Addendum to the Privacy Impact Assessment for the

Justice Security Tracking and Adjudication Record System

April 14, 2010

Contact Person
Dorianna Rice, Data Owner
Assistant Director Personnel Security Group
Department of Justice
(202-514-2351)

Selicia Copening, User Representative
Chief of Operations Section, Personnel Security Group
Department of Justice
(202-514-2351)

Reviewing Official
Nancy C. Libin
Chief Privacy and Civil Liberties Officer
Department of Justice
(202) 514-0201

1.0 BACKGROUND

The Justice Security Tracking and Adjudication Record System (JSTARS) automates the tracking of personnel security investigation activities for the Department of Justice (DOJ). The purpose of JSTARS is to enable the DOJ Security and Emergency Planning Staff (SEPS), Personnel Security Group (PERSG) to store and manage DOJ personnel security information, including the courtesy copies of Background Investigations sent by the Office of Personnel Management (OPM).

This addendum to the JSTARS Privacy Impact Assessment (PIA), dated May 2, 2008, addresses a change in the manner in which documents are received from OPM. In an effort to move away from paper-based processing, security related documents, such as background investigations, are digitized and uploaded into JSTARS manually today. The purpose of JSTARS release 2.2 is to automate the transmission of the background investigation into JSTARS through OPM's eDelivery offering which replaces the paper-based, courier-based transmission of completed investigations to electronic delivery.

What is eDelivery?
Electronic Delivery (eDelivery) is the electronic packaging and delivery of closed complete investigation files to customer agencies in a usable electronic format. It eliminates the mail out of hardcopy investigative files, and allows agencies to process as needed based on the automation/technology systems they have in place.

How is the file transfer done?
Direct:Connect Secure+, a product from Sterling Commerce, is used to do the file transfer. Direct:Connect Secure+ is certified to meet the security requirements of FIPS 140-2. In addition it allows authentication and encryption to be applied between servers to ensure secure file transfer. With Secure + Option, Transport Layer Security (TLS) is used to perform authentication between servers and provides data encryption for transferring files.

What is in each transmission and what is the frequency of the transmissions?
Each night the following files will be transmitted to DOJ from OPM via the Direct:Connect Secure+ software using a Data Interchange File (*.DIF) and a transport eXtensible Markup Language (XML) manifest file:

- Background Investigation for a Candidate in PDF format
- Background Investigation for a Candidate in XML format
- eQIP Application for a Candidate in XML format

Upon DOJ receipt of the files, the files will be uploaded in the JSTARS database and stored

within the personnel security case file for the specific employee or contractor. Once there is a successful load into the JSTARS database, the transport manifest and DIF files will be deleted.

What logs exist to document this electronic transfer of information?

There are two sets of logs that will exist with implementation of eDelivery.

- OPM and DOJ transmission logs that record the successful transmission of information from OPM to DOJ. These logs are inspected if failed transmission occurs.
- JSTARS system case log that records the ingestion of the *.DIF file into the JSTARS database and the upload of information into the case file for a specific employee or contractor. This log remains valid until the case is deleted according to the records retention policy for the personnel security case.

2.0 Privacy Impact

The eDelivery process automates an existing manual process whereby OPM transfers information about individuals' background investigations. Thus, no new personally identifying information is being sent to DOJ with the eDelivery service. Additionally, the encrypted electronic transfer of information eliminates the possibility of the loss of paper copies in transit to DOJ from OPM.

Therefore, the eDelivery process has no adverse privacy impact.

APPROVAL SIGNATURE PAGE

/s/ 4/14/10

Nancy C. Libin
Chief Privacy and Civil Liberties Officer
Department of Justice

Date