Next Generation IAFIS (NGI)

Privileged User Security Guide
Interstate Photo System Facial Recognition Pilot (IPSFRP) Project

Version 1.3
7 September 2011

NGI-DOC-08440-1.0

Contract No. J-FBI-08-041

Prepared by:

Keane Federal Systems Inc.

Produced for:
Federal Bureau of Investigation
Criminal Justice Information Services Division
1000 Custer Hollow Road
Clarksburg, WV 26306

SIGNATURE PAGE

Prepared by:

b6
b7C

Name: [redacted]

Title: **Principle Consultant**

Organization **Keane Federal Systems, Inc.**

Signature: [redacted] **Date:** **September 7, 2011**

Submitted by:

Name: _____

Title: _____

Organization _____

Signature: _____ **Date:** _____

Coordinated by:

Name: _____

Title: _____

Organization _____

Signature: _____ **Date:** _____

Approved by:

Name: _____

Title: _____

Organization _____

Signature: _____ **Date:** _____

CHANGE STATUS LOG

b6
b7C

VERSION	DATE	REVISED BY	PAGES AFFECTED	REMARKS
1.1	7/19/2011		Cover Page	Updated cover to include new document number, FBI symbol, and CJIS address. Also updated footer.
1.2	9/1/2011		1-22	Made multiple updates per comments received. Also corrected formatting in multiple locations.
1.3	9/7/2011		All	Added page numbers
1.3	9/7/2011		Cover	Minor editing correction

INTRODUCTION

The intent of the Interstate Photo System Facial Recognition Pilot (IPSFRP) is to provide the capability to accept facial search submission requests and return a list of candidates to the user, much like the current latent fingerprint search capability. In addition, a Universal Face Workstation (UFW) will be developed for deployment to users for preparation of facial search transactions, as well as display and processing of search responses. To support the IPSFRP project, a repository of criminal facial images will be compiled from the Interstate Identification Index (III) database. This purpose for this pilot is to provide a proof-of-concept for the final Facial Recognition

The IPSFRP Privileged User Security Guide describes IPSFRP Privileged User's security responsibilities and provides guidelines to assist in meeting those responsibilities.

