The Office on Violence Against Women

Privacy Impact Assessment
for the
Peer Reviewer Database

Issued by:
Cathy Poston and Marnie Shiels,
Attorney Advisors,
Co-Senior Component Officials for Privacy (co-SCOP)

Approved by: Erika Brown Lee, Chief Privacy and Civil Liberties Officer, Department of Justice

Date approved: [April 29, 2014]

Section 1: Description of the Information System

The Peer Reviewer Database (Database) is a system that allows the Office on Violence Against Women (OVW) to select individuals to serve as grant application reviewers during the peer review process in connection with OVW's annual administration of grant awards. Lockheed Martin (LM), an outside contractor, maintains the database for OVW.

OVW approves the names of potential reviewers for inclusion in the Database and sends each name to LM. The LM staff generates and sends a nominating email from the system web interface to the reviewer, which includes the reviewer's User ID and a temporary password. The reviewer is invited to the web site and prompted to create a new password and enroll in the Database, indicating the reviewer's interest in being a reviewer. Once OVW preliminarily reviews grant applications for the basic minimum requirements (i.e., eligible entity, complete application) and determines how many peer review panels should be organized based on the number of applications moving forward to peer review, peer reviewers are selected based on their expertise and availability.

Currently, the Database maintains a reviewer's name and contact information. Reviewers may also upload a resume or curriculum vitae (CV) as well as self-identified information such as employee type, job categories, and expertise areas. On a voluntary basis, reviewers may provide their gender, education level and ethnicity. The system also maintains basic grant applicant information, retrieved from the U.S. Department of Justice's Office of Justice Programs' (OJP) Grants Management System (GMS), such as applicant's legal name, GMS application number, applicant contact name and information, peer reviewer scores, project description, and funding request amount in connection with certain peer review panels for different OVW solicitations. It also contains information in order to track payments due and the status of payments (e.g., invoice received, invoice paid) for those individuals who serve as peer reviewers on a particular OVW peer review panel. The Database does not, however, capture any information related to a reviewer's bank account information, federal tax ID number, or social security number.

The Database is available via the web only to authorized users. Users must provide valid credentials in order to access the system. Once the user's credentials are verified, varying functionality is available based on the user's role. There are three user roles: (1) Reviewers; (2) OVW staff; and (3) LM staff. There are multiple levels of access that are dependent on the role of the user and the authentication and authorization process (including user ID and encrypted passwords that are used to establish the level of access).

While peer reviewers can access the Database on an as-needed basis at any time, they can only access their own profile to provide updates and edit their information. For example, when a reviewer logs in, s/he can only access his or her own record and update personal information, add or edit educational and other job-related information, and upload a resume. OVW staff can access the Database to perform searches and appraise peer reviewer profiles. OVW staff can retrieve information by name,

area of expertise, profession, and availability. OVW staff access the Database only during the peer review planning phase to identify potential individuals to serve as reviewers. OVW staff will not access the database on a frequent and ongoing basis. LM staff can search, add, modify, and delete records as needed in an administrative or management capacity.[1]

All information in the Database is protected using Secure Sockets Layer (SSL). SSL provides an encrypted link between the user and the web server, so that sensitive information including login credentials and other personally identifiable information (PII) (such as name, email address, and phone numbers) are transmitted securely.

The Database is a stand-alone system and there are no processes that systematically connect it to any other system. A manual process exists to upload applications and store information into the Database from the GMS. LM receives application and score information from GMS in the form of an Electronic Reporting Tool (ERT) report (Excel) and this data is uploaded into the Database using a script that is external to the system.

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

General personal data					
Name	X	Date of birth		Religion	
Maiden name		Place of birth		Financial info	
Alias		Home address	X	Medical information	
Gender	X	Telephone number	X	Military service	
Age		Email address	X	Physical characteristics	

[1] LM staff has the ability to modify a profile. However, in practice, an LM employee edits or modifies a profile only in order to provide assistance to the reviewer at their request (i.e. they are having technical difficulties in making modifications themselves). Further, LM staff has the ability to delete a profile, but, in practice, an LM staff administrator only deletes a profile when directed to do so by an OVW staff member.

