



Privacy Impact Assessment for the
Grants Management System (GMS)
Office of Justice Programs

January 29, 2007

Contact Point

Jeffrey Test, Ph.D.
Office of the Chief Information Officer
Office of Justice Programs
202-514-8460

Reviewing Official

Jane C. Horvath
Chief Privacy Officer and Civil Liberties Officer
Department of Justice
(202) 514-0049

Introduction

The Grants Management System (GMS) provides the Office of Justice Programs (OJP) with the capability to accept and manage grant applications electronically. GMS is designed to support the grant management process from the receipt of grant applications to post-award activities, such as creating budget modifications and grant monitoring activities. GMS provides the capability for decision makers to expeditiously obtain available results of (external) peer or internal reviews of applications and quickens grant funding decisions. The electronic tracking and approval capability enables the reviewing offices to complete their review concurrently and notify program offices of completed and incomplete tasks. GMS also provides OJP with the capabilities to post public solicitations announcing that grant money is available, process applications for grant money and generate award documents for successful applications. The GMS system is extended with an interconnection to the Grants.Gov system which is owned by the Department of Health and Human Services (HHS). This interconnection allows a one way pull by GMS from Grants.Gov. The interconnection allows GMS to download grant applications from Grants.gov.

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?

The information which GMS collects is an applicant's full legal name, POC, alternate POC, address, phone number, Employer Identification Number (EIN#) or Social Security Number (SSN) if the application is for an individual, Dun and Bradstreet number (DUNS #), name of the Signing Authority (authorized representative), principal investigator (conditional), e-mail address, OJP vendor number and the GMS user-id. Once an applicant has established an account on GMS, additional information is collected from the applicant via GMS request forms.

Additionally, GMS collects the Catalog of Federal Domestic Assistance Number, congressional districts, applicant identifier, state application identifier, federal identifier for applicants. An applicant is also able to submit attachments through GMS which could possibly contain additional personally identifiable information (PII) depending on the grant solicitation's information requirements.

A State Criminal Alien Assistance Program (SCAAP) application is submitted by the applicant when applying for SCAAP based GMS grant solicitation. Applications for SCAAP grants in GMS require different information from applicants. The information collected on a SCAAP application is the alien number (A-number); first, last and middle names; DOB; unique inmate identifier number; foreign country of birth; date taken into custody; date released from custody and FBI number.

1.2 From whom is the information collected?

The information which GMS collects is gathered directly from grant applicants (external users). A grant applicant could be an individual 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 GMS 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?

GMS collects the information as described in section 1.1 in an effort to support the grant management process via the receipt of grant applications, grant processing activities (to include grant monitoring) and post-award grant activities for the OJP offices and program bureaus. Ultimately, GMS would provide a means in which to ease public access to Federal grant programs and reduce the flow of paper award packages.

2.2 What specific legal authorities, arrangements, and/or agreements authorize the collection of information?

The Federal Financial Assistance Management Improvement Act of 1999 and the E-Grants Initiative both authorize OJP's Grant Management System (GMS) to collect the information as described in section 1.1. GMS was developed in part to satisfy requirements of the Federal Financial Assistance Management Improvement Act of 1999 and additional functionality was added in an effort to address the intent of the E-Grants Initiative.

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.

Based on the information provided in section 1.0 and 2.0, there is personal information being provided by GMS applicants. Based on this information, there are two identified risks associated with this information. The possible misuse of GMS applicant data by government and external personnel (i.e., peer reviewers) and the possible unauthorized modification of application information by government personnel. To mitigate the possible misuse of GMS data by government and external personnel, a DOJ background check is performed on all DOJ government personnel working under OJP on GMS. In addition, the auditing features for GMS enable the collection of information which allows for the reconstruction or review of actions taken by an individual. The auditing features for GMS mitigate the risk of a government

employee making unauthorized modifications to an applicant's application information. To mitigate the possible unauthorized disclosure of application information, External Peer Reviewers are required to acknowledge and accept a Peer Reviewer Certification form which provides assurances via a pre-review nondisclosure form. The current electronic version of the form is shown in Appendix A.

For the groups identified in section 1.2, there is an inherent risk of information sharing if more than one individual will manage the GMS account for the applicant group(s) in question. If so, the GMS user-id and password would be known to more than one person and would not provide individual accountability. To mitigate this risk, GMS incorporates auditing features which collect enough information from which to reconstruct or review the actions taken by an individual.

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.