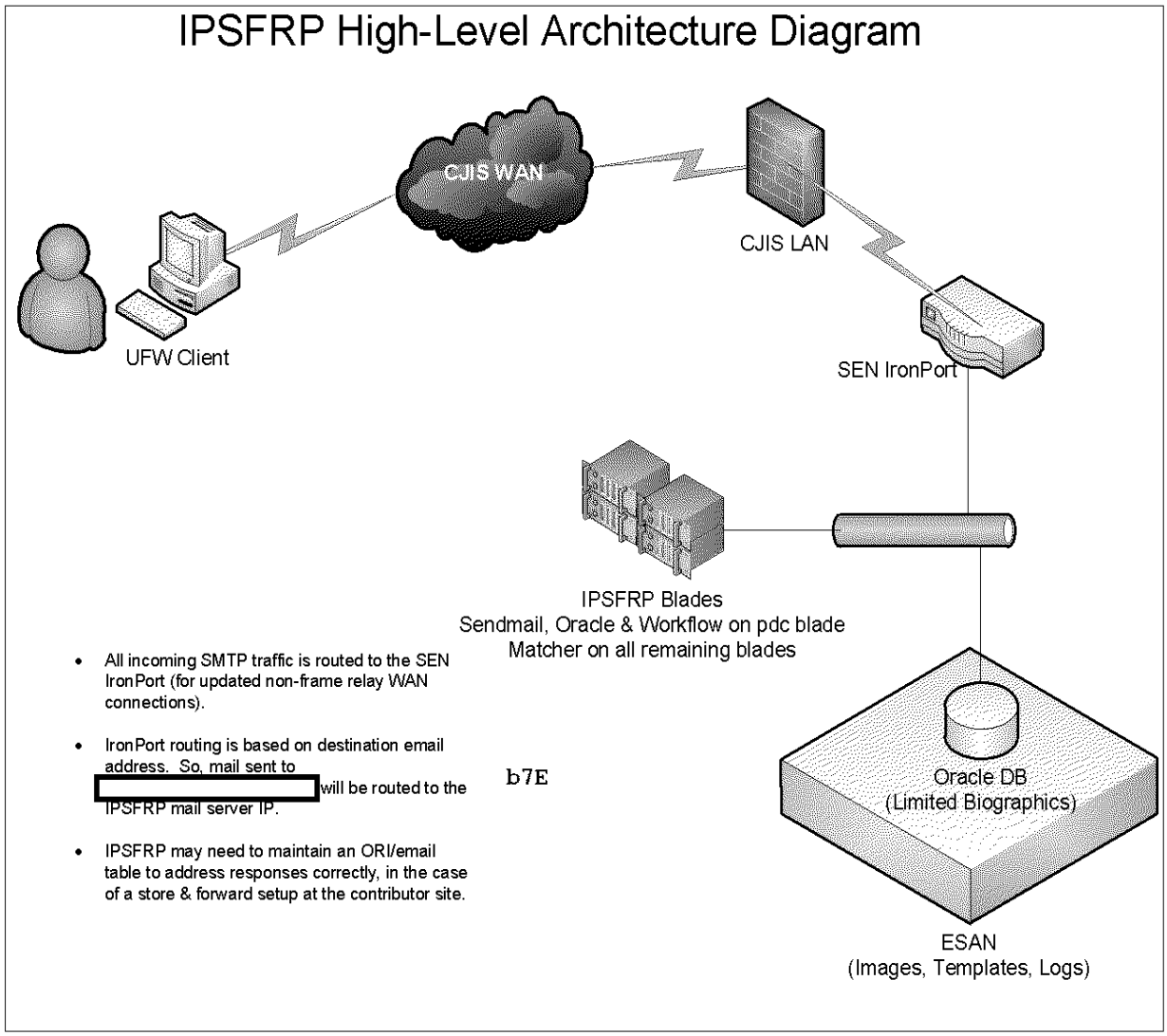
PURPOSE

The PUSG describes the operational procedures and activities used to maintain, configure, and ensure security for the Interstate IPSFRP Project. CJIS personnel, with the appropriate level of technical expertise, use this guide to perform the functions described herein. The PUSG is not a training manual for entry-level personnel.

POLICY

The IPSFRP meets the requirements mandated by Federal, Department of Justice (DOJ), and FBI regulations and standards. All IPSFRP administrators will meet minimum DOJ/FBI clearance requirements to be allowed to administer FBI systems. They will also complete the latest version (2011) Annual Privileged User Security Training

SYSTEM CONFIGURATION, INSTALLATION, AND OPERATION



The IPSFRP system consists of 14 HS-22 Blades configured with 13 active Blades in an IBM Blade chassis with the additional blade serving as redundancy. Each blade provides computing services similar to a stand-alone server.

The server assignments are as follows:

[redacted] This is the Transaction Manager/Database server which handles the parsing and validation of incoming transactions. The Transaction Manager also spawns searches on the match servers and generates response transactions. b7E

[redacted] This server will be clustered with [redacted]

b7E

[redacted]: These eleven servers are the process servers that will perform the actual face matching.

(Hot Spare): This server will act as a hot spare and be built with the matching server system image as needed from a system failure.

Each IBM Blade is configured with:

- 14 Blade Slots
- 2 Management Modules with 1GB Copper interfaces
- 2 4GB Fiber Channel host bus adapters (1 cable in each utilized)
- 2 10GB network interface boards (1 cable in each utilized)

Each IBM Blade is configured with:

- 2 Intel Xeon Central Processing Units (CPUs)
- 96 Gigabyte (GB) of Random Access Memory (RAM)

All IPSFRP servers are installed with the Red Hat Enterprise Linux (RHEL) 5.4 operating system (OS).

STORAGE

All servers will subscribe to the CJIS ESAN Service for disk storage, there will be no local storage on any of the servers.
Space allocation on the CJIS ESAN will be as follows

- Boot LUN's on each blade will be set at 32GB
- Each blade will have a general data LUN of 200GB

b7E • [redacted]

  - /opt/oracle: 20GB - Oracle Database information store
    - Data: 36GB
    - Index: 32GB
    - Archive: 34GB
  - /u01: 70GB – Additional database space
  - /applog: 100GB – Application log space
  - /images: 2000GB – Parsed type 10 images to be used by system
  - /transactions: 14000GB – III EFT's (copied from Electronic Fingerprint Conversion (EFCON)), incoming and outgoing transactions
    - /iii_holding
    - /incoming
    - /outgoing

b7E • [redacted]

- /templates: 500GB – Each matching server's portion of the face matching gallery as well as temporary processing space

BACKUP

See Backup Policy

NETWORKING

The IPSFRP system utilizes network services provided by the CJIS SEN (Shared Enterprise Network). Each IBM Blade chassis has 4 physical interfaces configured to access the SEN. 2 1GB interface for the Management Module and 2 10GB interfaces to various other network resources. These networks are required for management and monitoring of each partition by the system administrators, database administrators, etc., and service provider access, respectively. The IPSFRP Controller/Database Servers [redacted] have connectivity to external networks. b7E

- The controller/db servers receive search and image requests from authorized contributors and internal service providers (via UFW client).
- There are several other network VLAN/subnets configured for use by the IPSFRP systems. Each blade in the configuration has access to:
  - Client - Used for transaction traffic and some applications communications. Data is transferred from other networked systems to IPSFRP via this VLAN.
  - Admin - Used for administrative access to the Operating environment (ssh, backups, maintenance operations, etc.)
  - HB - These are used to maintain cluster health and monitoring
- The IPSFRP system receives submissions from the CJIS WAN via e-mail which is routed through the CJIS DMZ.

NETWORK TRAFFIC

The IPSFRP will utilize existing CJIS SEN networks.

