

Civil Division



Privacy Impact Assessment for the Victims Compensation Fund Claims Infrastructure System

Issued by:
Jim Kovakas

Reviewed by: Luke J. McCormack, Chief Information Officer, Department of Justice

Approved by: Joo Y. Chung, Acting Chief Privacy and Civil Liberties Officer, Department of Justice

Date approved: September 28, 2012

Section 1: Description of the Information System

Provide a non-technical overall description of the system that addresses:

- (a) the purpose that the records and/or system are designed to serve;
- (b) the way the system operates to achieve the purpose(s);
- (c) the type of information collected, maintained, used, or disseminated by the system;
- (d) who has access to information in the system;
- (e) how information in the system is retrieved by the user;
- (f) how information is transmitted to and from the system; and
- (g) any interconnections with other systems.

The response should be written in plain language and should be as comprehensive as necessary to describe the system. If it would enhance the public's understanding of the system, please include system diagram(s).

On January 2, 2011, President Obama signed into law the James Zadroga 9/11 Health and Compensation Act of 2010 (Zadroga Act). Title II of the Zadroga Act reactivates the September 11th Victim Compensation Fund (VCF) of 2001 and requires Special Master, Sheila Birnbaum, recently appointed by the Attorney General, to provide compensation to any individual (or a personal representative of a deceased individual) who suffered physical harm or was killed as a result of the terrorist-related aircraft crashes of September 11, 2001, or the debris removal efforts that took place in the immediate aftermath of those crashes. Estimates for this program far surpass the previous effort with significant changes in eligibility opening up the program to many more claimants. Current estimates are that as many as 70,000 claims may be filed with an estimated 40,000 awards. The Department of Justice established the Victims Compensation Fund Claims Infrastructure Systems (VCFCIS) for the purpose of assisting the Department of Justice and the Special Master to meet the statutory requirements of the Zadroga Act in a comprehensive and cost-effective manner.

The VCFCIS is a secure web based Claims Management System to be available for use by the VCF Special Master and staff in order to process compensation claims under the Zadroga Act. Information in the VCFCIS is primarily obtained by individuals or their representatives who file electronic or paper claims for compensation under the Zadroga Act. Electronic claims can be submitted via a public-facing website located at www.vcf.gov, which is hosted at the Department of Justice's Justice Management Division's (JMD) Rockville data center. All external traffic from this website will be routed from JMD to the VCF databases that will be maintained by IBM, a Department contractor, at its fully accredited Federal Data Center. DOJ personnel, contracted personnel, and claimants will have access to the VCFCIS depending on their assigned roles and access privileges.

The purpose of the modification to this PIA is to further clarify and update certain sections of the PIA including: the description of the system; the source of information to file a claim; the internal transfer of information to the Special Masters Office; the external transfer to the U.S. Department of Treasury and National Institute for Occupational Safety and Health (NIOSH); and the notices provided

to and consents obtained from individuals when filing a claim for compensation.

Section 2: Information in the System

2.1 Indicate below what information is collected, maintained, or disseminated.

(Check all that apply.)

Identifying numbers					
Social Security	<input checked="" type="checkbox"/>	Alien Registration	<input type="checkbox"/>	Financial account	<input type="checkbox"/>
Taxpayer ID	<input type="checkbox"/>	Driver's license	<input type="checkbox"/>	Financial transaction	<input type="checkbox"/>
Employee ID	<input type="checkbox"/>	Passport	<input type="checkbox"/>	Patient ID	<input type="checkbox"/>
File/case ID	<input checked="" type="checkbox"/>	Credit card	<input type="checkbox"/>		<input type="checkbox"/>
Other identifying numbers (specify):					

General personal data					
Name	<input checked="" type="checkbox"/>	Date of birth	<input checked="" type="checkbox"/>	Religion	<input type="checkbox"/>
Maiden name	<input checked="" type="checkbox"/>	Place of birth	<input type="checkbox"/>	Financial info	<input type="checkbox"/>
Alias	<input type="checkbox"/>	Home address	<input checked="" type="checkbox"/>	Medical information	<input checked="" type="checkbox"/>
Gender	<input checked="" type="checkbox"/>	Telephone number	<input checked="" type="checkbox"/>	Military service	<input type="checkbox"/>
Age	<input checked="" type="checkbox"/>	Email address	<input checked="" type="checkbox"/>	Physical characteristics	<input type="checkbox"/>
Race/ethnicity	<input type="checkbox"/>	Education	<input type="checkbox"/>	Mother's maiden name	<input type="checkbox"/>
Other general personal data (specify):					

