

Memorandum of Understanding / Agreement
Between
The Department of Energy
and
The Office of Personnel Management
Federal Investigative Services Division
for the
Agency Delivery Pilot

I. Purpose

The purpose of this Memorandum of Understanding (MOU) is to formalize an agreement between The Department of Energy (DOE) and the Office of Personnel Management (OPM) Federal Investigative Services Division (FISD) regarding participation in the Agency Delivery pilot. This MOU sets forth expectations and responsibilities for participation in this pilot.

II. Background

The Office of Personnel Management (OPM) Federal Investigative Services Division (FISD) is committed to utilizing technological tools in order to expedite elements of background investigations conducted on individuals (employees or applicants) for federal employment, consultants, volunteers and/or contractor personnel and for national security purposes.

Therefore, wherever possible and mutually beneficial, OPM FISD encourages user agencies to connect to its investigative applications/systems in order to meet the timeliness deadlines set forth in the Intelligence Reform and Terrorism Prevention Act of 2004. This MOU sets forth the basic principles and guidelines under which DOE will connect to OPM FISD's applications/systems.

Agency Delivery is the electronic assembly and delivery of a closed case file from OPM FISD to the requesting agency. Agency Delivery will replace the current process of mailing closed case files. It is the vision of FISD to increase the timelines, efficiency, and accuracy of the investigative process through Agency Delivery.

III. Authority

This MOU is authorized in accordance with E.O. 10450—Security Requirements for Government Employees, E.O. 12968—Access to Classified Information, the Homeland Security Presidential Directive (HSPD-12) of August 2004, the Clinger-Cohen Act of 1996, the Government Paperwork Elimination Act of 1998, the President's Management Agenda of 2002, the e-Government Act of 2002, and the Intelligence Reform and Terrorism Prevention Act of 2004 with the general cooperative authority provided under the Economy Act of 1932, 31 U.S.C. Section 1535. These Federal provisions provide for the relevant Federal agency to utilize other Federal agencies in providing goods or services when the requests are in the best interest of the government. In accordance with 31 U.S.C. 1535 and with Section 17.503 of the Federal Acquisition Regulation, the contracting official of DOE makes determinations and findings

(D&F), as attached hereto; Section 204 of E Government Act of 2002 (44 U.S.C. 3501 note); and 40 U.S.C. 11318.

IV. Expectations

Agency Delivery consists of three distinct aspects; the content, packaging, and delivery of a closed case file.

Content

The content of the Agency Delivery closed case file will be identical to the content of the current paper mail out.

Packaging

Agency Delivery will package the contents of a closed case file in a 128-bit encrypted ZIP file known as a Distributed Investigative File (DIF). The DIF will serve as an electronic representation of a closed case file and will provide both a graphic representation of the normally printed file and a data representation of certain documents (see Appendix A for specifics). The DIF will contain the following three files:

- A Portable Document File (PDF) containing:
 - Images of all the documents in a closed case file
- An Extensible Markup Language (XML) file (see Appendix B) containing:
 - Subject Information
 - Closing Documents (Closed Case Transmittal (CCT), Certificate of Investigation (COI), Report of Agency Adjudicative Action (79A), Report of Investigation (ROI), Credit Report, and FBI Fingerprint)
- An XML file containing
 - The SF 86 form data from e-QIP

Delivery

Closed case files will be transferred to requesting agencies via a nightly batch file push from OPM's data center using Connect:Direct Secure + containing:

- DIFs (ZIP files)
- An XML transfer manifest (see Appendix C) in a 128-bit encrypted ZIP file containing a list of all closed case files included in the transfer along with the following information:
 - Case number
 - Subject name
 - Subject SSN
 - Closed case file names
 - Closed case file passwords

V. Privacy Act

The Privacy Act of 1974, 5 USC §552a, regulates the collection, maintenance, use, and dissemination of personal information in government records when that information is retrieved by the name or other personal identifier of the subject of record. As DOE is requesting services of OPM in complying with various legal and identity processing requirements, it is OPM's responsibility to ensure that the requirements of the Privacy Act are complied with, including publication of an appropriate Privacy Act System of Records Notice in the Federal Register. Failure to publish such a timely notice in the Federal Register shall be grounds to terminate this agreement.