FIREWALL

The IPSFRP will utilize existing CJIS SEN Firewall services

INTRUSION DETECTION

The IPSFRP will utilize existing CJIS Intrusion Detection services to include host-based intrustion detections systems (HIDS) and network based intrusion detection systems (NIDS).

INSTALLATION AND OPERATION COMMON PROCESSES

The HS-22 blades are loaded via kickstart and require no special operational processes for installation other than connectivity to the kickstart server. This kickstart script contains the

following but is not limited to: the Linux RH Base Operating System, Unix Operating System STIGs, security patches, EMC Master Agent install, EMC Solutions Enabler Agent, PowerPath, and IBM Systems Director Client install.

FILE SYSTEM SELECTION

For all servers, Red Hat Enterprise Linux 5.4 will be used.

MAINTAINING RESTRICTED GROUPS

There are three types of IPSFRP privileged users—system administrators, security administrators, and database administrators.

Privileged Users are defined by the FBI C&A Handbook {Section 2.15, Page 2-19} as: "The Privileged User is any user having super-user, root, privileged, or equivalent access to an IS (e.g., system administrators, computer operators, backup operator). They are individuals who who setup and administer user accounts, authenticators, etc., or who have near or complete physical control of an IS."

AUTHORITIES AND QUALIFICATIONS:

U.S. Citizen and U.S. Government or Contractor Employee with current FFBI (or SSBI, as appropriate), current access approvals, and need-to-know for all levels of information processed within his/her purview.

Knowledge of system functions, security policies, technical security safeguards, and operational security measures. Where technically feasible, the Privileged User will be limited to the minimum number of privileges needed to perform assigned functions.

RESPONSIBILITIES OF THE PRIVILEGED USER:

- Reports all suspected IS security-related problems, security anomalies, system vulnerabilities, or suspicious activities of authorized users to the Information System Security Officer (ISSO) or the Information System Security Manager (ISSM).
- Notifies the ISSO of any system configuration changes that might adversely affect system accreditation.
- Maintains security features of the IS to include local accounts and passwords.
- Does not exercise vulnerability assessment tools without written authorization of the ISSM.

SEPARATION OF DUTIES

Each type of privileged user is assigned specific duties and operates within a controlled sphere of influence. Each type of user will have an individual login, including user name and authenticator, tied to

a role allowing them to perform their specific responsibilities. The following paragraphs describe the roles of the privileged users.

SYSTEM ADMINISTRATOR

The System Administrator ensures the system operates in accordance with IPSFRP program operating procedures. System Administrators support both the IPSFRP OE and NOE environments. System Administrators install, maintain, configure, update, and monitor the IPSFRP system. System Administrators have system access based on their function, role, and a need-to-know basis.

THE SYSTEM ADMINISTRATOR MUST:

- Be a U.S. citizen with current FBI clearance.
- Be an employee or Contractor of the United States Government.
- Have a working knowledge of system functions, security policies, technical security safeguards, and operational security measures.

THE SYSTEM ADMINISTRATOR IS RESPONSIBLE FOR (BUT IS NOT LIMITED TO):

- Accesses only that data, control information, software, hardware, and firmware for which they are authorized access and have a need-to-know, and assume only those roles and privileges for which they are authorized.
- Immediately reports all security incidents and potential threats and vulnerabilities involving IPSFRP to the Next Generation Identification (NGI) ISSO and security administrator.
- Protects his/her authenticators and reports any compromise or suspected compromise of an authenticator to the NGI ISSO.
- Ensures that system media and system output are properly classified, marked, controlled, stored, transported, and destroyed.
- Protects terminals/workstations from unauthorized access.
- Informs the ISSO when access to a particular component or function of the IPSFRP system is no longer required.
- Observes rules and regulations governing the secure operations and authorized use of the IPSFRP system.
- Uses IPSFRP for authorized purposes only.
- Does not introduce malicious code into the IPSFRP system and/or physically damage the system.
- Does not bypass, strain, or test security mechanisms. If security mechanisms must be bypassed for any reason, users will coordinate the procedure with the ISSO and receive written permission for the procedure.

- Does not introduce or use unauthorized software, firmware, or hardware on the IPSFRP system.
- Does not relocate or change IPSFRP equipment or the network connectivity of IPSFRP equipment without proper security authorization.
- Implements, operates and maintains timely patch management in accordance with IPSFRP standards and procedures.
- Performs all system maintenance on the IPSFRP System.
- Support system fault and degradation remediation and trouble calls.
- Reports all security concerns to ISSO and ISSM.

SECURITY ADMINISTRATORS

The Security Administrator ensures the system operates in accordance with the IPSFRP System Security Plan and IPSFRP program security operating procedures. Security Administrators support both the IPSFRP OE and NOE environments. Security Administrators install, maintain, configure, update, and monitor IPSFRP Security Controls and audit IPSFRP System and user activities. Security Administrators have system access based on their function, role, and a need-to-know basis.

THE SECURITY ADMINISTRATOR MUST:

- Be a U.S. citizen with current FBI clearance.
- Be an employee or Contractor of the United States Government.
- Have a working knowledge of system functions, security policies, technical security safeguards, and operational security measures.