Work-related data					
Occupation	<input type="checkbox"/>	Telephone number	<input type="checkbox"/>	Salary	<input checked="" type="checkbox"/>
Job title	<input type="checkbox"/>	Email address	<input type="checkbox"/>	Work history	<input type="checkbox"/>
Work address	<input type="checkbox"/>	Business associates	<input type="checkbox"/>		<input type="checkbox"/>
Other work-related data (specify):					

Distinguishing features/Biometrics					
Fingerprints	<input type="checkbox"/>	Photos	<input type="checkbox"/>	DNA profiles	<input type="checkbox"/>
Palm prints	<input type="checkbox"/>	Scars, marks, tattoos	<input type="checkbox"/>	Retina/iris scans	<input type="checkbox"/>
Voice recording/signatures	<input type="checkbox"/>	Vascular scan	<input type="checkbox"/>	Dental profile	<input type="checkbox"/>
Other distinguishing features/biometrics (specify):					

Department of Justice Privacy Impact Assessment
 [Civil Division/Victims Compensation Fund
 Claims Infrastructure System]

System admin/audit data					
User ID	<input checked="" type="checkbox"/>	Date/time of access	<input checked="" type="checkbox"/>	ID files accessed	<input checked="" type="checkbox"/>
IP address	<input checked="" type="checkbox"/>	Queries run	<input checked="" type="checkbox"/>	Contents of files	
Other system/audit data (specify):					

Other information (specify)	

2.2 Indicate sources of the information in the system. (Check all that apply.)

Directly from individual about whom the information pertains					
In person	<input checked="" type="checkbox"/>	Hard copy: mail/fax	<input checked="" type="checkbox"/>	Online	<input checked="" type="checkbox"/>
Telephone	<input checked="" type="checkbox"/>	Email	<input checked="" type="checkbox"/>		
Other (specify): Attorneys and associated firms have the capability of submitting bulk applications via electronic format or paper form.					

Government sources					
Within the Component	<input checked="" type="checkbox"/>	Other DOJ components	<input checked="" type="checkbox"/>	Other federal entities	<input checked="" type="checkbox"/>
State, local, tribal		Foreign			
Other (specify):					

Non-government sources					
Members of the public	<input checked="" type="checkbox"/>	Public media, internet		Private sector	
Commercial data brokers					
Other (specify):					

2.3 Analysis: Now that you have identified the information collected and the sources of the information, please identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Please describe the choices that the component made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data,

include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

The process of collecting information directly from the claimant or their representative mitigates the risk of reliance on inaccurate information to determine eligibility of the compensation claim. In addition, the Department determined to collect only the personally identifiable information necessary to accurately identify the claimant and to determine eligibility of the VCF claim.

Section 3: Purpose and Use of the System

3.1 Indicate why the information in the system is being collected, maintained, or disseminated. (Check all that apply.)

Purpose			
<input type="checkbox"/>	For criminal law enforcement activities	<input checked="" type="checkbox"/>	For civil enforcement activities
<input type="checkbox"/>	For intelligence activities	<input checked="" type="checkbox"/>	For administrative matters
<input type="checkbox"/>	To conduct analysis concerning subjects of investigative or other interest	<input type="checkbox"/>	To promote information sharing initiatives
<input type="checkbox"/>	To conduct analysis to identify previously unknown areas of note, concern, or pattern.	<input type="checkbox"/>	For administering human resources programs
<input type="checkbox"/>	For litigation	<input type="checkbox"/>	
<input checked="" type="checkbox"/>	Other (specify): Personal information is being collected by the VCF system for analysis to determine the correct amount of compensation for each claimant.		

3.2 Analysis: Provide an explanation of how the component specifically will use the information to accomplish the checked purpose(s). Describe why the information that is collected, maintained, or disseminated is necessary to accomplish the checked purpose(s) and to further the component’s and/or the Department’s mission.

