Privacy Impact Assessment for the

Web-based Standard Form 269 (Web269)

September 26, 2007

Contact Point
Holly Ridgeway
Office of the Chief Information Officer
Office of Justice Programs
202-616-0653

Reviewing Official
Vance Hitch
Chief Information Officer
Department of Justice/Office of the Chief Information Officer
(202) 514-0507

Approving Official
Kenneth Mortensen
Acting Chief Privacy Officer and Civil Liberties Officer
Department of Justice
(202) 353-8878

Introduction

Web269 supports the Office of the Chief Financial Officer (OCFO) by allowing grantees to view grant information and send the Financial Status Report Form SF269A electronically. Web269 allows recipients of OJP funds to file quarterly SF269 reports electronically online, view historical SF269 reports and print hard copies of the reports. Web269 also allows system administrators to manage users, user permissions and security, enter status reports by proxy, monitor grant information, draft e-mail notification wording, and create custom e-mail notification policies. Grantees access the system via Internet Explorer.

Section 1.0 The System and the Information Collected and Stored within the System.

The following questions are intended to define the scope of the information in the system, specifically the nature of the information and the sources from which it is obtained.

1.1 What information is to be collected?

Web269 collects the grantees name, title, complete address including zip code, phone number with area code and extensions, Federal Grant Identifying Number Assigned By Federal Agency, Employer Identification Number, Grantee's Reported Expenditures, Remarks/Comments, and signature of authorized certifying official.

1.2 From whom is the information collected?

The information which Web269 collects is gathered directly from grantees (external users). A grant applicant could be a grantee acting on his/her own behalf or someone who will be providing the information on behalf of a state, county, municipal, township, interstate, intermunicipal, special district, independent school district, state-controlled institutions of higher learning, private university, Indian tribe, profit organization, non-profit organization or other as described and accepted by the grant solicitors.

Section 2.0 The Purpose of the System and the Information Collected and Stored within the System.

The following questions are intended to delineate clearly the purpose for which information is collected in the system.

2.1 Why is the information being collected?

Web269 collects the information as described in section 1.1 in an effort to maintain, manage, report and update the financial status of awarded grants for grantees (external users).

2.2 What specific legal authorities, arrangements, and/or

agreements authorize the collection of information?

The Federal Financial Assistance Management Improvement Act of 1999 (Public Law 106-107) provides the authorization to collect the information as stated in Section 1.1 Public Law 106-107 was passed to improve the effectiveness and performance of Federal financial assistance programs, simplify Federal financial assistance application and reporting requirements, and improve the delivery of services to the public.

2.3 Privacy Impact Analysis: Given the amount and type of information collected, as well as the purpose, discuss what privacy risks were identified and how they were mitigated.

Personal information collected in Web269 is provided by grantees. Based on this information, there are two identified risks associated with this information. First, the possible misuse of Web269 data and, secondly, the possible unauthorized modification of a grantee's information by government personnel (to also include contractors). To mitigate the possible misuse of Web269 data by government personnel, a DOJ background check is performed on all DOJ contractors and government personnel working under OJP on Web269. Web269 is accessible to authorized OJP personnel and grantees only. In addition, Web269 is configured to ensure individual accountability via unique identifiers and passwords for all authorized users of the system. A POA&M will be created to eliminate the display of the SSN.

Section 3.0 Uses of the System and the Information.

The following questions are intended to clearly delineate the intended uses of the information in the system.

3.1 Describe all uses of the information.

Web269 uses the information, as described in section 1.1, for financial status reporting information on grantees. Internal employees use the information in the system to manage and report information on grantees.

3.2 Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern? (Sometimes referred to as data mining.)

No. Web269 does not assist users with any type of data analysis. There are no built in reports that provide an analysis on the information collected and used by Web269 other that described in section 3.1

3.3 How will the information collected from individuals or derived from the system, including the system itself be

checked for accuracy?

The grantees information submitted through Web269 is verified by internal government employees which includes the Customer Service Center Personnel within the Office of the Chief Financial Officer (OCFO). Grants Financial Management Division (GFMD) also checks the accuracy of the WEB269 data submitted. OCFO compares actual expenditures to reported expenses on WEB269. GFMD contacts the grantees via phone or site visit that are deemed to be in excess cash.