THE SECURITY ADMINISTRATOR IS RESPONSIBLE FOR (BUT IS NOT LIMITED TO):

- Accesses only that data, control information, software, and hardware for which they are authorized access and have a need-to-know, and assume only those roles and privileges for which they are authorized.
- Immediately reports all security incidents and potential threats and vulnerabilities involving IPFRSP to the NGI ISSO.
- Protects his/her authenticators and reports any compromise or suspected compromise of an authenticator to the NGI ISSO.
- Ensures that system media and system output are properly classified, marked, controlled, stored, transported, and destroyed.
- Protects terminals/workstations from unauthorized access.
- Informs the NGI ISSO when access to a particular component or function of the IPSFRP system is no longer required.
- Observes rules and regulations governing the secure operations and authorized use of the IPSFRP system and security controls.

- Uses IPSFRP for authorized purposes only.
- Does not introduce malicious code into the IPSFRP system and/or physically damage the system.
- Does not bypass, strain, or test security mechanisms. If security mechanisms must be bypassed for any reason, users will coordinate the procedure with the NGI ISSO and receive written permission for the procedure.
- Does not introduce or use unauthorized software, firmware, or hardware on the IPSFRP system.
- Does not relocate or change IPSFRP equipment or the network connectivity of IPSFRP equipment without proper security authorization.
- Ensures that all users have the requisite security clearances, authorization, and need-to-know, and are aware of their security responsibilities before being granted access to the IPSFRP network and administers/witnesses signed user agreements.
- Creates user accounts for IPSFRP system access.
- Establish and maintain IPSFRP password policy.
- Implements system security policies and procedures that are detailed in this document and in the SSP.
- Supports NGI ISSO and ISSM in system and user investigation and incident handling.
- Works with NGI ISSO and ISSM to ensure security compliance.
- Reports all security concerns to NGI ISSO and ISSM.

DATABASE ADMINISTRATOR

The Database Administrator (DBA) ensures the database operates in accordance with IPSFRP program operating procedures. DBAs support both the IPSFRP OE and NOE environments. DBAs install, maintain, configure, update, and monitor the IPSFRP system databases. Database Administrators have system access based on their function, role, and a need-to-know basis.

THE DATABASE ADMINISTRATOR MUST:

- Be a U.S. citizen with current FBI clearance.
- Be an employee or Contractor of the United States Government.
- Have a working knowledge of system functions, security policies, technical security safeguards, and operational security measures.

THE DATABASE ADMINISTRATOR IS RESPONSIBLE FOR (BUT IS NOT LIMITED TO):

- Accesses only that data, control information, software, hardware, and firmware for which they are authorized access and have a need-to-know, and assume only those roles and privileges for which they are authorized.

- Immediately reports all security incidents and potential threats and vulnerabilities involving IPSFRP to the ISSO and security administrator.
- Protects his/her authenticators and reports any compromise or suspected compromise of an authenticator to the ISSO.
- Ensures that system media and system output are properly classified, marked, controlled, stored, transported, and destroyed.
- Protects terminals/workstations from unauthorized access.
- Informs the ISSO when access to a particular component or function of the IPSFRP system is no longer required.
- Observes rules and regulations governing the secure operations and authorized use of the IPSFRP system.
- Uses IPSFRP for authorized purposes only.
- Does not introduce malicious code into the IPSFRP system and/or physically damage the system.
- Does not bypass, strain, or test security mechanisms. If security mechanisms must be bypassed for any reason, users will coordinate the procedure with the ISSO and receive written permission for the procedure.
- Does not introduce or use unauthorized software, firmware, or hardware on the IPSFRP system.
- Does not relocate or change IPSFRP equipment or the network connectivity of IPSFRP equipment without proper security authorization.
- Implements, operates and maintains timely patch management in accordance with IPSFRP standards and procedures.
- Performs all database maintenance on the IPSFRP System.
- Support system fault and degradation remediation and trouble calls.
- Reports all security concerns to ISSO and ISSM.

BACKUP POLICY

The IPSFRP prototype will utilize to the the EMC Networker solution for system backup and restoration.
The EMC® NetWorker product is a suite of storage management software that provides backup, recovery, and other services to computers with a wide variety of operating systems and data types. NetWorker products for different operating systems are interoperable. This provides the flexibility to design a storage management system that works best with the current computing environment.

The NetWorker product has these components:

- NetWorker client
- NetWorker storage node
- NetWorker server
- NetWorker Management Console

The NetWorker client software communicates with the NetWorker server and provides recover and ad hoc (manual) backup functionality. The NetWorker client software is installed on all computers that are backed up to the NetWorker server.