General personal data					
Race/ethnicity	X	Education	X	Mother's maiden name	
Other general personal data (specify): Note: Education level, gender, tribal affiliation, and ethnicity may be provided on a voluntary basis.					

Work-related data					
Occupation	X	Telephone number	X	Salary	
Job title	X	Email address	X	Work history	
Work address	X	Business associates			
Other work-related data (specify): Area of expertise; licenses and certifications; current position responsibilities; prior positions and responsibilities; technology access and availability; payments made and status of payments.					

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): None.					

System admin/audit data					
User ID	X	Date/time of access	X	ID files accessed	
IP address		Queries run		Contents of files	
Other system/audit data (specify): The system tracks if an incorrect password is provided more than three times; if so, the user account is locked thereafter. The system also tracks when and who creates and updates records.					

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

Directly from individual about whom the information pertains					
In person		Hard copy: mail/fax		Online	X
Telephone		Email			
Other (specify):					

Government sources					
Within the Component	X	Other DOJ components		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):	Potential Peer Reviewers, LM staff				

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 greatest threats to privacy presented by this system may include unauthorized or inadvertent release of information in identifiable form (IIF) and unauthorized browsing of information. In order to prevent unauthorized access, only authorized users can gain access to the system after providing valid credentials and answers to a security question if using the 'Forgot Password' feature. A potential user is locked out of the system after 3 unsuccessful login attempts. Once logged on, access to various parts of the system is restricted based on a user's role. Also, the Database uses encryption software so that data fields that could potentially be used to identify an individual are encrypted and protected.

OVW considered what type of information would be necessary and critical to collect (e.g., areas of expertise and educational and professional credentials) from an individual in order to select the most qualified individuals for a particular grant review process. All information is provided by the peer reviewer him or herself. No other sources provide information on peer reviewers. This ensures that records on peer reviewers are provided by a reliable source. A potential peer reviewer can only access and edit his or her own profile. OVW staff is unable to edit peer reviewer profiles. OVW staff can only access the database to search by name, occupation, expertise, or availability. LM staff can only access the database for maintenance and administrative purposes. Role-based training is available to all database users. Further, a user is automatically logged out of the system after an established period of inactivity.

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): To keep a current list of individuals who volunteer to serve as peer reviewers during the process of reviewing grant applications submitted in response to solicitations for federal grant programs administered by OVW.		

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.

Every year, OVW posts solicitations for its numerous grant programs authorized by the Violence Against Women Act. Federal funding through grants and cooperative agreements enable communities to increase their capacity to respond to crimes of domestic violence, dating violence, sexual assault, and stalking. OVW grantees support the enforcement of protection orders; provide legal assistance and other services to victims; provide intensive training to police officers, prosecutors, and judges; and support local efforts to respond to domestic violence, dating violence, sexual assault, and stalking. Each year OVW receives far more applications for grant funding than it can possibly fund. Therefore, it is critical that OVW carefully consider which applications to recommend for funding in order to support programs that support grant-funded activities authorized by the statutory provisions of the Violence Against Women Act.

OVW assembles peer review panels comprised of experts and practitioners to help evaluate and score grant applications based on the requirements outlined in the different solicitations for the OVW grant programs. These experts and practitioners may include victim advocates, judges, prosecutors, police officers, legal professionals, and others with expertise on certain issues. For example, those with expertise relating to tribal communities, colleges and universities, rural areas, urban areas, disabled and elderly populations, and service provisions to victims, including those provided by the faith community, as they relate to violence against women. The vast majority of peer reviewers are active practitioners or recent retirees from the professions mentioned above, who can provide current and on-the-ground knowledge of violence against women issues.

As mentioned above, the name and contact information, as well as work-related information relevant to that individual, is collected and maintained in the Database. This information is necessary for OVW to ensure the selection of the most qualified individuals with the expertise and knowledge necessary to serve on different peer review panels to discuss and score applications submitted in response to a specific OVW solicitation for a particular OVW grant program. OVW strives to have individuals who have specific expertise or certain professional experiences serve on a peer review panel where that expertise or experience is invaluable. Further, OVW seeks to attain a balance of peer reviewers by varying the type of professions or backgrounds of the individuals selected to serve on a given peer review panel. It is also important that these individuals are available to serve as a peer reviewer. All potential peer reviewers will be considered and approved by OVW management.

