Civil Division

Privacy Impact Assessment
for the
[September 11th Victim Compensation Fund]

Issued by:
[Allison Stanton]

Approved by: Peter A. Winn, Acting Chief Privacy and Civil Liberties Officer, Department of Justice

Date approved: September 24, 2018

EXECUTIVE SUMMARY

The September 11th Victim Compensation Fund (VCF) Claims Management System (CMS) and additional tools support the fund in the following ways:

- Online form submission;
- Document upload and review;
- Claim review;
- Payment package preparation and review;
- Eligibility and Compensation decisions;
- Amending and updating claims;
- Correspondence;
- Hard copy document ingest;
- External data collection; and
- Internal data export.

The purpose of the modification to this Privacy Impact Assessment (PIA) is to clarify and update the PIA to account for:

- Changes to the Fund after reauthorization in December 2015;
- External sources of data; and
- Tools outside of CMS.

Section 1: Description of the Information System

[On January 2, 2011, President Obama signed into law the James Zadroga 9/11 Health and Compensation Act of 2010 (Pub. L. 111-347) ("Zadroga Act"). Title II of the Zadroga Act reactivated the September 11th Victim Compensation Fund ("VCF" or "Fund") of 2001, and expanded eligibility for 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.

On December 18, 2015, President Obama signed into law a bill reauthorizing the Zadroga Act, which included the reauthorization of the VCF. The reauthorization extended the VCF for five years and included important changes to the VCF's policies and procedures for evaluating claims and calculating each claimant's loss. The new deadline to file claims is December 18, 2020, and the VCF will remain in operation for the time period required to complete all claims and properly close down the operation.

The Department of Justice (DOJ) established the VCF CMS 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. CMS consists of two secure web-based portals (one internal, one public-facing) which support claims submission and processing. CMS is hosted by IBM, a contractor to the VCF, at the Smart Cloud for Government Federal Data Center (FDC), which is FedRAMP certified, as discussed below. IBM operates, maintains, and administers the entire Claims Management System in support of the VCF program. The Rational Team Concert system is also hosted at the FDC. This system is the CMS production support ticket tracking. The individual tickets include VCF numbers at VCF's request to provide faster triage, assessment and resolution of tickets to meet business needs.

Information in CMS is primarily obtained from individuals or their representatives who file electronic or paper claims for compensation under the Zadroga Act. Additional information is received from external sources, including the National Institute for Occupational Safety and Health (NIOSH), private physicians, the New York City Police Department (NYPD), the Fire Department of the City of New York (FDNY), the Social Security Administration (SSA), Public Safety Officers' Benefits (PSOB) program and Consolidated Edison (ConEd). DOJ personnel, contracted personnel, and claimants have access to CMS depending on their assigned roles and access privileges through the portals and through system-generated reports. Information can be transmitted to and from the system through the user interface, system-generated reports, and automated ingests and exports. CMS is a stand-alone system and a major application maintained by IBM.

In addition to CMS, the VCF leverages the tools built and maintained by PAE-Labat, a contractor to the VCF, who provides these tools to support the administrative processing functions for VCF. The tools control and manage these functions with data stored in a common Structured Query Language (SQL) database. The VCF tools receive data extracted from CMS; the extracted data is manipulated and then ingested by the tools. The tools include the following:

- Archive/Box Tracking – tracks claim number and location where the claim file is stored (i.e. the identifier and the date archived) when the claim's hard copy data is sent to the archiving facility.
- Authorized Users table editor – supports account management / access management for some of the VCF tools based on Justice Consolidated Office Network (JCON) account.
- Automated Clearing House (ACH) – database which contains bank account information for law firms who are paid on behalf of their claimants.
- Batch Process – compiles Portable Document Format (PDF) copies of all correspondence generated by the Fund, generates eXtensible Markup Language (XML) for ingest of correspondence (maintained as PDFs) and related metadata (XML), to CMS, and posts data to the SQL database.
- Claim Look Up – presents a read-only, dashboard-like view of the claim to facilitate claim review and generates emails and calendar reminders to VCF users using data from CMS, the Mail Intake tool, settlement and workers compensation data, third party data, the Data Discrepancy tool, and the Fraud database.
- Congressional Inquiry – tracks inquiries received from Congress, including claim number, victim name, and status.
- Correspondence – uses logic and inputs from CMS and users to generate letters, which are

then printed and mailed to claimants, their representatives, and/or their attorneys; these letters are also exported and uploaded to CMS in PDF format.