As stated above in Section I, the Civil Division will use the information in the VCFCIS to evaluate the eligibility for and amount of compensation under the Zadroga Act. The pertinent information is collected from each claimant or his/her representative to ensure that the information relied upon for evaluation of compensation eligibility is accurate and reliable.

3.3 Indicate the legal authorities, policies, or agreements that authorize collection of the information in the system. (Check all that apply and include citation/reference.)

Authority	Citation/Reference
------------------	---------------------------

X	Statute	Zadroga Act
	Executive Order	
	Federal Regulation	
	Memorandum of Understanding/agreement	
	Other (summarize and provide copy of relevant portion)	

3.4 Indicate how long the information will be retained to accomplish the intended purpose, and how it will be disposed of at the end of the retention period. (Reference the applicable retention schedule approved by the National Archives and Records Administration, if available.)

All information will be retained by IBM on DOJ’s behalf for six years. Thereafter, DOJ will assimilate the entire information system and retain the information for at least an additional 5 years. The information will be disposed of at the end of the retention period.

3.5 Analysis: Describe any potential threats to privacy as a result of the component’s use of the information, and controls that the component has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

The risks identified are the risk of unauthorized access to or use of VCF claimant personal information. In order to mitigate these risks, access to individual electronic case files will be limited to those authorized personnel who manage and have direct control over case file information. All VCF personnel, to include system administrators, have accepted the rules of behavior regarding the proper handling of DOJ computer systems and information. All VCF personnel will receive computer security training specific to DOJ or to IBM. In addition, the VCFCIS will be maintained in the FISMA-compliant IBM Federal Data Center. Further, to ensure accountability of the information maintained in the system, audit logs will be kept and checked at regular intervals.

Section 4: Information Sharing

4.1 Indicate with whom the component intends to share the information in the system and how the information will be shared, such as on a case-by-case basis, bulk transfer, or direct access.

	How information will be shared
--	--------------------------------

Department of Justice Privacy Impact Assessment
[Civil Division/Victims Compensation Fund
Claims Infrastructure System]

Recipient	Case- by-case	Bulk transfer	Direct access	Other (specify)
Within the component			X	Special Master's Office
DOJ components				
Federal entities	X	X		U.S Dept. of Treasury, NIOSH
State, local, tribal gov't entities				
Public				
Private sector			X	IBM
Foreign governments				
Foreign entities				
Other (specify):				

4.2 Analysis: Disclosure or sharing of information necessarily increases risks to privacy. Describe controls that the component has put into place in order to prevent or mitigate threats to privacy in connection with the disclosure of information. (For example: measures taken to reduce the risk of unauthorized disclosure, data breach, or receipt by an unauthorized recipient; terms in applicable MOUs, contracts, or agreements that address safeguards to be implemented by the recipient to ensure appropriate use of the information – training, access controls, and security measures; etc.)

Once a compensation decision has been reached for an individual claimant, and after approval from the Special Master's Office, Civil Division will use DOJ's Financial Management Information System (FMIS) to disburse payment determination to the U.S. Department of Treasury. The transfer of information will be a manual process initiated by the Special Master and transferred to DOJ Civil for input into FMIS. All decisions are to be based upon the information stored within VCFIS and act as the final record. Information contained in the transmission will be limited to only those portions of PII required by FMIS to initiate the transfer of funds from Treasury.

Data transfer (name, address, social security number, date of birth, and medical condition) to National Institute for Occupational Safety and Health (NIOSH) is performed so that verification of the medical certificates is done before compensation. The transfer takes place through DOJ's MyFX tool, a secure web site that DOJ designed specifically for transferring files outside of the Department.

Section 5: Notice, Consent, and Redress

5.1 Indicate whether individuals will be notified if their information is collected, maintained, or disseminated by the system. (Check all that apply.)