Based on the purpose of this MOU the parties agree that information which is exchanged that is source selection sensitive, proprietary, or Sensitive Security Information (SSI) shall be protected in accordance with applicable statutes. The parties agree to protect these communications and information from unauthorized disclosure. Any release of SSI to any third party is prohibited unless legally required. The Parties agree that if personal information is collected and used in any manner that collection and use shall be only for the limited purposes set forth in this MOU.

In accordance with OMB Circular A-130, Management of Federal Information Resources, DOE and OPM agree information in the Agency Delivery package (DIF) covered by this MOU is considered "Information about Persons," defined as "information related to personnel and similar data." As such, the sensitivity level of the system is rated moderate, with an impact description of "moderate," with the potential for a breach to cause severe impairment of missions, functions, image and reputation. The impact of a breach would place the government at a significant disadvantage or would result in major damage, requiring extensive repairs to assets or resources.

VI. Responsibilities

OPM FISD Agrees to the Following:

- OPM will provide an Agency Delivery package (DIF) validation process for DOE prior to the full acceptance of Agency Delivery.

DOE Agrees to the Following:

- DOE will procure Connect:Direct Secure +.
- DOE will report Adjudicative Actions using the "Enter Agency Adjudication" function on the PIPS Agency Menu which is accessible through either a dedicated PIPS terminal or FISD's web-based Secure Portal.
- DOE will destroy the Agency Delivery package (DIF) after an eligibility has been rendered and the data is no longer needed.
- DOE will not reproduce or distribute the Agency Delivery package (DIF) without the consent of OPM-FIPC.

VII. CJIS IT Security Responsibility for OPM and Agency Customers

OPM, Federal Investigative Services Division is designated as a CJIS Systems Agency and has been informed by the FBI that it is responsible for both ensuring that CJIS data is protected within the OPM environment and that agencies receiving CJIS data (criminal history fingerprint results, rap sheet information, or "No Record" information) enforce CJIS security policy and requirements for the dissemination and protection of CJIS data. OPM will further be responsible for auditing federal agency customers or Interface Agencies for their compliance with the CJIS security policy beginning in 2008. OPM, Federal Investigative Services Division, IT Security, and Assurance requests the following information for coordination of this effort:

IT Security Point of Contact: Raymond C. Holmer
Telephone No.: 301-903-7325
Email: Raymond.holmer@hq.doe.gov

Please see the CJIS Security Policy reference information below for broader clarification:

3.1 CJIS Systems Agencies

The CJIS Systems Agency (CSA) is responsible for establishing and administering an IT security program throughout the CSA's user community, to include the local levels. The CJIS Systems Officer is therefore responsible to set, maintain, and enforce the following:

- a) Standards for the selection, supervision, and separation of personnel who have CJIS systems access.
- b) Policy governing the operation of computers, access devices, circuits, hubs, routers, firewalls, and other components that comprise and support a telecommunications network and related CJIS systems used to process, store, or transmit criminal justice information, guaranteeing the priority, integrity, and availability of service needed by the criminal justice community.
- c) Responsibility for the management of security control shall remain with the criminal justice agency. Security control includes the authority to set and enforce policy governing the operation of computers, circuits, and telecommunications terminals used to process, store, or transmit CJIS data and to guarantee the priority service needed by the criminal justice community. This control is to ensure that privatization and/or delegation to noncriminal justice agencies does not diminish the existing degree of control exercised by the CSA prior to the CFR changes in October, 1999 as stated in the March 2000 White Paper on Management Control.
- d) Responsibility for the management control of network security shall remain with the criminal justice agency. Management control of network security includes the authority to set and enforce policy governing the operation of circuits and network equipment used to transmit CJIS data and to guarantee the priority service as determined by the criminal justice community. If the CSA is not satisfied that the CSA exercises the necessary management control of network security on any network segment transmitting CJIS data, then that network segment shall be considered a foreign network. The CSA shall meet all necessary security requirements in connecting to that foreign network segment, such as encryption, firewalls, etc. that are applied to the transmission of CJIS data over the Internet or any foreign network.

