The Bureau of the Fiscal Service

Privacy Impact Assessment

The mission of the Bureau of the Fiscal Service (Fiscal Service) is to promote the financial integrity and operational efficiency of the federal government through exceptional accounting, financing, collections, payments, and shared services.

This Privacy Impact Assessment is a Public document and will be made available to the general public via the Fiscal Service Privacy Impact Assessment (PIA) webpage (shown below).

Fiscal Service - Privacy Impact Assessments (PIA):
https://www.fiscal.treasury.gov/fsreports/rpt/fspia/fs_pia.htm

Name of System: Digital Signature Storage and Verification (DSSV)

Document Version: 1.1

Document Date: May 19, 2018

SYSTEM GENERAL INFORMATION:

1) System Overview: Describe the purpose of the system.
The Digital Signature and Storage Verification (DSSV) application stores the activation history of all current and former Federal Agency personnel with a designated and/or delegated status and it supports the first and most basic internal control in the Payment Management's payment systems – all payments must be certified by an active, properly designated Certifying Officer, whose "wet" signature is stored in DSSV.

DSSV reduces the administrative burden on Fiscal Service RFCs and agencies, streamlines the delegation and designation process, and enhances the integrity of the signature system underlying the disbursement process. Federal Agencies submit delegation/designation forms to Fiscal Service. The forms are scanned and stored in DSSV along with the 'wet' signature. A reference card is created for the individual that associates the delegation/designation forms, the 'wet' signature and any additional documentation related to the individual (e.g. renewal letters and CO training certificates).

The DSSV application will be used internally and is not interconnected to any other applications. While DSSV streamlines required signature verification, the business unit can operate uninterrupted in its absence.

2) Under which Privacy Act Systems of Records Notice (SORN) does the system operate? Provide number and name.
FMS .002 Payment Records

3) If the system is being modified, will the SORN require amendment or revision?
__yes, explain.
x_no

4) Does this system contain any personal information about individuals?
x__yes
__no

a. Is the information about members of the public? No

b. Is the information about employees or contractors? Yes

5) What legal authority authorizes the purchase or development of this system?
31 USC 3325 (a)(3)(d)- Vouchers
31 U.S.C. 3321

DATA in the SYSTEM:

1) **Identify the category of individuals in the system**
   Check all that apply:
   - **x_ Employees**
   - **x_ Contractors**
   - **__ Taxpayers**
   - **__ Others (describe)**

2) **Identify the sources of information in the system**
   Check all that apply:
   - **x_ Employee**
   - **__ Public**
   - **x_ Federal agencies**
   - **__ State and local agencies**
   - **__ Third party**

   a. What information will be collected from employees or contractors?
   Information required on Fiscal Service 210 Series Forms and Form 2958DO. Designee Name, Designee Agency Name, Designee Agency Address, Designee Agency Phone Number, Designation, Designee Agency Location Code, Designee Signature, Approving Official Name, Approving Official Title, Approving Official Signature.
   b. What information will be collected from the public? No information will be collected from the public.

   c. What Federal agencies are providing data for use in the system? Every Federal agency in the Executive Branch, except for most Department of Defense and certain independent agencies such as the U.S. Postal Service.

   d. What state and local agencies are providing data for use in the system? No state or local agencies are providing data for use in the system.

   e. From what other third party sources will data be collected? No data will be collected from other third party sources.

3) **Accuracy, Timeliness, and Reliability**

   a. How are data collected from sources, other than Fiscal Service records, verified for accuracy?
   The data in DSSV comes from the agencies and is verified by the agencies prior to being sent to the Fiscal Service. The data is entered into the system by one user and verified by another user. Head of Agency is verified against the Yellow Book to confirm their authority.

   b. How will data be checked for completeness?
   The data is entered in the DSSV system by one user and verified by another.

c. **What steps or procedures are taken to ensure the data is current?**
Designees are required to renew every two years. Unless notified by the Agency, it is assumed data is current.

d. **In what document(s) are the data elements described in detail?**
Treasury Financial Manual Volume 1 Part 4A Chapter 3000 describes the fields on the Fiscal Service Forms.

ATTRIBUTES OF THE DATA:

1) **How is the use of the data both relevant and necessary to the purpose for which the system is being designed?**
The data is necessary to identify and verify the signatures of Federal employees who are designated as Head of Agency, Delegating/Designating Officials, Certifying Officer, Designated Agent, and SPS Data Entry Operator.