- Data Discrepancy – tracks hard copy documents that contain a data discrepancy requiring investigation and resolution of the discrepancy with notes.
- Federal Bureau of Investigation (FBI) Batch Receive – ingests data received from the FBI regarding claimants.
- FBI Send – normalizes the data exported from CMS to send to the FBI.
- Fraud – tracks claims (claim number, victim name, date of birth, notes, dates sent to and received from the Office of the Inspector General (OIG)) with a potential for fraudulent activity which are either sent to the OIG for investigation or are pre-review and are flagged for later investigation.
- Generic Table Editor – allows edit of data in tables in SQL database for VCF Tools.
- Intake Tables editor – supports management functions for the Intake team, including editing and deleting data in the Mail Intake tool, marking a claim as expedited for the Intake team, controlling the document types list, and reporting and querying.
- Loss Calculation – reference database which contains Quality Review assessment information for claims prior to the distinction between Group A and Group B (as required by the December 2015 reauthorization statute); this database is no longer updated and has been replaced by the Quality Review tool.
- Mail Intake / Mass Mailing List (MML) – tracks all scanned hard copy documents with metadata which includes type, victim name, social security number, representative, source, and unique identifier (which is not the same as the VCF claim number).
- Payment – partially developed application which will house data to calculate payments and produce payment documents, will retain a history of payments made, and will include audit logging.
- Payment Form – Excel form which compiles data from the ACH database (via SQL server database), CMS, and user entry, and generates an exportable form which is provided to the Office of Budget, Planning, and Evaluation (OPBE) to request processing of a payment on a claim.
- Private Physician – supports private physician data verification workflow, and contains data regarding private physician-diagnosed conditions for claims, as well as data sent to and received from the World Trade Center Health Program (WTCHP) in verification of the private physician data.
- Quality Review – supports Quality Review assessment for Group A and Group B claims and contains assessment results.
- SQL query – supports technical management, administration, and testing functions for the VCF tools.
- SSA Exhibit1 Entry – compiles data from the Mail Intake tool; exports data which is sent to the SSA; stores data on past exports to the SSA, including claim number, name, send date, and notes; imports SSA data and converts it into a format for the Generic Import ingest to CMS.
- Standardized Attorney List – tracks updates to the standardized attorney list (including primary attorney name, law firm name, and law firm address) and exports an email request

to make updates to the standardized attorney list in CMS.

The VCF Tools use source data from CMS, the FBI, SSA, private physicians, NIOSH WTCHP, OPBE, public mail, other third parties, claimants (or their legal representatives), and VCF users. Some of the VCF Tools generate exports of data which are sent to the public (including claimants, their representatives, attorneys, and third parties), CMS, NIOSH WTCHP, and the FBI; other tools manipulate data, display data, allow entry of data, or otherwise support the claim review and decision-making workflow. The VCF Tools are accessed by internal members of the Fund only. These members access the data through Excel tools and Access databases which are posted to folders on drives maintained by the Office of Litigation Support (OLS). Access is controlled via network drive access controls (administered by OLS) and, for some of the VCF Tools, also via the Authorized Users tool. Data enters the VCF Tools through user entry and ingests of files from third parties external to the VCF. External parties with whom the VCF exchanges data are listed later in this document. Data leaves the VCF Tools in the form of spreadsheets, PDFs, and XML files. The VCF Tools and supporting databases do not connect directly to other systems, but some of the VCF Tools connect to each other or to a shared SQL database.]

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

(Check all that apply.)