3.4 What is the retention period for the data in the system? Has the applicable retention schedule been approved by the National Archives and Records Administration (NARA)?

Web269 does not have NARA approved retention schedule for records and information maintained. DOJ's OCIO department is working with the department retention team and NARA to develop a schedule.

3.5 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

External Web269 users submit personally identifiable information when submitting the financial status report. There is a possible risk for this information to be used or obtained for unauthorized purposes. To mitigate the possible misuse of Web269 data by government personnel, a DOJ background check is performed on all DOJ contractors and government personnel working under OJP on Web269. In addition, Web269 also has segregation of duties between the program and support office users. Roles assigned to users have sufficient granularity to ensure that users have access only to data based on function and need.

Section 4.0 Internal Sharing and Disclosure of Information within the System.

The following questions are intended to define the scope of sharing both within the Department of Justice and with other recipients.

4.1 With which internal components of the Department is the information shared?

Only authorized personnel within OJP have the ability to access the Web269 system and applicable information.

4.2 For each recipient component or office, what information is shared and for what purpose?

The information listed in section 1.1 is shared for the purposes of maintenance, management, reporting, and updating financial status information. The information as listed in section 1.1 is accessible only by authorized individuals within all authorized offices under OJP.

4.3 How is the information transmitted or disclosed?

The information in Web269 is transmitted via a secure HTTPS internet connection. Internal information is disclosed via a secure Intranet connection from each authorized user's workstation to the server which hosts the Web269 system application.

4.4 Privacy Impact Analysis: Given the internal sharing, discuss what privacy risks were identified and how they were mitigated?

The only risk identified with the internal sharing of Web269 information is the possible disclosure or modification of a grantee's information by internal government or contract personnel. This risk is mitigated by the DOJ background check which is performed on all DOJ government personnel or contractors working under OJP on Web269.

In addition, Web269 also has segregation of duties between the program and support offices. Roles assigned to users have strict permissions to ensure that users have access only to data based on role and need. User's actions are also audited and logged by the system. Upon discovery of anomalies and or inappropriate usage the logs can be reviewed to trace the events or determine the extent of the changes.

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to DOJ which includes foreign, Federal, state and local government, and the private sector.

5.1 With which external (non-DOJ) recipient(s) is the information shared?

N/A. Web269 does not share information with any non-DOJ offices.

5.2 What information is shared and for what purpose?

N/A. See section 5.1 above.

5.3 How is the information transmitted or disclosed?

N/A. See section 5.1 above.

5.4 Are there any agreements concerning the security and privacy of the data once it is shared?

N/A. See section 5.1 above.

5.5 What type of training is required for users from agencies outside DOJ prior to receiving access to the information?

N/A. See section 5.1 above.

5.6 Are there any provisions in place for auditing the recipients' use of the information?

N/A. See section 5.1 above.

5.7 Privacy Impact Analysis: Given the external sharing, what privacy risks were identified and describe how they were mitigated?

No privacy risks were identified with external sharing of Web269 information since information is not shared or disclosed with non-DOJ recipients.

Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the opportunity to consent to uses of said information, and the opportunity to decline to provide information.

6.1 Was any form of notice provided to the individual prior to collection of information? If yes, please provide a copy of the notice as an appendix. (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register Notice.) If notice was not provided, why not?

Yes. There is a privacy statement displayed on the log-in page for WEB269. A copy of this privacy statement is attached as Appendix A. In addition, as System of Records Notices and Privacy Act Notices are updated, as appropriate, this PIA will be updated to reflect those changes.

6.2 Do individuals have an opportunity and/or right to decline to provide information?

Yes. The information provided on the Web269 form has optional fields that the grantee (external user) is not required to be provided information. Only identifiable information on the form such as Federal Grant ID Number, Name, and Address are required.

6.3 Do individuals have an opportunity to consent to particular uses of the information, and if so, what is the procedure by which an individual would provide such consent?

No. All aspects of system usage for Web269 as described in Section 3.1 are necessary tasks for Web269 application.

6.4 Privacy Impact Analysis: Given the notice provided to individuals above, describe what privacy risks were identified and how you mitigated them.

There are no associated risks identified with the privacy notice provided by Web269.

Section 7.0 Individual Access and Redress

The following questions concern an individual's ability to ensure the accuracy of the information collected about him/her.

7.1 What are the procedures which allow individuals the opportunity to seek access to or redress of their own information?