GMS uses the information, as described in section 1.1, solely for the purpose of supporting the grant management process to award an application and monitor grant processing activities. The information collected by GMS from external users allows the user the capability to create user accounts within GMS, search for funding, apply for funding, complete and submit applications, monitor status of the application, receive awards, submit progress reports, and provide post-award reporting via the Grants Adjustment Notice (GAN Module). The internal users of GMS have the capability to use information within GMS to confirm eligibility of applicants, receive online applications, perform initial and peer reviews, generate award packages, process awards through program and support offices, notify stake holders and grantees, receive and review progress reports, enter grant monitoring reviews in GMS, and process any adjustment requests from the grantee.

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. There is no information analysis performed on the information collected and used by GMS other than 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 applicant information submitted thru GMS is reviewed by the government personnel prior to granting an award and/or disbursement of funds. The GMS system itself implements

form field checking on the interface. Specific information like the DUNS and EIN numbers are verified directly with the issuing party by GMS internal users. The application information is verified through the workflow process to include an initial review and approval by the Program Office, General Counsel (in special cases), Office of Budget and Management Services, Office of the Comptroller, Assistant Attorney General for OJP (“AAG”), Office of Communications, and finally the Control Desk.

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)?

The GMS retention schedule for records or information maintained was initially approved in 1974 and its permanent status has been upheld through the last approval in 1986. An Appraisal Archivist at the NARA/Life Cycle Management Division (NWML) is evaluating the appraisal of this information. In order to determine if the records should continue as permanent, OJP is preparing updated information to NARA/NWML for this evaluation.

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 GMS users submit personally identifiable information when creating a GMS account and when applying for individual grants. There is a possible risk for this information to be used or obtained for unauthorized purposes. This risk is compounded with the fact that GMS records and grant information are not deleted from the system. Records within GMS are maintained for auditing, archival and historical purposes. This only increases the amount of information which could be exploited by this risk. This risk is mitigated by having only cleared government personnel utilize GMS and having the ability to establish individual accountability for system usage via the system auditing capabilities. In addition, GMS 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?

There are many offices within the Department of Justice (DOJ) that are allowed to access information pertaining to their office only. The DOJ components that have offices that are

allowed access to GMS are the OJP, Justice Management Division (JMD), the Faith-Based Office located in the Deputy Attorney's Office, and the Office on Violence Against Women (OVW). By default, authorized staff within the entities listed above (and their authorized offices) all have the ability to access applicable GMS information. If necessary, information can be shared provided individuals from each office have a need to access the information and are also authorized.

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

Only the offices, as listed in section 4.1, have access to GMS. These offices are only allowed to view all applicable applications which were submitted under a solicitation from their office only. The offices listed in section 4.1 all have the ability to view GMS information for the purposes described in section 3.1.

4.3 How is the information transmitted or disclosed?

The information in GMS is shared between the offices as listed in section 4.1 via GMS system access. Each office as listed in section 4.1 has access to GMS and thus allowed access to the appropriate applications submitted by applicants. The information contained within GMS is located within the system. There is no need to transmit any information outside of GMS to any of the offices listed in section 4.1. All transmissions and disclosures of information would be performed electronically by role-based access to the system, when necessary.

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 GMS information is the possible disclosure or modification of an applicant's information and application by internal government personnel. This risk is mitigated by the DOJ background check which is performed on all DOJ government personnel or contractors working under OJP on GMS. In addition, GMS also has segregation of duties between the program and support offices. Roles assigned to users have sufficient granularity to ensure that users have access only to data based on function and need.

The auditing features for GMS enable the collection of information which allows for the reconstruction or review of actions taken by an individual. The auditing features for GMS mitigate the risk of a government employee making unauthorized modifications to an applicant's application information.

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?

The only external non-DOJ office with access to GMS is the Department of Homeland Security's Office of Grants and Training (OG&T). By default, authorized individuals within OG&T have the ability to access applicable GMS information as would the components and offices listed in section 4.1.

For SCAAP applications, GMS information is shared with authorized individuals within the Department of Homeland Security's Bureau of Immigration and Customs Enforcement (ICE) group to validate criminal alien incarceration records.

Authorized external users with the Peer Review role also have access to information via the GMS system. External Peer Reviewers for GMS validate and rank specific information in an applicant's grant request.

5.2 What information is shared and for what purpose?

Only the components/offices, as listed in section 4.1 and the OG&T office listed in section 5.1 have access to GMS. These offices are allowed to view only applicable applications which were submitted under a solicitation from their office. The offices listed in section 4.1 and the OG&T office all have the ability to view GMS information for the purposes described in section 3.1.