Identifying numbers					
Social Security	[X]	Alien Registration	[]	Financial account	[X]
Taxpayer ID	[X]	Driver's license	[]	Financial transaction	[]
Employee ID	[]	Passport	[X]	Patient ID	[]
File/case ID	[X]	Credit card	[]		
Other identifying numbers (specify): [National ID, if any, as assigned by country of origin, WTCHP Member ID]					

General personal data					
Name	[X]	Date of birth	[X]	Religion	[]
Maiden name	[X]	Place of birth	[X]	Financial info	[X]
Alias	[X]	Home address	[X]	Medical information	[X]
Gender	[X]	Telephone number	[X]	Military service	[X]
Age	[X]	Email address	[X]	Physical characteristics	[X]
Race/ethnicity	[]	Education	[]	Mother's maiden name	[]
Other general personal data (specify): [Names and information of familial relationships for purposes of filing a claim on behalf of a deceased individual.]					

Work-related data					
Occupation	[X]	Telephone number	[X]	Salary	[X]

Work-related data					
Job title	[X]	Email address	[X]	Work history	[X]
Work address	[X]	Business associates	[]		
Other work-related data (specify): [Employment status (e.g. retired, contractor, current employee).]					

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]): Some of the features may be included in medical records submitted by the claimant. Photographs are submitted by some claimants to establish proof of presence at a covered site.]					

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	[X]
Other system/audit data (specify): [The CMS record audit databases capture changes to many fields in both CMS databases.]					

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	[X]
State, local, tribal	[X]	Foreign	[X]		
Other (specify): [ ]					

Non-government sources					
Members of the public	[X]	Public media, internet	[]	Private sector	[X]
Commercial data brokers	[]				

Non-government sources
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, or another authorized third party filing on the claimant's behalf (e.g., family member), mitigates the risk of reliance on inaccurate information to determine eligibility of the compensation claim. Collecting from such sources also reduces the risk of fraud and decreases the burden placed on the claimant when filing a claim (if the information is provided directly to the VCF by the third party). In addition, the VCF collects only the personally identifiable, medical, and financial information necessary to accurately identify the claimant, to determine eligibility, to identify the correct amount of compensation, and to process payment of compensation for the VCF claim. Data is collected from external sources only when independent validation is needed that the information provided is accurate (e.g. medical or presence information). In the new claim form released after the reauthorization of the VCF in December 2015, the VCF decided to collect less data from claimants based on experience reviewing and deciding claims in the past few years. Since revising its claim form, VCF no longer collects data regarding when the claimant first sought treatment for their claimed condition(s) or the WTC Health Program site providing medical treatment for the claimant.]

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	☒	For civil enforcement activities
□	For intelligence activities	☒	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 eligibility and the correct amount of compensation for each claimant, to process claims for compensation, and to handle related administrative and management functions.

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 VCF will use the information collected to evaluate eligibility, determine the amount of compensation, and support payment of compensation under the Zadroga Act. The pertinent information is collected from each claimant, his/her representative, or external sources, to ensure that the information relied upon for evaluation of compensation eligibility and preparation of payment forms 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 Reauthorization Statute H.R. 2029—759 • Air Transportation Safety and System Stabilization Act, Pub. L. No. 107-42 (2001). • James Zadroga 9/11 Health and Compensation Act of 2010, Pub. L. No. 111-347 (2011).
[X]	Executive Order	• Exec. Order No. 12,866, 58 Fed. Reg. 51,735 (Oct. 4, 1993). • Exec. Order No. 13,563, 76 Fed. Reg. 3,821 (Jan. 21, 2011).

[X]	Federal Regulation	- James Zadroga 9/11 Victim Compensation Fund Reauthorization Act Interim Final Rule: ID: DOJ-LA-2016-0021-0001, RIN:1105-AB49, CFR: 28 CFR Part 104, Federal Register Number: 2016-21216 - Final Rule: Federal Register /Vol. 81, No. 171 / Friday, September 2, 2016 /Rules and Regulations 60617, DEPARTMENT OF JUSTICE, 28 CFR Part 104, [Docket No. CIV 151], RIN 1105–AB49, James Zadroga 9/11 Victim Compensation Fund Reauthorization Act - Final Rule: Federal Register / Vol. 76, No. 169 / Wednesday, August 31, 2011 / Rules and Regulations 54112, DEPARTMENT OF JUSTICE, 28 CFR Part 104, [Docket No. CIV 151], RIN 1105–AB39, James Zadroga 9/11 Health and Compensation Act of 2010
[X]	Memorandum of Understanding/agreement	See descriptions below in Section 4.
□	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.)