OVERVIEW OF EMC NETWORKER

EMC NetWorker solution is Government Furnished Equipment (GFE) and only the client software resides on IPSFRP systems. The EMC NetWorker solution that is GFE is a General Support System (GSS) within the FBI/CJIS operational environment and resides within the under the Enterprise Storage Solution (ESS) information system boundary..
EMC NetWorker backup policies and restore operations are controlled external to the system boundary of IPSFRP systems. The only piece of EMC NetWorker software that is installed on IPSFRP systems is the EMC NetWorker client. The only EMC NetWorker functionality, via the EMC NetWorker client, that is available to a user that has successfully authenticated to an IPSFRP system is the ability to do a user level backup or restore of files that are readable and writable by that user to a directory that is writable by that user. All other backup and restore functions for the IPSFRP systems are controlled by the EMC NetWorker Server.

USER CONTROLLED BACKUP

EMC NetWorker provides the ability for users to execute backups on demand to save their work and restore it accordingly. These processes can be executed from within the IPSFRP system boundary. In order to perform a backup the user must have read permissions on the files/directories and to perform a restore the user must have read/write permissions on the files/directories.

BACKUP OF USER-OWNED DATA:

b7E

AUDITING

Audit functionality for the EMC NetWorker solution resides on the server side of the implementation which is GFE. Additional details about auditing capabilities for the EMC NetWorker can be found in the *NetWorker Administration Guide* which is delivered in the EMC NetWorker documentation suite.

ACCOUNT CREATION

IPSFRP identification, authentication, and authorization will be controlled via the NGI LDAP service. All accounts will be created following the same process used to create NGI accounts. For accountabilty purposes, each privileged user is required to have their own unique identification associated with their respective roles. LDAP adminstration is done by NGI O&M staff.
This procedure to create new accounts requires the Security Administrator, ISSO, and Security Program Officer in order to sign off on an account creation. The procedure initiates with the submission of the Account Request by the user's manager.
Steps to creating a new NGI account:

RECEIVE ACCOUNT REQUEST:

User's manager fills out the required user forms requesting the user be granted functional access based on the role the user performs. The user must fill out and sign the User Briefing statement, Non Disclosure Agreement and User Access Forms. The Manager verifies completeness of the forms, and submits them to the IPFSRP Security Administrator. The IPFSRP Security Administrator provides the forms to the NGI ISSO, and stores forms for future validation, so that the same User Form Validation process can be used as needed for future validations and audits, and upon personnel changes.

VALIDATE USER FORM:

Upon receiving the user forms the ISSO validates the completeness of all the forms. Any discrepancies require the manager to clarify and the form to be updated. Once the form is complete the ISSO checks off on the valid form providing the User Accounts Form to the Security Program Officer.

1. **Validate User Credentials**: The SPO validates the user's security clearance and checks the Verified FBI clearance checkbox on the User Account Form.

2. **Validate Security Awareness Training**: The SPO validates the user has completed the CJIS Security Awareness training. If the user has not completed the training the SPO provides the training. Once the training is complete the SPO checks the Verified Security Awareness Training checkbox and signs the User Account Form. The SPO then returns the form to the NGI ISSO.

3. **Validate Access Level and Role(s)**: Upon receiving the User Account Form the ISSO validates the SPO has signed off on the form. The ISSO then signs off that the account roles meet the separation of duties and least privilege principles. The NGI ISSO then assigns the User a User ID ensuring it is unique. User IDs must comply with the User ID standards as defined in Section ***Error! Reference source not found.***4.3.1.1.

4. **Create User Account(s)**: Account creation is then processed by the specific system role required to create the user account. Upon creation of the account the administrator performing the task will then sign off on the User Account Form and return the form to the NGI ISSO. The Security Administrator with user provisioning privileges creates the account on the NGI Directory Server LDAP.

5. **Document User Account and Role(s)**: Upon receiving the User Account Form, the ISSO saves the form with the other forms signed by the user. The ISSO will then update the list of Privileged Users and their assigned roles in the:
   a. IPSFRP SSP for Authorized Administrators

6. **Distribute User Account and Initial Password**: When the user accounts are created and documented the ISSO will notify the IPSFRP Security Administrator. The IPSFRP Administrator then notifies the user with the User ID and password through the phone, in person, or by courier. The Security administrator also notifies the user's manager that the account was created and the user now has a valid account.

Note: When the User receives their user account they will log onto the system, the system will force the user to change their password. The password will need to meet the minimum complexity as described below

Note: If the NGI Administrator also requires access to the CJIS data center, fill out either the FBI CJIS Division Data Center Badge Access Request Form or Data Center Visitor Access Request Form. Both forms are available from the FBI CJIS Division OMU Data Center Policy and Procedures document.

PASSWORD REQUIREMENTS

Along with the requirement for each Privileged User to have a unique identification for logging into the various hosts pertaining to their roles, they are also required to have a unique authenticator of a strength that is compliant with the CJIS Security Policy and CJIS CAPP.

PASSWORDS MUST BE:

- At least eight characters in length
- At least one characters each in three of four categories: uppercase alphabet, lowercase alphabet, numerals, and special (non-alphabetic or non-numeral character, such as: @#$%^&*)
- No reuse of the last six passwords, in accordance with the pre-defined password history retention set size.