The grantee (external user) has the ability to seek access to Web269 by contacting the OCFO Customer Service Center via e-mail or telephone using the number listed on the main page of the Web269 website. Grantees can also seek access of their own information by initiating a Freedom of Information Act (FOIA) and/or a Privacy Act request.

7.2 How are individuals notified of the procedures for seeking access to or amendment of their information?

Web269 displays information for grantees to amend their information which is located on the Web269 site. A notification on the site and main page advises grantees (external users) of the e-mail address or phone number to OCFO Customer Service Center.

7.3 If no opportunity to seek amendment is provided, are any other redress alternatives available to the individual?

N/A. See 7.1 above.

7.4 Privacy Impact Analysis: Discuss any opportunities or procedures by which an individual can contest information

contained in this system or actions taken as a result of agency reliance on information in the system.

Grantees (external users) can contest information contained in Web269 by amending the information in a Web269 amendment or by faxing over a signed Web269 form to the OCFO Customer Service Center.

Section 8.0 Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 Which user group(s) will have access to the system?

Access to Web269 is granted to external users (grantees), and authorized contractors or government personnel to also include system administrators.

8.2 Will contractors to the Department have access to the system? If so, please submit a copy of the contract describing their role with this PIA.

Contractors will have access to the system. However, a copy of the contract describing their roles with this PIA was not provided. Please see Appendix B for a copy of the contract.

8.3 Does the system use "roles" to assign privileges to users of the system?

Yes. Roles are assigned according to a user's function and need. The Web269 system has administrator roles, help desk (customer service) administrator roles, and grantee (external user) roles.

8.4 What procedures are in place to determine which users may access the system and are they documented?

OJP has approved and utilizes a Standard Operating Procedure (SOP) for the Account Management process. This SOP also includes accounts created for Web269 as well.

8.5 How are the actual assignments of roles and rules verified according to established security and auditing procedures?

OJP has approved and utilizes a Standard Operating Procedure (SOP) for the Annual Re-certification process for all applicable systems to include Web269. This SOP ensures the appropriate rules and roles that have been assigned are still necessary as documented.

8.6 What auditing measures and technical safeguards are in place to prevent misuse of data?

The segregation of duties between the program and support offices in addition to role-based privileges prevent the misuse of Web269 data by allowing all roles specific rights based on function and need. Grantees only have access to their own data and their sessions are monitored every time they login. In addition internal users are allowed to view and generate reports and information associated with solicitations from their respective offices unless authorized.

8.7 Describe what privacy training is provided to users either generally or specifically relevant to the functionality of the program or system?

There is no specific privacy training relating to the external user. All grantees (external users) are provided access to a Web269 online training tutorial in which to become familiar with the system. The training is located under the HELP menu of the Web269 log-in page.

8.8 Is the data secured in accordance with FISMA requirements? If yes, when was Certification & Accreditation last completed?

Yes. Web269 is in compliance with DOJ policy and NIST SP 800-37. The system has been certified and accredited using the NIST 800-53 security controls. The last certification and accreditation was completed for Web269 on May 19, 2006 and will be valid until May 2009.

8.9 Privacy Impact Analysis: Given access and security controls, what privacy risks were identified and describe how they were mitigated?

The only risk associated with external users is the invalid assignment of external users for the sole purpose of obtaining information for unauthorized use or disclosure. To mitigate this risk, all applicants are initially verified prior to being allowed access to Web269.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware, RFID, biometrics and other technology.

9.1 Were competing technologies evaluated to assess and compare their ability to effectively achieve system goals?

Yes. Web269 was also developed according to the DOJ's Systems Development Life

Cycle (SDLC). System goals were achieved via the DOJ's SDLC guidance.

9.2 Describe how data integrity, privacy, and security were analyzed as part of the decisions made for your system.

Web269 was developed in accordance with the DOJ SDLC document. The DOJ SDLC addresses both privacy and security of the system and its data. The segregation of duties between the program and support offices in addition to role-based privileges prevent the misuse of Web269 data by allowing all roles specific rights based on function and need.

9.3 What design choices were made to enhance privacy?

Web269's privacy was enhanced by providing system access roles and encryption for passwords.

