MEMORANDUM OF AGREEMENT

Between

The Office of the Federal Detention Trustee,

The Federal Bureau of Prisons,

And

The Southern District of Texas

(U.S. Probation Office and U.S. Marshals Service)

for secure eDesignate Access and Use

Pursuant to authority contained in 28 U.S.C. 534 regarding the "acquisition, preservation, and exchange of identification records and information" between agencies, and in 28 C.F.R. 0.96(c) regarding designations of sentenced federal prisoners, this Memorandum of Agreement (MOA or Agreement) is entered into between the Office of the Federal Detention Trustee (OFDT), the Federal Bureau of Prisons (BOP) and the Southern District of Texas offices of the United States Marshals Service (USMS) and the United States Probation Office (USPO), who hereby **agree as follows:**

SECTION 1. BACKGROUND

1.1 OFDT. The Office of Federal Detention Trustee was created by Congress to look for systemic detention processes with the intention of making improvements and correcting inefficiencies wherever possible. Identifying cost efficiencies and facilitating the development of enterprise solutions, such as streamlining and automating the designation process, are at the core of OFDT's mission.

1.2 THE NEED FOR TECHNOLOGY. With an average daily population of 55,000 detainees across 94 federal judicial districts and an annual federal detention budget exceeding one billion dollars, the goal of improving time and cost savings is paramount. Using technology to share information and process designations results in immediate benefits to the federal agencies that include:

* Streamlining District workload
* Greater efficiency, saving time and money
* Improving process and reporting for management
* Moving prisoners faster to incarceration

1.3 eDESIGNATE OVERVIEW. To facilitate faster processing and reduce workload, the eDesignate system replaces paper-based mail with an electronic alternative. Working together, the agencies field operators and OFDT developed a solution to transfer designation cases via a secure, centralized web server, across varied operating systems and agencies.

1.3.1 Based on user profile access, the eDesignate system collects and displays -

* the Judgment and Commitment order (J&C)
* Pre-Sentence Investigation report (PSR)
* the Statement of Reasons (SOR)
* the USM-129 and detainers, and
* other designation data as required

1.3.2 The electronic solution presents these documents in one complete designation package to BOP, at a single point in time. The system also provides feedback mechanisms across agencies for faster case resolution. The eDesignate system then passes necessary information back to the respective agencies to allow for more effective scheduling of prisoners for ground and air transportation to designated facilities.

1.3.3 eDesignate is a web-based, workflow software developed to accelerate and track the designation process beginning with the sentencing of an individual and ending with the commitment of the inmate to a Federal Prison facility. eDesignate enables its users to access a secure server hosted within DOJ's Data Center via their desktop browser and pass designation documents and required data encrypted by Secure Socket Layer to the necessary agencies within the designation workflow.

SECTION 2. PURPOSE AND SCOPE

2.1 The purpose of this Memorandum of Agreement is to formalize an agreement between OFDT, the Southern District of Texas' USPO and USMS, and the BOP to identify and assign responsibilities for the Southern District of Texas' secure use of OFDT's eDesignate enterprise solution.

2.2 The eDesignate system is for the express purpose of electronically transferring designation data and documents from the Courts (USPO) and USMS to the BOP via eDesignate, owned by the Office of Federal Detention Trustee. End users at the agencies described herein will require access to the eDesignate system where court documents and limited designation specific data from PACTS will be shared with the BOP via eDesignate.

2.3 This Agreement shall not affect any pre-existing independent relationship or obligation between the parties or with any third party or parties.

SECTION 3. PERFORMANCE

3.1 OFDT RESPONSIBILITIES.

3.1.1 ADMINISTRATIVE. As the system owner, OFDT will develop and maintain the system in accordance with applicable federal information security laws and regulations, e.g. the Computer Security Act of 1987, PL 100-235, and the Department of Justice's (DOJ) policy, certification and accreditation standards. Designation specific data from PACTS and electronic court documents will be subject to the same business rules and security considerations as established under the original paper-based process. Specifically, OFDT will:

3.1.1.1 Provide centralized account and password administration for eDesignate.

3.1.1.2 Issue eDesignate Rules of Behavior that apply to all authorized users of eDesignate and correspond to the same business rules for security and safe handling of the paper-based documents.