This policy is enforced in LDAP and also implemented for local accounts on the Oracle DBs.

CJIS WARNING BANNER

The IPSFRP Warning Banner is displayed without requiring any shortened version on any IPSFRP user interface where a banner is capable of being displayed.

CJIS approved usage and security banner published in the CJIS CAPP:

> *"You are accessing a U.S. Government information system, which includes this computer, this computer network, all computers connected to this network, and all devices and/or storage media attached to this network or to a computer on this network. This information system is provided for U.S. Government-authorized use only. Unauthorized or improper use of this system may result in disciplinary action, and civil and criminal penalties.*
> *By using this information system, you understand and consent to the following:*
> *You have no reasonable expectation of privacy regarding any communications transmitted through or data stored on this information system. At any time, the government may monitor, intercept, search and/or seize data transiting or stored on this information system. Any communications transmitted through or data stored on this information system may be disclosed or used for any U.S. Government-authorized purpose."*

CONFIGURATION MANAGEMENT

The IPSFRP system will follow the same configuration management procedures and boards (NGI, IAFIS, TISU, ETIB) as the NGI system as outlined in NGI CDRL 12 (NGI-DOC-05509-8.1) Configuration Management Plan.

DISASTER RECOVERY

In the event of any disaster in which Face Pilot equipment is rendered unusable, the hardware will be replaced, as feasible, and the software reloaded from a gold disk or from a SITs backup if available. The gold disk will reside in the NGI CM library.

However, as this is a pilot program, if CJIS should be unaccessable, there will be no hot site to replace this functionality. The Face Pilot will only be reconstituted when/if resources become available and if deemed necessary.

SYSTEM SECURITY

IPSFRP MEMORANDUM OF UNDERSTANDING

The CJIS Division has established IPSFRP Memorandums of Understanding (MOUs) to formalize the information sharing and interconnection agreements between the IPSFRP

participants. The MOUs cite applicable security policies and procedures, and data classifications or categorizations of the user communities. In addition, the MOUs detail IPSFRP related trusted behavior expectations, communication responsibilities, incident reporting duties, audit trails, training and awareness, certifications, and accreditation. The IPSFRP piloting agencies have been informed that there is no guarantee of system availability. IPSFRP outages may be scheduled or unannounced. All IPSFRP users must sign IPSFRP user agreements that explain the procedures for granting and revoking access to the IPSFRP application.

SECURITY DETAILED DESIGN

The IPSFRP security approach is to implement a best practices strategy that relies on the intelligent application of technologies. The IPSFRP strategy mirrors the NGI security approach, as described in the following paragraphs, by providing a balance between protection capabilities, cost, performance, and operational considerations. The IPSFRP design deploys mechanisms to detect and react to security violations, and ties operational policies to the maintenance of technologies.

SECURITY ASSUMPTIONS

Three key system component classes were identified as having a role in the security picture for IPSFRP as a system: the RHEL host/partitions, the Oracle DBMS implementation, and IPSFRP application layer security controls and business logic:

Host Partitions – 1 Segment Control (Transaction Manager)/Database server [redacted] 11 Process Servers [redacted]. All partitions were installed from the same image utilizing a previously evaluated security baseline from NGI. The primary security controls implemented by the IPSFRP system are provided by the native mechanisms of the installed RHEL 5.4 baseline. b7E

Oracle -- DBMS software installed on 1 Database server [redacted] to host the schemas that make up the IPSFRP repository. The Oracle DBMS also provides a level of security controls relative to the IPSFRP system for which the implemented configuration will need evaluation/verification.

IPSFRP Application -- Application code and business logic governing the IPSFRP processes and services. Specifically, any security controls governing level of access or functions available by direct individual user, indirect group user (ORI), or group membership.

Since the IPSFRP prototype will be integrated within the NGI security boundary, which currently falls under the IAFIS accreditation, certain baseline or "contextual" assumptions were made and leveraged during the evaluation of its security picture as a subsystem of IAFIS. The following are the contextual assumptions identified and used during the preliminary evaluation:

ACCREDITED SECURITY INFRASTRUCTURE

The IPSFRP Prototype shall be integrated into the accredited security infrastructure of IAFIS (services/components utilized include Administrative Workstations (APWs), Service Provider Workstations (SPWs)). IPSFRP hardware will reside within the M2 community of the Shared Enterprize Network (SEN) behind SEN provided firewalls and intrusion detection systems. All internal IPSFRP traffic will ride the SEN network infrastructure.

SECURE OS BASELINE

The IPSFRP Prototype shall utilize a securely configured and previously evaluated NGI OS baseline on all hosts/partitions.

SECURE CONFIG

The IPSFRP prototype shall utilize and securely configure the all hardware following the NGI model utilizing hardening scripts based on DISA STIGs. The IPSFRP prototype shall also tie into NGI's Tripwire integrity monitorinig solution which provides for integrity monitoring, resource monitoring and resource management. Tripwire administration and configuration is outside the scope of the FACE Pilot and will be done by NGI O&M resources.