Conclusion

Web269 was developed to allow grantees the ability to view grant information and send the Financial Status Report Form SF269A electronically. The system was developed such that it requires only pertinent applicant and application information as to provide the capability for authorized users to manage grants efficiently and effectively. By doing so, privacy is being considered regarding the information which is requested by specific grant applications. The information collected by Web269 is used only for purposes of managing grant applications and the associated activities. This information is accessible only by authorized Web269 users and personnel.

Responsible Officials

Holly Ridgeway

Department of Justice

Approval Signature

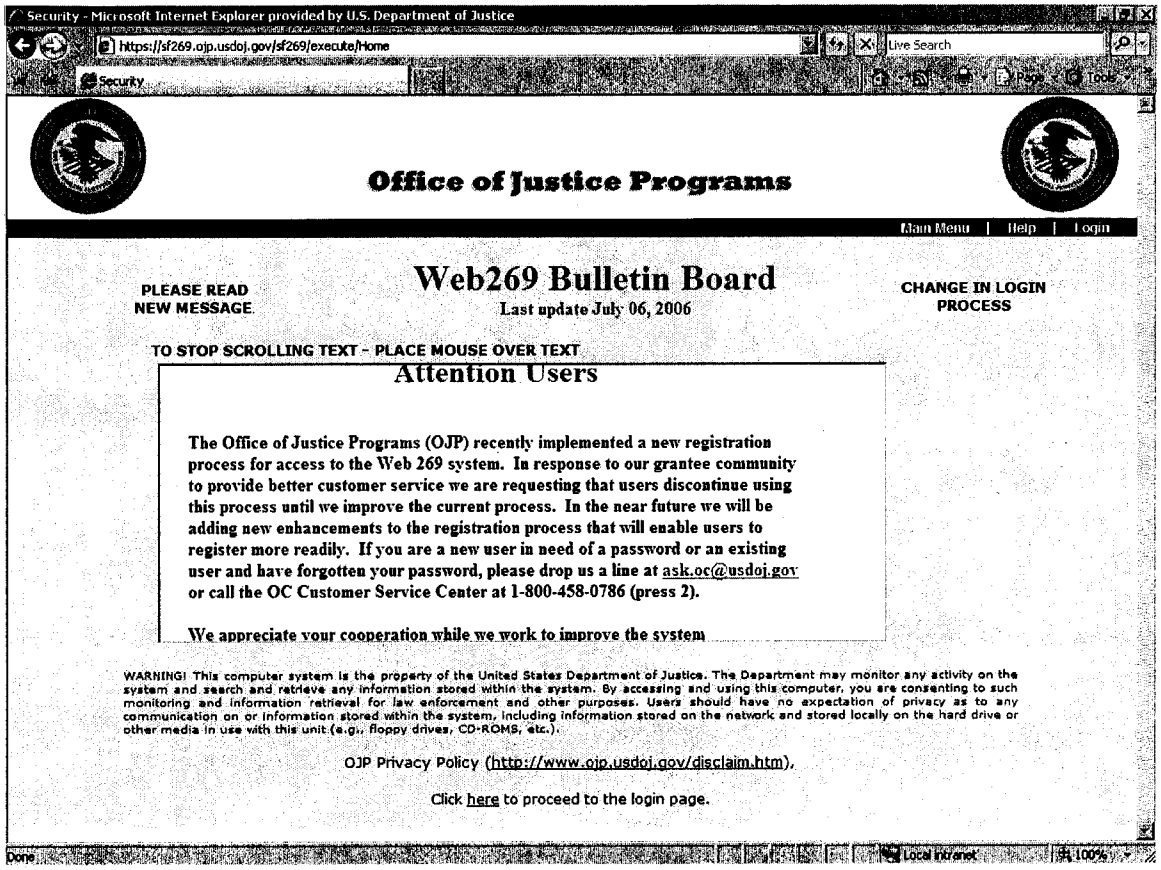
/s/ — 09/25/2007

Kenneth Mortensen — **Date**
Acting Chief Privacy and Civil Liberties Officer
Department of Justice

For Jonathan Wackrow — 9-25-07

Holly Ridgeway — **Date**
OJP IT Director of Security
Department of Justice

Appendix A. Web269 Privacy Notice



Appendix B. Copy of Contract for Contractor Roles & Responsibilities

Contact Holly Ridgeway to obtain a copy of the contract that explains the contractor's roles and responsibilities.