The records retention schedule approved by the National Archives and Records Administration (NARA) is DAA-0060-2012-0020.

CMS: Operationally, IBM will retain all information contained in CMS on DOJ's behalf for six years after the end of the program. Thereafter, DOJ will assimilate the entire information system and retain the information for seven years after the cut off, the end of the program. At that time, VCF will transfer the CMS data to NARA and the information will be retained as a permanent record.

VCF tools: All information will be retained by PAE-Labat as stored on OLS drives until the end of the program. Seven years after the cut off, the end of the program, VCF will transfer the data to NARA and the information will be retained as a permanent record.

Note: Both CMS and the VCF Tools are live systems, which means that the state of data at any point in time is subject to change based on additions, modifications, and deletions to data. When the systems are no longer in use, the data will reflect the last actions taken.

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 risks of unauthorized access to, misuse of, or misappropriation of VCF claimant personal information.

Program-level: All VCF personnel, including 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 on a yearly basis. Additionally, all VCF personnel are required to maintain appropriate security clearances with DOJ in order to receive access to any VCF systems. IBM contractors also take annual data security and privacy training offered by IBM, and PAE-Labat contractors take annual security training offered by PAE-Labat. In addition, the Civil Division offers privacy and security training specific to the VCF program and the type of information it maintains.

CMS: In order to mitigate these risks, access to individual electronic case files are limited to those authorized personnel who manage and have direct control over case file information. On the internal Admin portal, only cleared VCF personnel can access data. On the external Claimant portal, only claimants and their designees (law firm users, etc.), as well as designated VCF internal users, can access the claim. In addition, CMS is maintained in the Federal Information Security Modernization Act (FISMA)-compliant IBM FDC, which has received FedRAMP certification as discussed below. Further, to ensure accountability of the information maintained in the system, audit logs are kept and checked at regular intervals.

VCF tools: OLS network folder permissions and the access controls inherent in JCON workstations are used to control access to VCF tools. Tools are only provided to users based on team role, as determined by the team manager. Additionally, the tools and databases are protected by the security implemented by OLS and JCON on drives and workstations. In certain cases, in certain tools, usernames and date stamps are logged for certain actions taken in the tool.]

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	[]	[X]	[X]	[ ]
DOJ components	[]	[X]	[X]	[ ]
Federal entities	[X]	[X]	[X]	[ ]

Recipient	How information will be shared			
	Case-by-case	Bulk transfer	Direct access	Other (specify)
State, local, tribal gov't entities	[X]	[X]	☐	[ ]
Public	[X]	[ ]	[X]	[Claimants/law firms have direct access to their own claims]
Private sector	☐	☐	[X]	[IBM (Contractor)]
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.)

[Entities within the DOJ:

The Fund discloses or shares information with the following entities within the DOJ: Federal Bureau of Investigation (FBI), Office of the Inspector General (OIG), the Civil Division's Office of Planning Budget Execution (OPBE), and the Public Safety Officers' Benefits (PSOB) Program. VCF exchanges data with the FBI to perform a limited background review of the claimant as required by the statute. In response to audits, VCF shares requested data with the DOJ's OIG. VCF also exchanges data with the Civil Division's Office of Planning Budget and Execution, which facilitates financial transactions on behalf of VCF. In order to calculate any award offset by prior or current PSOB awards, the VCF exchanges data with that organization.

Each of these entities receives annual DOJ training regarding safety and security of data. Additionally, some of these entities have access to the data within DOJ systems (internal email and/or the Justice Enterprise File Sharing (JEFS) service), and are subject to the security thereof. JEFS is a Department-approved secure file sharing system that allows users to share sensitive files with authorized personnel within the Department or other approved outside users. The information is only maintained for 60 days and is encrypted in transit and at rest.

Entities external to the DOJ:

VCF exchanges data with the following external entities: claimants and law firms, Consolidated Edison, FDNY, New York National Guard, NYPD, NIOSH, New York City Employee Retirement System, United States Congress, WTC Health Registry, and the WTC Volunteer Fund. DOJ personnel only exchange specific data needed by these entities for administration and management of the VCF program.