SECURITY ORACLE CONFIG

The IPSFRP Prototype shall securely implement and configure Oracle modeled upon a previously validated Oracle implementation for NGI.

SECURITY FIREWALL CONFIG

The IPSFRP Prototype shall utilize securely configured and previously validated firewall services from the SEN Firewalls limited to specifically formatted messages sent to a specific email address assigned to the IPSFRP prototype.

SECURITY ESAN SERVICE

The IPSFRP Prototype shall utilize a securely configured and previously validated data storage service: Enterprise Storage Area Network (ESAN).

PERIMETER DEVICES

FIREWALLS AND SWITCHES

The IPSFRP prototype will utilize the current SEN dedicated network switches and firewall suites to provide IPSFRP network connectivity to the CJIS WAN.

The existing SEN firewalls provide stateful access control lists (ACLs) that are used to specify who or what is allowed access, and what operations are allowed. The firewalls also have the capability to note and remember the events in a sequence of interactions with a user or another system, program or hardware device. The stateful inspections performed by the SEN firewalls include inspection of the information being received, inspection of the dynamic connection, and the transmission state of the information being received (communication information, communication-derived state, application-derived state and information manipulation).

The IPSFRP security team will determine the IPSFRP related ACL rule sets and the firewall address configurations on IPSFRP hardware. The IPSFRP team will also request implementation of inbound and outbound ACL entries for each rule, based upon security and business needs. All changes to firewall settings will be reviewed and approved prior to implementation, through the existing NGI change control processes (i.e NPPRs, SPCRs, CPRs, ECRs).

The network layer will implement basic IP address filtering on devices such as firewalls, routers, and servers. This will provide a method of layered authentication when combined with higher-level authentication mechanisms.

b7E

DEVICE HARDENING

Device hardening refers to changing the default posture of a system in order to make it more secure. It is a process that requires updates to lockdown strategies as security needs and network functionality change over time. All network devices will be subject to hardening. Devices secured in a form complementary to their existing counterparts will allow for the seamless integration of the IPSFRP functionality. Device hardening for the IPSFRP project will follow the NGI model using hardening scripts base on DISA STIGs.

OPERATING SYSTEM HARDENING

IPSFRP will utilize the security features in RHEL 5.4. IPSFRP will will follow the NGI model using hardening scripts base on DISA STIGs

DATABASE AND APPLICATION HARDENING

Database and application security has many of the same considerations as host operating system security. IPSFFRP will deploy database and application technologies available through Oracle Enterprise Edition 11g R2. The IPSFRP team will also will follow the NGI model using hardening scripts base on DISA STIGs.

PATCH MANAGEMENT

A major component of device hardening involves the application of the latest security fixes. The IPSFRP team will apply patches to switches, firewalls, and other network components individually.

MANAGEING SECURITY

DATABASE ADMINISTRATION

The IPSFRP Database Administrators (DBAs) will be responsible for the initial creation, installation, configuration and deployment of the IPSFRP database. After deployment, the IPSFRP DBAs will manage and maintain the database to ensure that the data is available at all times and that it is secured and reliable. The IPSFRP DBAs will retain responsibility for all database administration duties until the prototype is decommissioned or the administration duties are transferred to NGI operational personnel.

MANAGING OPERATING SYSTEM ACCESS

Some IPSFRP users (DBA, developers) require access to both the IPSFRP operating system and the IPSFRP database. For security purposes, these are separate user accounts that require separate logons. The system login at the operational level is performed on a host machine and is controlled by the UNIX user authentication and permissions. The database access is a role-based, password protected access.

Secure pathways, provided by protocols such as Secured File Transfer Protocol and secured shell logins, can be used to facilitate administrative functions. All encryption algorithms will meet FIPS 140-2 standards.

MANAGING DATABASE ACCESS

Limiting access to a database is one of the most effective methods for protecting the database and the data within it. IPSFRP will use a role-based access control approach to restrict system access to authorized users. Within the database, the IPSFRP DBAs will create named roles for various job functions. They will then assign "permissions' to perform certain operations to each specific role. System users are then assigned roles, either directly or through group memberships, and through those role assignments acquire the permissions to perform particular system functions. An IPSFRP user may have multiple roles.

User accounts are login identification names associated with a password that are used by the IPSFRP user to access the IPSFRP database. The IPSFRP DBAs will be responsible for creating the IPSFRP user accounts and for following the security guidelines in the CJISCAPP for proper userID naming and password conventions. All direct users of IPSFRP will be assigned their own unique login identification name and will be required to choose a new password after the first, initial login under that user name. IPSFRP will store all IPSFRP password files as encrypted or hashed values.

IPSFRP DATABASE MONITORING

Monitoring of the IPSFRP components will be performed by the IPSFRP DBAs. This will include monitoring IPSFRP performance and responding to system alerts. IPSFRP user auditing will generally rely on the tools provided by the Oracle database. The IPSFRP DBAs are responsible for space and resource monitoring. Oracle Enterprise Manager (OEM) will be used for all monitoring capabilities.