Each year, the number of peer reviewers needed for each OVW grant program is determined based on the number of grant applications received. The information contained in the Database is necessary for OVW to organize and manage the peer review process. This process furthers OVW's mission to provide federal leadership in developing the nation's capacity to reduce violence against women and administer justice for and strengthen services to victims of domestic violence, dating violence, sexual assault, and stalking.

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	5 U.S.C. 301; The Violence Against Women Act of 1994 (42 U.S.C. 13925), as amended by P.L. 113–4 [S. 47], Enacted March 7, 2013, 127 Stat 54; 44 U.S.C. 3101.
	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.)

Records are retained and disposed of in accordance with the National and Records Administration's General Records Schedule (GRS) 3, Item 14. Database information is maintained as long as an individual is interested in serving as an OVW peer reviewer. For instance, if new information is entered into the Database the record for that individual is considered new and will be retained and disposed in accordance with the GRS listed above.

Alternatively, if OVW decides that a particular individual should not serve as a peer reviewer they can request that LM remove the individual from the system. However, reviewer records are not deleted; they are inactivated with a note attached as to why the record was inactivated. Inactive records are "ineligible" for participation in peer reviews. Such records are later deleted in accordance with the GRS listed above. Further, a reviewer cannot delete, or set his or her profile as inactive. A reviewer can also request that OVW delete or make his or her profile inactive, at which point OVW requests LM to inactivate the record with a note indicating the request and the reason.

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.)

There are some potential privacy threats associated with the Database. There is the possibility of misuse of peer reviewer information by OVW personnel and LM personnel, including unauthorized modification of peer reviewer information by LM personnel. To mitigate the possible misuse of Database information by OVW, role-based management is used to limit access to the system to authorized users, as described in section 2.3 above. The Database has segregation of access and abilities according to the type of user.

There is appropriate training for people who have access to the database. All LM employees are required to take an information security course entitled "Information Protection," and those who have access to this system must obtain a Public Trust-Minimum Background Investigation clearance. Also, a DOJ background check is performed on all personnel working in OVW, and such personnel must abide by DOJ's Computer Use Rules of Behavior.

In addition, the auditing features of the Database enable the collection of information, which allows for the reconstruction or review of actions taken by any person with access. The auditing features for the Database mitigate the risk of misuse by an OVW or LM employee of the Database information because any action that that the employee takes can be traced back to him or her.

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	Direct access is provided on an "as needed" basis to OVW staff for the selection of peer reviewers for a particular peer review panel in connection with a specific OVW solicitation. OVW staff does not access this Database on an ongoing basis, and only use it when they are engaged in selecting peer reviewers.
DOJ components				
Federal entities				
State, local, tribal gov't entities				
Public				
Private sector				
Foreign governments				
Foreign entities				
Other (specify): LM (contractor)			X	

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.)

Threats to privacy in connection with the disclosure of information include unauthorized and inadvertent release of information in identifiable form (IIF). Only authorized users can gain access to the system by providing valid credentials and providing answers to security questions, if using the 'Forgot Password' feature. A potential user is locked out of the system after three unsuccessful login attempts. Once logged on, access to various parts of the system is restricted based on a user's role, as mentioned above. Role-based management is used to limit access to the system to authorized users.

Also, even if unauthorized disclosure or inadvertent release of information occurs, the Database uses encryption software, so that data fields that could potentially be used to identify an individual are encrypted and protected. All communication transmitted to and from the system is encrypted by Secure Socket Layer (SSL). SSL provides an encrypted link between the user and the web server so that sensitive information including login credentials and other personally identifiable information (PII) (such as name, email address, and phone numbers) are transmitted securely.

Further, vulnerability scans, conducted routinely by the Information Security Team for the Database, are authorized and conducted on all network devices, servers, and workstations. Security directives are generally implemented by applying patches during the monthly maintenance window. In addition, LM's system infrastructure leverages a defense-in-depth approach of multi-layered external boundary security countermeasures (e.g., protected Internet connections, routers, firewalls, multiple vendor Intrusion Prevent System devices, and Secure Socket Layer (SSL) terminations). Only permitted communication ports and protocols are allowed. All traffic flowing from external boundaries to internal boundaries is filtered, logged, and monitored. The system is stored in a secure data center with appropriate access and environmental controls.

