



**Memorandum of Understanding
Between
The Office of Personnel Management
Federal Investigative Services Division
and
The Department of Energy (DOE)
For Access to the Fingerprint Transaction System (FTS)
and processing of Fingerprint-Only Electronic Special Agreement Checks (e-SACs)**

I. Background

- A. 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 Federal employees, applicants for Federal employment, members of the military, consultants, volunteers and/or contractor personnel and for national security purposes.
- B. 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 National Security Intelligence Reform Act of 2004. This Memorandum of Understanding (MOU) sets forth the basic principles and guidelines under which DOE will connect to OPM FISD's application/systems.

II. Purpose

The purpose of this MOU is to establish the requirements that must be in place in order to allow access to the Fingerprint Transaction System (FTS) and submission of fingerprint-only Electronic Special Agreement Checks (SAC's) by DOE to OPM FISD.

III. Authority

- A. This MOU is authorized in accordance with **E.O. 10450—Security Requirements for Government Employment, E.O. 12968—Access to Classified Information, and the Homeland Security Presidential Directive 12 (HSPD-12)—Policy for a Common Identification Standard for Federal Employees and Contractors**, with the general cooperative authority provided under the Economy Act of 1932, 31 U.S.C. Section 1535. These Federal provisions allow for the relevant Federal agency to utilize other Federal agencies to obtain 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 Regulations (48 CFR 17.503), 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.

- B. DOE enters into this agreement specifically under 5 CFR 736.101 and the Economy Act of 1932 (31 U.S.C. 1535-36), to request from OPM reimbursable services to process e-SACs for DOE on Federal employees, applicants for Federal employment, members of the military, consultants, volunteers, and/or contractor personnel.**

IV. Processing e-SAC Requests

- A. e-SAC requests must be submitted using the appropriately certified and tested hardware and software components.**
 - i. Electronic fingerprinting hardware must be certified as compliant with the FBI's Integrated Automated Fingerprint Identification System Image Quality Specifications.**
 - ii. Systems must employ OPM-approved software.**
 - iii. All systems must be tested for compliance prior to DOE being authorized to submit fingerprints.**
- B. e-SAC requests must indicate the appropriate value in the Retention Field (EFTS Field 2.0005 labeled "RET").**
 - i. "Y" (Retain) for all federal employees, applicants and members of the military.**
 - ii. "N" (Do Not Retain) for all contractor, consultant, and volunteer personnel.**
- C. Each submission must include the agency's Submitting Office Number (SON), Security Office Identifier (SOI), and Agency Locator Code (ALC) in the Controlling Agency Identifier (CRI) field.**
- D. Requests may only be made on individuals who complete an SF 85, SF 85P or SF 86. Fingerprint checks for other purposes will be processed if the appropriate Special Agreement Check (SAC) has been signed.**
- E. OPM requires all electronic fingerprint submissions to pass basic image quality and data validation checks in order to be processed. OPM will notify DOE via telephone of submissions failing the validation, along with the associated subject and error information. DOE must validate the appropriate data and/or transmit a new set of fingerprints for that subject when requested.**
- F. Results of the e-SACs will be provided by OPM to the appropriate Security Office identified by the SOI in the same format as previously provided. (The results will not be returned via the livescan system.)**

V. Interconnection Security Agreement

The technical details of the interconnection will be documented in an Interconnection Security Agreement (ISA). The parties agree to work together to develop an ISA for each FTS site, which must be signed by all parties before the interconnection is activated. Proposed changes to either system or the interconnecting medium will be

reviewed and evaluated to determine the potential impact on the interconnection. The ISA will be renegotiated before changes are implemented. Signatories to the ISA shall be the Designated Authority for each system.

The following components are contained in the associated ISA between OPM and DOE:

- * RULES OF BEHAVIOR
- * SECURITY CONTROLS
- * LIST OF INTERCONNECTED APPLICATIONS
- * SYSTEMS AND APPLICATION/SYSTEM IDENTIFIERS
- * RULES FOR INTERCONNECTING APPLICATIONS/SYSTEMS
- * PROTECTING SHARED DATA

VI. Effective Date and Termination

This MOU will become effective upon the latest date of signature. It shall remain in effect for five (5) years unless otherwise modified or terminated. Any party may withdraw upon 90 days written notification to the other. This MOU can be modified through mutual written agreement among the Parties, and shall remain in effect until modified or terminated by either party, or as terminated for other reasons described in this MOU.

VII. 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.

VIII. Privacy Act

- A.** The Privacy Act of 1974, 5 U.S.C. 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. FTS data will be stored or retrieved by a personal identifier, thus the Privacy Act applies to the use of FTS. Because **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.
- B.** 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.

- C. In accordance with OMB Circular A-130, Management of Federal Information Resources, **DOE** and OPM agree information in the FTS 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.

IX. Security Controls

In order to comply with the provisions of the Privacy Act, information captured by FTS (which includes personally identifiable information) will be secured and not subject to unauthorized distribution. The FTS application provides security protections to afford compliance with the Federal Information Security Management Act (FISMA) and Privacy Act provisions, as follows:

Authorization: The application uses role-based authorization, which enhances confidentiality. In addition, strong and encrypted passwords provide filers with greater assurance of confidentiality.

Authentication: Applicant information in FTS will be stored in a way to assure that each applicant has a unique identity. This unique identity will allow accurate authentication and creation of records that retain confidentiality through integrity controls. Assuring a user's identity will be accomplished through the use of unique shared secrets (e.g., portion of the SSN string, DOB, and name).

Secure Data Storage and Transmission: Any sensitive data sent over FTS is encrypted before transmission. This encryption meets federal standards and occurs within an encrypted tunnel.

Integrity: Users and organizations are validated by FTS security controls.

Least-privilege access controls, based on roles assigned to the users, mitigate the risk of disclosure and inadvertent deletion of data.

X. Material Changes to System Configuration

Planned technical changes to the system architecture that directly affect the other party will be reported to technical staff before such changes are implemented. The initiating party agrees to conduct a risk assessment on significant system architecture changes.

The parties will modify and re-sign the ISA within one (1) month of implementation if the system architecture change has a significant impact to either party.

XI. Liaison

Liaison will be maintained between the DOE Acting Director, Office of Departmental Personnel Security, Stephanie S. Grimes, and the OPM Chief, Agency Liaison Group, Janice L. Condo.

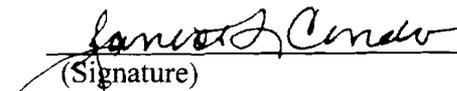
XII. Approvals

Department of Energy:

 11/8/07
(Signature) (Date)

Stephanie S. Grimes
Acting Director
Office of Departmental Personnel Security
Department of Energy

Office of Personnel Management:

 Oct 17 2007
(Signature) (Date)

Janice L. Condo
Chief, Agency Liaison Group
Federal Investigative Services Division
Office of Personnel Management