The GMS SCAAP application information, as described in section 1.1, is submitted to ICE and ICE will return the information in a validated, categorized format which is uploaded back to GMS. The purpose of this validation is to accurately determine the appropriate funding amount based on the information in the SCAAP application.

5.3 How is the information transmitted or disclosed?

The information in GMS is shared between the offices as listed in section 4.1, the OG&T office and external Peer Reviewers via GMS system access controls. Each office as listed in section 4.1, the OG&T office all have users authorized to access the GMS system. All external users access GMS via an external public website using a Secure Hyper Text Transmission Protocol (HTTPS) session. All internal users, to include the OG&T users, access GMS via an intranet web site accessible by authorized internal individuals only. External Peer Reviewers are selected and authorized by the components and offices listed in section 4.1 and the OG&T office. GMS internal users, including OG&T users are only allowed access to the appropriate applications submitted by applicants. External Peer Reviewers are only allowed access to the assigned Peer Review Panels assigned by authorized GMS internal personnel. The information contained within GMS is located within the system. There is no need to transmit any information outside of GMS to any of the offices listed in section 4.1, the OG&T office or external Peer Reviewers. All transmissions and disclosures of information would be performed electronically by role-based access to the system, when necessary.

The SCAAP information is taken from GMS and downloaded to a CD and hand-delivered to ICE.

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

OJP currently has a Memorandum of Understanding in place to facilitate the sharing of information between OJP and ICE. Prior to accessing a Peer Review Panel within the system, after logging into GMS, External Peer Reviewers are required to acknowledge and accept a Peer Reviewer Certification form which provides assurances via an electronic pre-review nondisclosure form. If the External Peer Reviewer does not accept the Peer Reviewer Certification form he or she will not be granted any further access to GMS and has no other option but to close the web browser.

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

All internal users with access to GMS (to include internal users outside of DOJ) are required to take appropriate training prior to accessing the system. In addition, there is a service level agreement in place between DOJ OJP and DHS OG&T which states that OG&T will comply with all Government Policies and Guidelines. There is no GMS training required for ICE/DHS GMS users since ICE personnel do not access the GMS system.

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

External Peer Reviewers are only allowed access to the Peer Review Module when the Peer Review Panels to which they have been assigned is in session. Additional auditing features of GMS as described in section 2.3 provide additional capabilities in which to audit the actions of External Peer Reviewers in GMS. The GMS data is shared with only authorized ICE personnel based on function and need and is provided in a read-only format and thus does not allow for the possibility of data manipulation. The ICE group returns to OJP, the media used to store the GMS data. The ICE group does not retain any GMS data provided by OJP. There are no additional auditing provisions on the recipients' use of the information.

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

One risk identified with the external sharing of GMS information is the possible disclosure or modification of an applicant's information and application by internal government personnel. This risk is mitigated by the DOJ background check which is performed on all DOJ government personnel working under OJP on GMS. A similar background investigation is also performed on all DHS/ICE personnel who assist OJP with this task.

An associated risk for external users with the Peer Review role would be the possible misuse or unauthorized dissemination of an applicant's information and/or grant request. To mitigate this risk, all external users with the Peer Review role acknowledge and accept the Peer Reviewer certification prior to being allowed to perform the peer review function. See the attached electronic version of the Peer Reviewer Certification Form in Appendix A. In addition, a Peer Reviewer has access to the GMS Peer Review Module only when the Peer Review Panel to which he or she is assigned is in session.

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 an existing system of records notice published by DOJ in the Federal Register which provides some details as to the information collected and the usage of the system. However, the current SORN does not fully reflect the totality of the information collected. The SORN is being revised and we anticipate that the revisions will be published in the next few months. The existing GMS System Of Records Notice (SORN) can be found in the Federal Register, Vol. 53, No. 200 Monday, October 17, 1988 on page 40526. There is also a privacy statement displayed on the log-in page for GMS. A copy of this privacy statement is attached as Appendix B.

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

No. GMS applicants are not allowed an opportunity to deny information requests. Information requested by a solicitation is mandatory for grant consideration.

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 GMS as described in section 3.1 are necessary tasks for GMS applications.

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 GMS.

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?

Once an applicant has created an account and the initial review of the applicant information has been verified, external users are allowed the capability to view and or modify the existing profile which they created. After an award is made, the recipient can change any information via the Grant Adjustment Notice (GAN) module.