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: A Privacy Statement is displayed on the introductory screen of the system site where the individual logs on. It reads: ***Privacy*** *OVW will not share or exchange your personal information for commercial marketing or any other purpose. The information you submit will only be used by the OVW Peer Review Program to fulfill the stated purpose of the communication or to perform aggregated analysis to improve services.* *In addition, the following appears on the initial screen after the enrollment process has begun:* The Office on Violence Against Women (OVW) has identified you as a potential peer reviewer and invited you to complete an on-line application for enrollment into OVW's Peer Reviewer Database (PRD). The PRD is a secure, web-based system. Your information will only be accessed by OVW program managers and approved peer review support staff. To be selected for a specific peer review panel, you must complete all elements of the enrollment package. Once your application is submitted, you will be eligible to participate in peer reviews for the Office on Violence Against Women. Once you have entered your information in the PRD, you may update your information at any time using your assigned UserID and password. Reviewers are encouraged to periodically update their personal and professional information, as necessary, to ensure OVW has the most accurate information possible to best match your skills to individual program peer reviews. If you do not provide the requested information you may not be selected as a peer reviewer because your profile will be incomplete. There are no other effects on you if you do not provide this information. This information is collected to support the implementation and administration by the Office of Violence Against Women of grant programs authorized by The Violence Against Women Act of 1994 (42 U.S.C. 13925, et seq.), as amended. In addition, this information may be disclosed in limited circumstances pursuant to a routine use, under subsection 552a(b)(3) of the Privacy Act, as described in OVW's System of Record Notice, OVW-001, "Peer Reviewer Database," which will be reviewed and subsequently published in the Federal Register. We appreciate your willingness to participate in the peer review process, and look forward to working with you in the future. If you have questions or concerns about the PRD and the on-line application system, please send an e-mail to ovwreviewers@lmbps.com. *Note: Participation in this application process is completely voluntary.*
	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: Individuals may decide not to participate in the OVW Peer Review process by declining to provide their name, contact information, and work-related information.
	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: By initially participating, and supplying information for the Database, individuals have consented to be considered for selection by OVW to serve as peer reviewers in general. However, they are not giving consent to serve on a particular panel to review grant applications submitted in response to a specific OVW solicitation. Information in the Database is only available for LM and OVW to utilize in support of the peer review work for OVW grant applications, and is not available, used, or released to any other entity or individual.

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.

Potential peer reviewers are provided notice of how information is used and protected when first logging into the Database. By supplying the necessary information, individuals are expressing their consent to be part of the Database, and for their information to be used by OVW as part of the selection of individuals to invite to serve as peer reviewers. Individuals are not, however, providing consent to be part of a specific panel at the time of registration. However, individuals may decide to

serve or not serve as a Peer Reviewer on a particular panel when a request is made later on in the process.

Section 6: Information Security

6.1 Indicate all that apply.

	The information is secured in accordance with FISMA requirements. Provide date of most recent Certification and Accreditation: N/A If Certification and Accreditation has not been completed, but is underway, provide status or expected completion date: LM and OVW initiated this process in January 2013, after an award of a new contract for this Database. At this time, OVW was informed that the system must be transferred from a LM environment to a DOJ data center. LM has begun an internal audit and documentation in preparation for a C&A, but cannot fully complete this process until a final determination is made on the hosting environment.
	A security risk assessment has been conducted. A formal risk assessment has not been completed; however, assessments have been conducted internally
X	Appropriate security controls have been identified and implemented to protect against risks identified in security risk assessment. Specify: The following NIST 800-53 families have been implemented and informally assessed: Awareness and Training; Physical/Environmental; Incident Response; Systems and Communications Protection; and System and Information Integrity. These controls have passed the C&As conducted on other programs. The following NIST 800-53 families have been informally assessed and will need further process/application enhancements to fully support the related controls: Access Control; Identification and Authentication; Audit and Accountability; and Configuration Management. The following NIST 800-53 families have been informally assessed and will need collaboration between LM and OVW on related controls: Security Assessment and Authorization; Contingency Planning; Planning; Risk Assessment; Systems and Services Acquisitions; and Program Management.