Each CSA shall also establish an information security structure that provides for an ISO and shall ensure that each Interface Agency having access to a criminal justice network has someone designated as the security Point of Contact (POC).

Interface Agency

The *CJIS Security Policy* also applies to other types of authorized user agencies, organizations, entities, and public law applications, which for the application of this policy and within the confines of this policy, shall be referred to as an Interface Agency.

VIII. Resolution Mechanism

In the event of disagreement arising under this MOU; Lynn London, Information Technology Program (ITP) Manager for FISS, and the appropriate DOE personnel shall negotiate a resolution.

IX. Effect of Agreement

Nothing in this MOU shall be interpreted as limiting, superseding or otherwise affecting either agency's normal operations or decisions in carrying out its statutory or regulatory duties. This MOU does not limit or restrict DOE from participating in arrangements with other entities. This MOU does not in and of itself authorize the expenditure or reimbursement of any funds. Nothing in this MOU obligates DOE to expend appropriations or enter into any contract or other obligations.

X. Effective Date and Duration of Agreement

The effective date of this agreement will be the date of the last signature of the agreement. This agreement will last for a period of one year after which it will enter a period of review for renewal.

Any changes to this MOU will be by mutual consent of the parties, in writing, and will be published as an amendment to this MOU.

XI. Points of Contact

Chris DeMatteis
Office of Personnel Management
Federal Investigative Services Division
1137 Branchton Road
Boyers, PA 16018
(724)794-5612

Stephanie J. Brewer, Director
Office of Departmental Personnel Security
Office of Health, Safety and Security

U.S. Department of Energy
1000 Independence Avenue, SW
Washington, DC 20585
(202) 586-3249

XII. SIGNATURES

The undersigned agree to the terms and conditions of this Memorandum of Understanding:



Janice L. Condo
Program Manager
Office of Personnel Management
Federal Investigative Services Division
Agency Liaison Group
Washington, DC, 20301

_____ 5/1/08
Date



Stephanie J. Brewer
Director
Office of Departmental Personnel Security
Office of Health, Safety and Security
U.S. Department of Energy

_____ 4/24/08
Date



Lesley A. Gasperow
Director
Office of Resources Management
Office of Health, Safety and Security
U.S. Department of Energy

_____ 4/23/08
Date

Appendix A – The DIF Document Set

DOCUMENT	Distributed Investigative File (DIF)					Manifest XML
	DIF PDF		DIF XML		XML e-QIP*	
	PDF	PDF TXT	XML TEXT	XML DATA		
Closed Case Transmittal (CCT)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Certificate of Investigation (COI)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Report of Agency Adjudicative Action (79A)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Standard Form 86 (e-QIP AUB will be the first DOC Type*)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Report of Investigation (ROI from PIPS)*	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
FBI Fingerprint (B0#)*	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Credit Report (E0#)*	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Other Documents*	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Manifest XML (Crosswalk)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
*If Applicable	<input checked="" type="checkbox"/> In Document <input type="checkbox"/> Not in document					

Appendix B – The DIF XML File Layout

XML TAG	PARENT	DATA	DESCRIPTION
<?xml>	None		XML Header
<oprclosings>	None		Case Element
<cctData>	<oprclosings>		CCT Data Elements
<caseInfo>	<cctData>		Case Information; event='CM'
<caseNumber>	<caseInfo>	Char(8)	8 – 10 character Case Number
<createdDate>	<caseInfo>	Date	Date the DIF was created
<lastName>	<caseInfo>	Char(20)	Subject Last Name
<firstName>	<caseInfo>	Char(15)	Subject First Name
<ssn>	<caseInfo>	Char(9)	Subject Social Security Number
<dob>	<caseInfo>	Date	Subject Date of Birth
<eqipRequestNumber>	<caseInfo>		e-QIP Request Number (Blank or Number)
<closeDate>	<caseInfo>	Date	Date investigation closed
<soi>	<caseInfo>	Char(4)	Security Office Indicator
<son>	<caseInfo>	Char(4)	Submitting Office Number
<caseType>	<caseInfo>	Char(4)	Two Character Case Type*
<caseService>	<caseInfo>	Char(1)	Single Character Service Code*
<caseSeriousness>	<caseInfo>	Char(1)	Seriousness Codes (Blank or Code)*
<agencyData>	<caseInfo>	Char(25)	PIPS Accounting Data
<extraCovCodes>	<agencyData>	Char(2)	Extra Coverage Codes (Blank or Code)*
<documents>	<cctData>		Documents Element
<document>	<documents>		Document Element
<![CDATA[<document>		ASCII Text of Document
<itemIndex>	<cctData>		Item Index Element
<item>	<itemIndex>	Char(3)	Single Item Processed
<type>	<item>	Char(4)	Item Type*
<location>	<item>	Char(42)	Location Where Item Was Processed
<city>	<item>	Char(38)	City Where Item Was Processed
<method>	<item>	Char(1)	Item Coverage Method*
<result>	<item>	Char(2)	Item Result*