3.1.1.3 Provide authorized users with application training and help desk support.

3.1.2 TECHNICAL. The eDesignate process begins when the USPO PACTS system triggers a case to be loaded into the eDesignate system. This trigger process is created and owned by the USPO and consists of limited data being pushed to the eDesignate Web Service

and e-Work Transaction Protocol (TP) Client. OFDT then consumes the data via an OFDT created and owned Web Service that in turn transmits the data to the e-Work engine via Transaction Protocol. Once the initial case is established in eDesignate each agency can access the case at stages in the workflow process. The stages include:

3.1.2.1 USPO Stage.

3.1.2.1.1 The case will initially be displayed at the USPO Pool stage. A member of the USPO, normally an administrative clerk with the responsibility of preparing the designation packets, with appropriate user access rights can pick the case up from the USPO pool to take ownership of it.

3.1.2.1.2 Once "picked up," the USPO owner can attach the J&C, PSR, SOR, and any other case documents required for the designation process. Once completed, the USPO owner will submit the case to USMS.

3.1.2.1.3 The system will store all of the documents entered by USPO in the firewall protected OFDT server and will present the case on the To Do list of the USMS at the USMS Pool stage. Each document type is protected individually so that role based access can be applied. Example: Based on the business rules provided by the Southern District of Texas, the USMS will be able to access a case's J&C (see below) however will not be able to access the same case's SOR and PSR based on the access privileges determined by the court.

3.1.2.2 USMS Stage.

3.1.2.2.1 A member of the USMS, normally the criminal clerk with the responsibility of processing the designation packets, with the appropriate user access rights can pick the case up from the USMS pool to take ownership of it.

3.1.2.2.2 Once "picked up," the USMS owner can review the J&C and attach the USM-129 form and any Detainers that apply to the case.

3.1.2.2.3 Once complete, the USMS will submit the case to BOP.

3.1.2.2.4 The system will store all of the documents entered by USMS in the DOJ server and will present the case on the To Do list of the BOP at the BOP Pool stage.

3.1.2.3 BOP Stage.

3.1.2.3.1 A BOP staff member responsible for processing the Designations, with the appropriate access rights can pick the case up from the BOP pool to take ownership of it.

3.1.2.3.2 After reviewing the full set of designation documents included with the case and receiving the designation information through SENTRY, the BOP enters the designation information for the prisoner. This will send a notification of designation including designated facility and date designated to USPO and USMS for acknowledgement.

3.1.2.4 Any Stage. At any stage along the workflow, the case can be returned to a previous stage. All authorized users can access audit procedures that track the case through the entire workflow and associate it with specific users and stages. Management reports provide workflow, processing time, and user information as required.

3.1.2.5 User Identification. OFDT will provide users of eDesignate system-based mechanisms for unique identification and authentication using a password that meets DOJ standards and federal information security requirements.

3.1.2.6 Inactivity Protection. The eDesignate system will provide inactivity protection for the users. At a minimum, a user must enter a password to re-activate an account that has timed out with inactivity.

3.1.2.7 Encryption. Passwords and data will be encrypted prior to transmission. At a minimum end to end line encryption will be applied to transmitted data and documents to ensure security is not compromised.

3.1.3 PHYSICAL. The eDesignate server will be located within a secure, access controlled area, the DOJ Rockville Data Center, and provide 24 x 7 local monitoring and technical support.

3.1.4 PERSONNEL. DOJ personnel and contractors who have access to the eDesignate server and application will be required to have, at a minimum, a favorably adjudicated background investigation and security clearance.

3.2 END USER RESPONSIBILITIES

3.2.1 ADMINISTRATIVE.

3.2.1.1 Appoint an eDesignate end user point of contact who is responsible for interfacing with OFDT and eDesignate system support staff and ensure that the requirements of this Memorandum of Agreement (MOA) are met.

3.2.1.2 Provide OFDT with an initial authorized user list and periodic updates. Verify and certify each eDesignate user meets appropriate security requirements outlined by your organization. Monitor your agency's user list and provide additions and deletions as soon as possible, when applicable. In the case of an unfriendly termination or suspected misuse or compromise of a user's eDesignate ID or password immediately notify OFDT.

3.2.1.3 Distribute eDesignate Rules of Behavior (attachment A) to each authorized user and obtain their signature agreeing to abide by these rules prior to accessing eDesignate. The signed forms shall be maintained by the agency in a secure location and provided to OFDT upon request.

3.2.1.4 Report to OFDT all security incidents that could affect the eDesignate system or the data/documents it represents.

3.2.1.5 Use eDesignate only for authorized purposes and distribute eDesignate information only to authorized persons.

3.2.1.6 Notify OFDT eDesignate staff immediately if business rules for handling of court documents or designation data change so that the eDesignate technical business process- individual document access rules- can be updated to match.