X	Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify: **Infrastructure Safeguards:** The OVW PRMS web site currently resides in the shared server environment at the LM-Gaithersburg MD location. The network infrastructure is separated into multiple security layers or tiers. Security tiers are separated by air gaps and firewalls. The top-most layer, "North-Side," is the external tier or "Demilitarized Zone" (DMZ). The DMZ provides a buffered interface to external traffic. All inbound and outbound Internet traffic is routed through the DMZ. Within the DMZ, Denial of Service protection is provided through the use of 2 different vendors' Intrusion Prevention Systems. Anti-Virus software is configured to perform multiple scan types: • Full-system scans weekly against all running processes, local drives. • On-access scans against any files that are opened or written, which includes files from removable media and email. Vulnerability scans are conducted routinely by the Information Security Team on all network devices, servers, and workstations: • Monthly. • Prior to devices, servers, and applications entering the network. • Prior to web applications moving into production. • When significant new vulnerabilities potentially affecting the system(s) are identified and reported. The tools used for assessing vulnerabilities are: • OS Vulnerability Scanner: used to perform scans against all network devices, servers, and workstations. • Web Application Scanner: used to perform scans against web applications. To provide ongoing Continuous Monitoring capability to customers, LM Enterprise Operations Center (EOC) provides network and security operations monitoring coverage. Automated systems are employed to assist in the detection of system issues, to include issues with systems security functionality. Among the application used to assist, include: Centralized log management/review/report tool; System monitoring for availability and performance; Intrusion Prevention Systems Applications and monitoring; Anti-Virus implementation and monitoring; Centralized patch and compliancy monitoring; Centralized device vulnerability tool; Administrative privilege escalation; Execution of privileged functions; and Attack traffic (virus, worm, Trojan horse). **Applications Safeguards:** The PRMS system has been developed using secure coding practices. All developers have been trained in this area and institute these practices in all development and enhancement activities. Safeguards include (but are not limited to): Authentication and access controls (includes role-based access; access to least functionality; handling of failed login attempts; account lockouts and password reset functionality); Session management protections; Input validations; Output encoding; Cross domain attack prevention; Error handling; Upload controls; and Logging practices**.** Additionally, the OVW PRMS system has been scanned by the AppScan software, prior to installation into production. Every time there is a code update, the system is scanned, and identified vulnerabilities are addressed.

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: **Infrastructure Safeguards:** Policies and procedures are in place ensuring information system generates audit records for the following events, as applicable: Login attempts and password changes; Web session terminations; Administrative operating system shutdowns; Administrative modification of the operating system time; Administration modification of security-related log files; Administrative modification of file or directory security attributes; Administrative modification of security-related operating system policies; and Account creation and modification actions. In addition, the following events are audited as referenced include, but are not limited to, and where applicable: System Events; Software Events; System Health Events; Account Management events; User Events; File System Events; Remote Access Events; System Configuration Events; Policy change; and Log Access Events. **Application Safeguards:** Application auditing procedures are under development for OVW PRMS and will be based on the control requirements included in NIST 800-53a, in particular, those involved in Auditing and tied to Account Control and Identification and Authentication family controls. It is our current plan to use GUAM, a locally developed Global User Account Management system, to enhance user authentication and access management capabilities, to improve log audit records, and to provide enhanced support for audit analysis and reporting. The determination of whether GUAM will actually be used for PRMS is dependent upon where OVW PRMS will ultimately be hosted, specific local requirements, and any application access management capabilities available in that environment.
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.
	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.

The Database includes design choices that ensure that privacy protections exist for the sensitive information stored in the system. For example, role-based management is used to limit access to the system to authorized users. Also, the Database uses encryption software so that data fields that could potentially be used to identify an individual are encrypted and protected. As mentioned above, all communication transmitted to and from the system is encrypted. In addition, vulnerability scans are conducted routinely by the Information Security Team for the Database, and are authorized and conducted on all network devices, servers, and workstations.

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.)

	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:
X	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.

OVW and LM staff are able to retrieve information by name.