Civil Division

Privacy Impact Assessment
for the
Victims Compensation Fund Claims Infrastructure System

Issued by:
Jim Kovakas

Reviewed by: Eric Olson, Chief Information Officer, Department of Justice

Approved by: Nancy C. Libin, Chief Privacy and Civil Liberties Officer, Department of Justice

Date approved: September 29, 2011

(February 2011 DOJ PIA Form)

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 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 purpose of the Victims Compensation Fund Claims Infrastructure Systems (VCFCIS) is to assist the Special Master and the Department of Justice 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 Victim Compensation Fund Special Master, and staff.

USIS|Labat will create, manage and supply data to the VCFCMS database, which is being housed in IBM's FISMA-compliant, Federal Data Center facility in Boulder, CO. The public facing website (www.VCF.GOV) will be held at JMD's Rockville data center. All external traffic will be routed from JMD to the VCF databases being hosted by IBM at the Federal Data Center. DOJ personnel, contracted personnel (USIS|Labat, IBM and medical specialists contracted by IBM), and claimants will have access to the VCF system with different roles and access privileges. Information within the system is accessed via the external web site www.VCF.GOV, and an encrypted tunnel between DOJ JMD and IBM(for internal users).

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	X	Alien Registration		Financial account	
Taxpayer ID		Driver's license		Financial transaction	
Employee ID		Passport		Patient ID	
File/case ID	X	Credit card			
Other identifying numbers (specify):					

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

Work-related data					
Occupation		Telephone number		Salary	X
Job title		Email address		Work history	
Work address		Business associates			
Other work-related data (specify):					

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

System admin/audit data					
User ID	X	Date/time of access	X	ID files accessed	X
IP address	X	Queries run	X	Contents of files	

System admin/audit data
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	X	Hard copy: mail/fax	X	Online	X
Telephone	X	Email	X		
Other (specify):					

Government sources					
Within the Component	X	Other DOJ components	X	Other federal entities	
State, local, tribal		Foreign			
Other (specify):					

Non-government sources					
Members of the public	X	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 risks identified are the risk of unauthorized access to or use of VCF claimant personal information.

The VCF will be hosted in the FISMA-compliant IBM Federal Data Center. 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. To mitigate risks of unauthorized access, audit logs will be kept and checked at regular intervals.

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			
	For criminal law enforcement activities	X	For civil enforcement activities
	For intelligence activities	X	For administrative matters
	To conduct analysis concerning subjects of investigative or other interest		To promote information sharing initiatives
	To conduct analysis to identify previously unknown areas of note, concern, or pattern.		For administering human resources programs
	For litigation		
X	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.

The Component will use the information checked above to evaluate the need for compensation under the Zadroga Act. The pertinent information is collected from each claimant to ensure that the evaluation of compensation need is thorough and fair.

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
	Statute	
X	Executive Order	Zadroga Act
	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.

The VCF will be hosted in the FISMA-compliant IBM Federal Data Center. 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. To mitigate risks of unauthorized access, 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.

Recipient	How information will be shared			
	Case-by-case	Bulk transfer	Direct access	Other (specify)
Within the component				
DOJ components				
Federal entities	X			U.S Dept. of Treasury
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.)

Civil Division will be using the FMIS system to disburse payment determination to the U.S. Department of Treasury on a case by case basis. 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. The transfer of information will be a manual process initiated by the Special Master and transferred to DoJ Civil for input into FMIS.

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.

X	Yes, notice is provided by other means.	Specify how: Individuals will be notified via the claimant web site upon entrance.
	No, notice is not provided.	Specify why not:

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

X	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.
	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.

	Yes, individuals have an opportunity to consent to particular uses of the information.	Specify how:
X	No, individuals do not have the opportunity to consent to particular uses of the information.	Specify why not: All information within the VCF system is provided on a voluntary basis, either directly by the claimant or by their authorized representative.

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 VCF system is provided on a voluntary basis, either directly by the claimant or by their authorized representative. Notices are posted on the primary pages regarding usage and access to a government system, as well as privacy procedures.

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 is currently underway.	
X	Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify: JMD is currently testing and evaluating the VCF application.	
	The information is secured in accordance with FISMA requirements. Provide date of most recent Certification and Accreditation: Currently underway	
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 approved policies, procedures, standards and program plans fully meet the security policies and requirements of the Department of Justice and FISMA. 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.)

X	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: 66 FR 65991
	Yes, and a system of records notice is in development.
	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 any individual claimant 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. Although the system has not been fully realized at this time, searches should be accomplished using such factors as SSN, first name, last name, claimant ID, address, date of birth, location.