3.2.2 TECHNICAL

3.2.2.1 User Identification. Each agency will provide user information to establish system based mechanisms for unique identification and roles.

3.2.2.2 Provide workstation security protection in accordance with local computer security standards for those workstations that run eDesignate.

3.2.2.3 Encrypt PACTS data prior to transmission. Notify OFDT eDesignate staff when changes are made to PACTS data client if it affects transfer of designation data to eDesignate.

3.2.2.4 Permit access to eDesignate through the Internet Explorer browser. Disable the user's pop-up blocker or at a minimum, ensure the pop-up blocker registers the eDesignate URL as an authorized site.

3.2.3 PHYSICAL. Ensure any computers that access eDesignate are in an access controlled area and are password protected.

3.2.4 PERSONNEL. Each agency will ensure all personnel who have access to eDesignate have met locally prescribed requirements for the secure handling of data and documents.

SECTION 4. LIABILITY AND IMDEMNIFICATION

4.1 Each party shall be responsible for any liability arising from its own conduct and retain immunity and all defenses available to them pursuant to federal law. Neither party agrees to insure, defend, or indemnify the other party.

4.2 Each party shall cooperate with the other party in the investigation and resolution of administrative actions and/or litigation arising from conduct related to the responsibilities and procedures addressed herein.

4.3 This Agreement is for the sole and exclusive benefit of the signatory parties, and shall not be construed to bestow any legal right or benefit upon any other persons or entities.

SECTION 5. ANTI-DEFICIENCY ACT

Nothing contained herein shall be construed to obligate the parties to any expenditure or obligation of funds in excess or in advance of appropriations, in accordance with the Anti-Deficiency Act, 31 U.S.C. 1341.

SECTION 6. PERIOD OF AGREEMENT/TERMINATION

This MOA is valid for two years after the last date of any signature below, unless terminated sooner by mutual agreement of all parties or [assuming each party wants to maintain a right to unilaterally terminate participation] by any party's written notice to the other parties 30 days in advance of that party's withdrawal from the MOU.

THE UNDERSIGNED AGREE TO THE PROVISIONS SET FORTH IN THIS DOCUMENT FOR THE SECURE OPERATIONS OF E-DESIGNATE.

Office of the Federal Detention Trustee:

///S////2/28/06
Stacia A. Hylton, Federal Detention Trustee — Date

U.S. Probation Office, Southern District of Texas:

///S////3/15/06
Becky Burks, Chief U.S. Probation Officer — Date

U.S. Marshals Service, Southern District of Texas:

///S////3/20/06
Ruben Monzon, U.S. Marshal — Date

Bureau of Prisons:

///S////4/01/06
John M. Vanyur, Assistant Director — Date
Correctional Programs Division

SECTION 7. MODIFICATIONS

Any party may propose to modify this MOA at any time. All modifications shall be effective only upon the signatory concurrence of all parties.

SECTION 8. DISPUTE RESOLUTION

In the event of a dispute between the parties, the parties agree that they will use their best efforts to resolve that dispute in an informal fashion through consultation and communication, or other forms of non-binding alternative dispute resolution mutually acceptable to the parties.

Attachment A
eDesignate Rules of Behavior

You have requested access to eDesignate because the unique requirements of your job dictate a need for access to the system from your computer. Because the data and documents passed through eDesignate are sensitive in nature and protected by the Privacy Act of 1974, 5 U.S.C. 552a, and other federal laws, regulations and practices, unauthorized access or disclosure of certain information herein could result in potential threats to the safety of agency staff or inmates, and subject the user to criminal and/or civil penalties. Therefore, special precautionary procedures must be adhered to while accessing and working within the eDesignate application.

1. Abide by all provisions of your agency's information security policy and procedures.

2. Ensure your user information is current and your ID and password are safeguarded.

3. Treat electronic documents and data with the same security business rules as paper-based documents.

4. Be cautious when working with the application to ensure eDesignate information is not disclosed inappropriately. This includes:

    a. Making sure monitors are not viewable by others

    b. Not sharing your eDesignate User ID/password

    c. Being aware of those around you and your surroundings

    d. Keeping your computer secure by enabling password protection

    e. Keeping all printed documents and data storage devices generated from an eDesignate session in your possession or locked in a secure place not accessible to the general public.

I, the undersigned, understand the requirements stated above and agree to comply with regulations related to protecting sensitive information.

_____ _____

Full Name, Office Date