Most data provided to or received from external entities is provided or received via Box.net (JEFS), which is the secure file transfer method endorsed by DOJ. Files posted to JEFS are only retained for 60 days. Members of the external entities who provide or receive the data are provided with access to only the folder(s) within JEFS relevant to their work with VCF and must use a secure username and password to access the system. In some cases, data is provided to, or received from, external entities via email with or without file passwords and/or encryption, depending on the exchange. DOJ personnel only transmit sensitive data—data that, if lost or accessed without authorization could result in substantial harm to an individual—by email when the email is encrypted or redacted for any mitigation otherwise appropriately secured.

Additionally, the VCF sends decision-related and other information in the form of hard-copy correspondence to claimants and their designees (which can include representatives and law firms). Letters are mailed only to the parties designated by the claimant and only with proper authorizations on file.

In addition to these protections, other protections apply in particular instances. For data exchanges with FDNY and NYPD VCF created a MOU to exchange data using JEFS to confirm presence and other information related to the claim.

For the purpose of exchanging information regarding a patient's conditions, VCF has MOUs with four entities within NIOSH – the WTCHP, private physicians, Discrepancies, and Inquiries. The purpose of the MOUs is to facilitate the data exchange to verify a patient's condition and treatment, clarify data where there is a discrepancy, and answer clarification inquiries from NIOSH.

To calculate compensation, VCF signed a MOU with the New York City Employee Retirement System (NYCERS). However, for the past year, this information has been collected directly from claimants instead of from NYCERS, as NYCERS suspended the data exchange due to resource constraints.

For communication with United States Congress Members or the Office of Legislative Affairs VCF ensures that the required claimant release forms are signed before sharing information about an individual claim file.

In order to confirm a victim's presence at a site, VCF created a MOU to exchange data using encrypted email files with WTC Health Registry. In addition, a data exchange with the WTC Volunteer fund is planned, but not yet begun.

To avoid releasing personally identifiable information beyond the described purposes, VCF redacts information as needed and/or limits information when sharing with other entities. For example, for those entities where information is exchanged through spreadsheets, such as FDNY and NIOSH, the VCF worked with each respective entity to define the minimum data needed in order to accomplish the goals of the data exchange. Templates were then established for each entity and only the agreed-upon data is included in the exchange.

Bulk Transfer of Data:

VCF provides bulk transfers of data to the SSA, FBI, NIOSH, FDNY, NYPD, and similar organizations when VCF requests documentation from these outside entities and in accordance with our established information sharing agreements. The bulk transfer of data is limited to the information those agencies require in order for them to efficiently provide VCF with substantive information about claimants as described above. The information exchanged in bulk is limited by the other agency's need to know in order to facilitate the processing of claims.]

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: [Privacy Act notice under 5 U.S.C. 552a(e)(3).]
[ ]	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: [Users are provided with a Privacy Act notice and other notices prior to official submission of the claim form online, before the registration page, and at the mandatory signature page for the form. Users can choose to decline to provide their information, or to rescind their submitted form, at any time. Note that rescinding information results in a claim status change and no further progress on the claim, but the previously submitted claim data will still be present in the CMS application.]
[ ]	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.

[X]	Yes, individuals have an opportunity to consent to particular uses of the information.	Specify how: [Individuals have an opportunity to consent to the use of their information prior to the official submission of the form. In addition to the privacy policy on the VCF homepage, the next portal update will include additional notice prior to the registration page.]
[]	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.

[The current notices in the system provide the Privacy Act notice text and request consent from the user for the VCF to use their information for the purposes of determining eligibility for compensation, and total compensation, and for the VCF to provide the information to other government entities in pursuit of information needed for the purposes of determining eligibility for compensation, and calculating awards. The notices are presented to the user at the beginning of the online claim form process as well as at the end of the process before submitting the form and providing a signature.]