IPSFRP SECURITY AUDITING

Audit data is generated in three distinct layers, OS-level, Database Management System (DBMS)-level, and Application-level. The primary audit data is generated by the OS, which is also the level where the central audit repository is kept, that is, as OS files.

Additional audit data is generated at the DBMS-level (ORACLE), as well as logs of messages and transactions processed at the application-level, which is stored in OS flat files or in ORACLE database tables. These logs are generated by the IPSFRP Middleware applications.

The IPSFRP security will enable auditing for all network devices to include application and database auditing.

AUDIT TRAILS WILL CONTAIN:

- The identity of the administrator or device accessing of attempting access.
- The time and date of access and logoff.
- Activities performed by administrators.
- All changes to security-relevant settings.
- Sufficient detail to facilitate reconstruction.

Relevant personnel will review audit trails on a regular basis with automated tools that will be available in the existing environment. IPSFRP will maintain audit trails on-line for 90 days and off-line back-ups for seven years, per policy. The IPSFRP Audit Policy will cover any additional information on audit trail management procedures.

All logs will be forwarded to the NGI provided LogLogic appliances.

NETWORK TIME PROTOCOL

Timestamps will be synchronized for generated audit information. All network devices will point to the M2 community network time protocol (NTP) server or router.

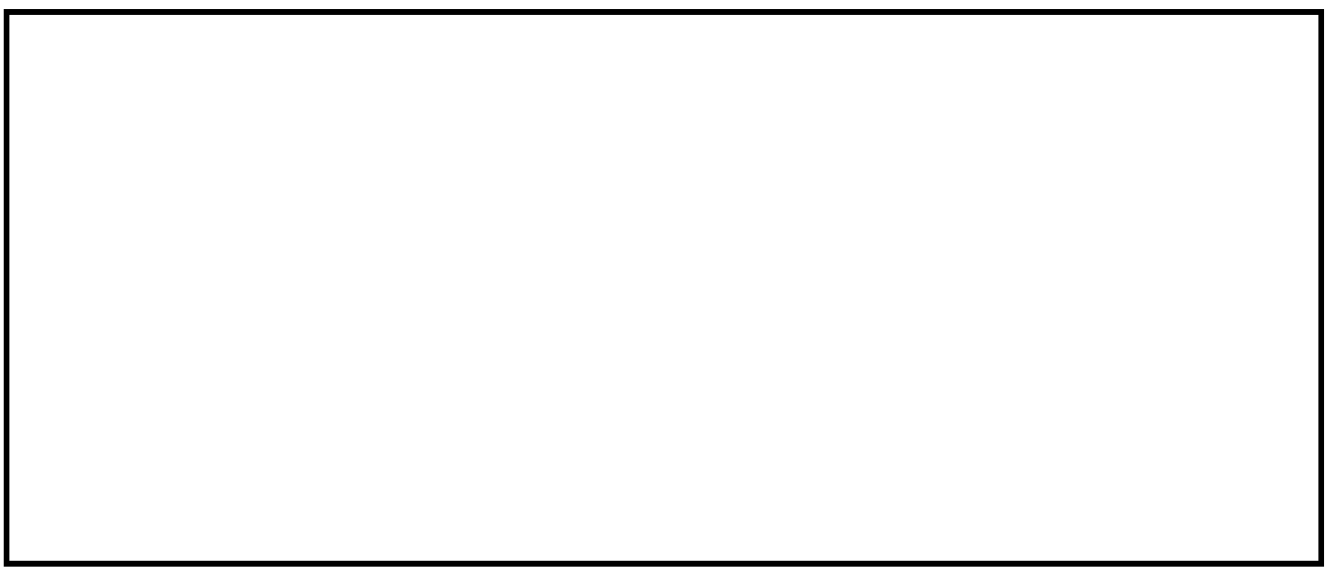
PHYSICAL SECURITY

The physical security of the data center, facilities, and campus safeguards and deterrents are available for those with the authorized Need-to-Know documented in the SSP from the NGI ISSM/ISSO. Access to the data center is restricted based on an automated, intermittent, escorted or emergency basis. Data center access points are monitored by cameras, badge readers and alarmed doors. All personnel access to the CJIS data center is tracked via automated badge readers or manual sign in/out logs. All logs are maintained and controlled by CJIS staff. Physical security also extends to server and equipment access, and wire closets and patch panels.

IPSFRP administrators as part of their secure operations periodically make physical checks of the IPSFRP system. This includes at a minimum:

- Check processors for USB or other unexpected devices attached to any IPSFRP hardware.
- Check processors for disconnected cables or loose cables.
- Check the data center for any Wi-Fi access points.
- Check data center physical access points for proper operation.
- Check for modems.

Note: Data Center personnel also periodically perform system inspections.



b7E

b7E

MISCELLANEOUS

PASSWORD CHANGE UPON DISCOVERY OF SECURITY VIOLATION

Upon the discovery of a suspected or known security violation, the privileged user will immediately change the password(s) on the affected system(s).