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 7.
---	--

Department of Justice Privacy Impact Assessment
 [Civil Division/Victims Compensation Fund
 Claims Infrastructure System]

<input checked="" type="checkbox"/>	Yes, notice is provided by other means.	Specify how: Claimants will be notified via the claimant web site upon entrance. The notice specifies the purpose of the collection of information and a specific checkbox alongside the user login will be employed to record the claimant's consent to the disclosures of information maintained in the system.
<input type="checkbox"/>	No, notice is not provided.	Specify why not:

5.2 Indicate whether and how individuals have the opportunity to decline to provide information.

<input checked="" type="checkbox"/>	Yes, individuals have the opportunity to decline to provide information.	Specify how: All information within the VCF system is provided on a voluntary basis, either directly by the claimant or by their authorized representative. Individuals are notified of the purpose of the collection of the information and the effects of not providing the information.
<input type="checkbox"/>	No, individuals do not have the opportunity to decline to provide information.	Specify why not:

5.3 Indicate whether and how individuals have the opportunity to consent to particular uses of the information.

<input checked="" type="checkbox"/>	Yes, individuals have an opportunity to consent to particular uses of the information.	Specify how: All information within the VCF system is provided on a voluntary basis, either directly by the claimant or by their authorized representative. A specific checkbox alongside the user login will be employed to record the individual's consent to the disclosures of information maintained in the system.
<input type="checkbox"/>	No, individuals do not have the opportunity to consent to particular uses of the information.	Specify why not:

5.4 Analysis: Clear and conspicuous notice and the opportunity to consent to the collection and use of individuals' information provides transparency and allows individuals to understand how their information will be handled.

Describe how notice for the system was crafted with these principles in mind, or if notice is not provided, explain why not. If individuals are not provided the opportunity to consent to collection or use of the information, explain why not.

[All information within the VCFCIS system is provided on a voluntary basis, either directly by the claimant or by their authorized representative. Claimants are provided with notice of the purpose of the collection of information when they create an account to file a claim under the Zadroga Act. In addition, a specific checkbox alongside the user login will be employed to record the individual's consent to the disclosures of information that may be made for the purpose of determining qualification for and/or compensation of a claim under the Zadroga Act.]

Section 6: Information Security

6.1 Indicate all that apply.

X	A security risk assessment has been conducted.
X	Appropriate security controls have been identified and implemented to protect against risks identified in security risk assessment. Specify: Risk assessment completed 02/16/2012.
X	Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify: JMD and Civil evaluation completed on 01/27/2012. Civil re-evaluation for additional functionality completed 2/16/2012.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Certification and Accreditation: January 27, 2012.
X	Auditing procedures are in place to ensure compliance with security standards. Specify, including any auditing of role-based access and measures to prevent misuse of information: The DOJ and IBM FDC each have developed and approved Audit and Accountability Policies and Procedures that address purpose, scope, management commitment and compliance. All approved policies, procedures, standards and program plans fully meet the requirements of FISMA.
X	Contractors that have access to the system are subject to provisions in their contract binding them under the Privacy Act.
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOJ policy.
X	The following training is required for authorized users to access or receive information in the system:
X	General information security training
X	Training specific to the system for authorized users within the Department.
X	Training specific to the system for authorized users outside of the component.
	Other (specify):

6.2 Describe how access and security controls were utilized to protect privacy and

reduce the risk of unauthorized access and disclosure.

All policies, procedures, standards and program plans for the VCFCIS fully meet the security policies and requirements of the Department of Justice and the Federal Information Security Management Act. Relevant procedural documents are created when needed. DOJ defines the frequency of reviews and updates for security documents (at least annually), certification and accreditation (C&A) of systems (at least every three years) and internal control reviews (ICR) (at least annually).

Section 7: Privacy Act

7.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. (Check the applicable block below and add the supplementary information requested.)

<input checked="" type="checkbox"/>	Yes, and this system is covered by an existing system of records notice. Provide the system name and number, as well as the Federal Register citation(s) for the most recent complete notice and any subsequent notices reflecting amendment to the system: September 11 th Victim Compensation Fund of 2001 File System, Civ-008, 66 Fed. Reg. 65,991 (Dec. 21, 2001), modified on (Jan. 31, 2001 and Jan. 25, 2007).
<input type="checkbox"/>	Yes, and a system of records notice is in development.
<input type="checkbox"/>	No, a system of records is not being created.

7.2 Analysis: Describe how information in the system about United States citizens and/or lawfully admitted permanent resident aliens is or will be retrieved.

Information about individual claimants can be retrieved via any of multiple points of information that they have provided, along with a claimant ID number that will be generated upon submission. Searches would be accomplished by authorized personnel using such factors as SSN, first name, last name, claimant ID, address, date of birth, and location.