Appendix C – The Transfer Manifest XML File Layout

XML TAG	PARENT	DATA	DESCRIPTION
<?xml>	None		XML Header
<opmclosings>	None		Case Element
<DIFCrosswalk>	<opmclosings>		Agency = AgencyName, date = date processed yyymmdd
<caseInfo>	<DIFCrosswalk>		Case Information
<subjectName>	<caseInfo>	Char(8)	Subject Full Name 35 Characters
<subjectSSN>	<caseInfo>	Date	Subject Social Security Number 9 Characters
<fileName>	<caseInfo>	Char(20)	File Name CaseNumber + first 5 of LastName
<firstPassword>	<caseInfo>	Char(15)	CaseNumber + SubjectSSN

Appendix D- Rules of Behavior

Data Exchange/Interconnection Security Agreement and Partner Rules of Behavior and Responsibilities

As a business partner of the US Office of Personnel Management (OPM), you are expected to understand and comply with the responsibilities outlined below. These responsibilities are security controls set up to protect the confidentiality, integrity and availability of OPM's stored data and information systems.

Service Restoration and Disaster Recovery Details: OPM maintains a Disaster Recovery Plan for restoration of service. The design of the process to exchange data has been engineered according to the details of the plan. If the plan is executed, you will be contacted with instructions how to alter the exchanges.

Problem Reporting: When problems occur, your organization is expected to report the incident to the OPM Data Center Group (DCG) promptly for resolution. The numbers available for contact are the OPM HELP Desk at 202-606-4927 or the DCG Data Exchange Coordinator at 202-606-1436.

Problem Resolutions: The availability of the computer systems is a matter of importance both to your organization and OPM. You are responsible for assisting OPM solving problems in the event the transfer process/connection becomes non-operational.

Protection of Data: You are not allowed to introduce any unauthorized data (including data protected by copyright, trademark, other proprietary data or material with other intellectual property rights) onto OPM's system. In addition, you will protect all sensitive information received from OPM. This includes records about individuals requiring protection under the Privacy Act, sensitive financial information, and information that cannot be released under the Freedom of Information Act. To be in compliance with the OMB memorandum M-06-16, you are required to delete sensitive data received from OPM within 90 days unless its use is still required as documented in a Memorandum of Understanding (MOU) with OPM.

Incident Reporting: All security incidents, along with the reporting and response actions taken, will be documented. At a minimum, the following information will be recorded for each incident:

- Date and time notified appropriate security and management personnel to include US OPM FISD ISSO at (202) 606-1042 and Privacy Officer at (724) 794-5612.
- Description of incident.
- Identification of the individual reporting the security incident.
- Identification of the loss, potential loss, access attempt, or misuse.
- Identification of the perpetrator (if possible).
- Document response and/or monitoring activities.

Use of Secure Point-of-Entry (SPOE): You will not be issued an OPM Userid and password. You will be using the Connect:Direct SPOE to exchange data with OPM's system. SPOE eliminates the need for data partners to exchange Userid and password information, by matching the incoming userid, IP address and Connect:Direct node name to an entry on the product's authentication table. However, you must protect your password from disclosure by all reasonable means, and not willingly divulge it or allow its use by any other person(s).

Questionnaire Updates: You agree to complete the questionnaire provided and to notify OPM promptly of changes in its information.