Section 6: Information Security

6.1 Indicate all that apply.

[X]	The information is secured in accordance with FISMA requirements. Provide date of most recent Certification and Accreditation: [VCF CMS: 3/16/2018 VCF Infrastructure Systems (i.e. infrastructure on which CMS is hosted): 1/23/2018 OLS Servers (i.e. servers on which VCF tools are hosted): 11/24/2017 IBM Smart Cloud for Government (i.e. Federal Risk and Authorization Management Program (FedRAMP)-certified cloud infrastructure, on which CMS is hosted): 8/15/2016 VCF Tools - VCF Tools are hosted and executed within another DOJ information system: OLS Servers Systems, which has a distinct Authority To Operate, risk assessment, and security procedures.] If Certification and Accreditation has not been completed, but is underway, provide status or expected completion date: [N/A]

[X]	A security risk assessment has been conducted. [VCF CMS: 3/16/2018 VCF Infrastructure Systems (i.e. infrastructure on which CMS is hosted): 1/23/2018 OLS Servers (i.e. servers on which VCF tools are hosted): 12/1/2014 IBM Smart Cloud for Government (i.e. FedRAMP-certified cloud infrastructure, on which CMS is hosted): 8/15/2016 VCF Tools are hosted and executed within another DOJ information system: OLS Servers Systems, which has a distinct Authority To Operate, risk assessment, and security procedures.]	
[X]	Appropriate security controls have been identified and implemented to protect against risks identified in security risk assessment. Specify: [CMS: Security controls have been identified and implemented pursuant to FISMA, which complies with NIST 800-53 Rev. 4 requirements and associated controls. VCF Tools: VCF Tools are hosted and executed within another DOJ information system: OLS Servers Systems, which has a distinct Authority To Operate, risk assessment, and security procedures.]	
[X]	Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify: [CMS: The following types of monitoring, testing, and evaluation are undertaken: functional system testing, user acceptance testing, application security scanning, database security scanning, infrastructure security scanning, and regular security assessments according to a schedule set by DOJ. VCF Tools: Functional system testing is undertaken to ensure the tools behave according to requirements. Monitoring, testing and auditing of the tools are performed within the OLS Servers Systems environment.]	
[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: [CMS: Auditing procedures are in place; the record audit databases capture changes to many fields in the database, and account management/role-based audit logs are reviewed on a weekly basis. Additionally, role-based access is in place and rules in the applications prevent misuse of information by role, ownership, etc. VCF Tools: Access restrictions are in place and auditing is taking place via enhanced monitoring within the OLS Servers Systems environment.]	
[X]	Contractors that have access to the system are subject to provisions in their contract binding them under the Privacy Act.[Yes]	
[X]	Contractors that have access to the system are subject to information security provisions in their contracts required by DOJ policy.[Yes]	
[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.
	[X]	Other (specify): [Provide training and "tip sheets" to law firms when there is a significant change to CMS and the claimant portal that are available on the "Information for Law Firms" page on the VCF website.]

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

and reduce the risk of unauthorized access and disclosure.

In general, VCF's systems are maintained in physically secure environments. Physical security controls include secured entrances and security officers who limit access to the building where the servers are located. To access the systems, the Civil Division enforces Department standards for accessing a network system, such as Personal Identity Verification (PIV) card entry.

CMS: In order to mitigate these risks, access to individual electronic case files are limited to those authorized personnel who manage and have direct control over case file information. On the internal administrative portal, only authorized VCF personnel can access data. On the external Claimant portal, only claimants and their designees (law firm users, etc.), as well as VCF internal users, can access the claim. In addition, CMS is maintained in the FISMA-compliant IBM FDC. Further, to ensure accountability of the information maintained in the system, application audit logs are kept and checked at regular intervals.

VCF tools: OLS network folder permissions, account management access controls, and the access controls inherent in JCON workstations are used to control access to VCF tools. Additionally, the tools and databases are protected by the security implemented by OLS and JCON on drives and workstations. In certain cases, in certain tools, usernames and date/time stamps are logged for certain actions taken in the tool.

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)

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: Justice/CIV-008, "September 11th Victim Compensation Fund of 2001 File System," 66 Fed. Reg. 65,991 (Dec. 21, 2001).
□	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.

The September 11th Victim Compensation Fund of 2001 File System is a system of records, CIV-008 "September 11th Victim Compensation Fund of 2001 File System," established to support the administration of the program to compensate individuals who were physically injured or the personal representatives of those who were killed as a result of the terrorist-related aircraft crashes of September 11, 2001. Information regarding a United States citizen or lawfully admitted permanent resident alien is retrieved in the same manner regardless of citizenship or immigration status. The data can be retrieved from the system using personal identifiers such as name or claim number.]