freight elevators at the site?	YES ☐	NO ☒
If no, how will the equipment be distributed?		
Is there a pallet jack or another means for moving pallets?	YES ☐	NO ☒
If no, what are the alternatives for moving pallets & boxes Hand delivery		
Is there are storage area available for boxes and pallets.	YES ☒	NO ☐
If not is there an alternate off site storage location available? Equipment can be stored in the interview rooms.		
Is the physical security adequate for storage of (e.g., controlled building access, limited access to computer room, secure cabinets)?	YES ☒	NO ☐
Are clearances required to gain access to the building	YES ☒	NO ☐
What kind of badge is needed for access? By appointment		
Are the computer rooms locked or access controlled?	YES ☒	NO ☐

Heating, Ventilation & Air Conditioning:

Will the HVAC for the building shut down at a specified time?	YES ☐	NO ☒
If yes, raise issue to local POC and OCIO management.		
Does the computer room have its own HVAC?	YES ☐	NO ☒

Electrical Power

Site Name	**Server Room**	**Is there dedicated power?**	**If yes, how much dedicated power overall for server rooms?** (amps/watts)	**Is there room for expansion** (i.e., addition of circuits)?	**# of circuits NOT in use today**	**Is there dedicated UPS?**

1. Washington County	A. Yes	YES ☒ NO ☐		YES ☒ NO ☐	na	YES ☒ NO ☐	
	B.	YES ☐ NO ☐		YES ☐ NO ☐		YES ☐ NO ☐	
	C.	YES ☐ NO ☐		YES ☐ NO ☐		YES ☐ NO ☐	

Electrical Outlets Required			
Site Name	**Room/** Location in Building (e.g., floor)	**Total # of Outlets Required**	N/A
1. Washington County	A. Interview Room	4	
	B.	0	

Computer Room

The computer room is located in located near the Investigations Office. It is secure, clean, and climate controlled. The walls are reinforced concrete and room complies with the local fire codes.

There *are no* extenuating circumstances involving the site's electrical power capabilities.

Cable Plant Assessment

Please provide the following:

Is there an existing cable plant?	YES ☒	NO ☐
Are modifications required?	YES ☒	NO ☐
If so please describe and provide scheduled date of completion. The site wants to install all new CAT5.		
Have you attached all copper/fiber/MDF/RWC layouts available?	YES ☐	NO ☒
Will there be sufficient rack space available in the Wiring Closet to add new equipment/ hardware? The site will install new rack for ICE equip.	YES ☒	NO ☐
Is there sufficient space in the Wiring Closet to add a cabinet or rack, if required?	YES ☒	NO ☐
Is there adequate cooling in the Wiring Closet?	YES ☒	NO ☐
Is there adequate power for the Wiring Closet?	YES ☒	NO ☐

Is the hardware in the Wiring Closet connected to a UPS? YES ☒ YES ☐ NO

Data Communication Recommendations

☐ DSL WITH VPN	☐ County Owned T1 With VPN TOKEN
Comments	**Comments**

☒ ICE T1
Comments ICE T-1 is needed.

Work Station Requests

A total of two (2) IAFIS workstations were requested. The locations were agreed upon by (b)(6), (b)(7)c The site will arrange to have the requisite CAT 5/6 cable run by local cabling company from the Demarc to the ICE Switch. The site will run all new CAT 5/6 cable from the Demarc to the IAFIS Workstations.

Interview/Processing Area for all Inmates

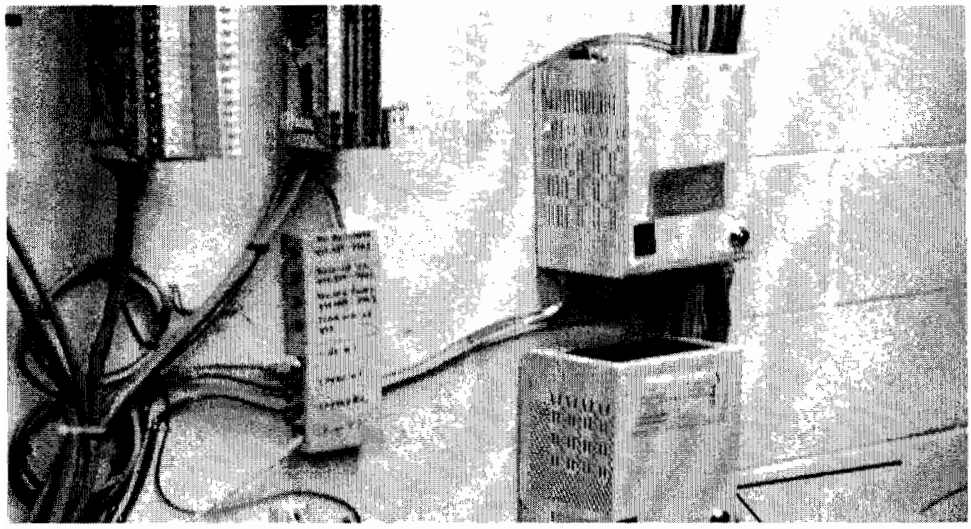
Two IAFIS workstations with a networked printer. The site will build out workspace to accommodate electrical and desktop needs to support the IAFIS workstation and all peripheral devices.

IAFIS work area above

Equipment required for locations pictured above:

2 Workstations
2 Ten Print Scanner
2 Camera
2 Flatbed Scanner
2 Xerox Printers (Networked)
2 HP 1320 Printers

Telecom Room



Training Room


ATTITUDES are contagious