2) **Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected? How will this be maintained and filed?**
No.

3) **Will the new data be placed in the individual's record?**
Not applicable. New data is not being derived from previously unavailable data about an individual.

4) **Can the system make determinations about employees or members of the public that would not be possible without the new data?**
Not applicable. New data is not being derived from previously unavailable data about an individual.

5) **How will the new data be verified for relevance and accuracy?**
Not applicable. New data is not being derived from previously unavailable data about an individual.

6) **If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?**
Data is not being consolidated.

7) **If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? (Explain)**
Processes are not being consolidated.

8) **How will the data be retrieved? (If personal identifiers are used to retrieve information on the individual, explain and list the identifiers that will be used to retrieve data.)**
Data will be retrieved by Designee Last Name, Designee First Name, and Designee Middle Initial.

9) **What kind of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?**

Aging reports and recertification letters are produced on the designees that calculate the period until the delegation or designation expires. The reports assist the system administrators in notifying the agencies that the delegation or designation requires renewal. The DSSV System Administrators have access to the reports.

10) **What opportunities do individuals have to decline to provide information (i.e., in such cases where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses)? How can individuals grant consent?**

The information in DSSV is required for individuals from agencies for which Fiscal Service provides disbursing functions. Agencies are required to inform Fiscal Service of the Head of the Agency, delegate designation authority to designating officials; and designate individuals to the positions of Certifying Officer for the Secure Payment System (SPS), International Treasury Services (ITS), and the Automated Standard Application for Payments (ASAP); and SPS Data Entry Operators (DEO) and designated agents. This information is closely held by Fiscal Service.

MAINTENANCE AND ADMINISTRATIVE CONTROLS:

1) **What are the retention periods of data in this system? How long will the reports produced be kept?**

- DSSV designation data is retained in the system for 2 months past the expiration of all designations for a reference card. The data is then archived through the aging process.
- The hard copy FS 210s, FS2958s, and completed recertification letters are maintained forever.
- The aging reports and recertification letters sent to Agencies will be retained for 7 years and then destroyed.

2) **What are the procedures for disposition of the data at the end of the retention period? Where are the disposition procedures documented?**

Any paper documentation is shredded.
Any electronic documentation is purged.

3) **If the system is operated in more than one site, how will consistent use of the system and data be maintained at all sites?**

DSSV is not operated in more than one site.

4) **Is the system using technologies in ways that Fiscal Service has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?**

DSSV is not using technology in ways that Fiscal Service has not previously employed.

5) **How does the use of this technology affect employee or public privacy?**

Not Applicable.

6) **Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.**

No.

7) **What kind of information is collected as a function of the monitoring of individuals?**
   Not Applicable.

8) **What controls will be used to prevent unauthorized monitoring?**
   Not Applicable.

ACCESS TO DATA:

1) **Who will have access to the data in the system?**
   Check all that apply:
   __ Contractors
   x_ Users
   __ Managers
   __ System Administrators
   __ System Developers
   x__ Others (explain)_ Fiscal Service Database Administrators

2) **How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?**
   Access is assigned to roles. Users are assigned roles by their supervisor, based on their job function. Criteria, procedures, and responsibilities are documented in the DSSV System Security Plan.

3) **Will users have access to all data on the system or will the user's access be restricted? Explain.**
   User access is defined and restricted by role based security. Users are assigned the level of access needed to perform job duties based on least privilege. Data interactions are written to a permanent, unalterable audit log.

4) **What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access? (Please list processes and training materials)**
   Audit reports will be reviewed weekly to prevent misuse of data.

5) **If contractors are/will be involved with the design, development or maintenance of the system, were Privacy Act contract clauses inserted in their contracts and were other regulatory measures addressed?**
   Not Applicable. Contractors are not involved.

6) **Do other systems share data or have access to the data in the system?**
   __yes
   x_no

   If yes,

   a. Explain the interface.

   b. Identify the role responsible for protecting the privacy rights of the public and employees affected by the interface.

7) Will other agencies share data or have access to the data in this system?

__yes
x_no

If yes,

a. Check all that apply:

__Federal
__State
__ Local
__Other (explain) _____

b. Explain how the data will be used by the other agencies.

c. Identify the role responsible for assuring proper use of the data.