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

Internal GMS personnel will submit a change request via e-mail to an applicant in which to provide notification of any issues or concerns regarding his or her information or application.

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

Not applicable.

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.

GMS does not provide the capability for the applicant or grantee to contest a determination via GMS. If necessary, an applicant can file a formal complaint with the OJP's Office of the General Counsel.

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 GMS is granted to external (e.g., GMS applicants and peer reviewers), and internal users (e.g., government GMS users and GMS administrators, including developers).

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.

Yes. The only contractors with access to GMS are the developers and administrators of the system. Their level of access is controlled by their assigned roles.

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. GMS roles have deep granularity; therefore, access is tightly controlled.

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

All users of the system are assigned a role according to function and need. For the external users this role is reviewed by internal GMS personnel. A GMS official and administrator will verify and or validate internal user assignments.

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

External roles under GMS are verified by internal GMS personnel after the initial account creation request. Internal GMS users undergo a recertification process at least annually. This process includes the review and validation of all internal GMS user roles and accounts.

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 GMS data by allowing all roles specific rights based on function and need. The auditing features for GMS also mitigate the risk of a potential misuse of GMS data. In addition internal users are allowed to view only applications 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. External users with the Peer Review role acknowledge and accept the Peer Reviewer certification prior to being allowed to perform the peer review function. Internal DOJ and OJP users undergo individual Computer Security Awareness Training annually, which includes information on general system privacy.

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

Yes. The GMS system has been certified and accredited using the NIST 800-53 security controls. The last certification and accreditation was completed for GMS on February 27, 2006 and will be valid until February 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 GMS. During this verification, the applicant's newly-created account is held in a locked state until the verification is complete.

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. GMS 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.

GMS 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 GMS data by allowing all roles specific rights based on function and need. The auditing features for GMS also mitigate the risk of a potential misuse of GMS data.

9.3 What design choices were made to enhance privacy?

There was a recent change to GMS to enhance the privacy of external users by incorporating FISCAM controls and guidance on system passwords into GMS.

Conclusion

The concluding section should inform the reader, in summary fashion, how you constructed your system, program, rule, or technology based on privacy risks and mitigation strategies.


GMS was developed in an effort to support the grant management process for DOJ components, DHS's OG&T and external users of the system. 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 GMS is used only for purposes of managing grant applications and the associated activities. This information is accessible only by authorized GMS users and personnel. Specific GMS information is shared with DHS/ICE. Usage of the information by DHS/ICE is clearly documented in the MOU in place between DOJ/OJP and DHS/ICE. Usage of GMS by DHS OG&T is governed by a service level agreement between DOJ OJP and DHS OG&T. Updates and modifications to GMS take into consideration the privacy and security of the information that it contains.

Responsible Officials

<< ADD Privacy Officer/Project Manager >>

Department of Justice

Approval Signature Page

 _____ <<Sign Date>>
Jane Horvath
Chief Privacy and Civil Liberties Officer
Department of Justice

9.3 What design choices were made to enhance privacy?

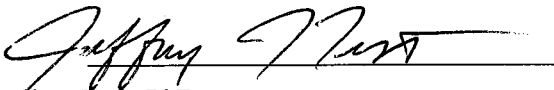
There was a recent change to GMS to enhance the privacy of external users by incorporating FISCAM controls and guidance on system passwords into GMS.

Conclusion

The concluding section should inform the reader, in summary fashion, how you constructed your system, program, rule, or technology based on privacy risks and mitigation strategies.

GMS was developed in an effort to support the grant management process for DOJ components, DHS's OG&T and external users of the system. 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 GMS is used only for purposes of managing grant applications and the associated activities. This information is accessible only by authorized GMS users and personnel. Specific GMS information is shared with DHS/ICE. Usage of the information by DHS/ICE is clearly documented in the MOU in place between DOJ/OJP and DHS/ICE. Usage of GMS by DHS OG&T is governed by a service level agreement between DOJ OJP and DHS OG&T. Updates and modifications to GMS take into consideration the privacy and security of the information that it contains.

Responsible Officials



Jeffrey Test, PhD.

Department of Justice/Office of Justice Programs
Division Director, Information Technology Security Division

Approval Signature Page

<<Sign Date>>

Jane Horvath
Chief Privacy and Civil Liberties Officer
Department of Justice

APPENDIX A. Peer Review Reviewer Certification Form

Peer Review Reviewer Certification

NOTE: You must click on the "Accept" button at the bottom of the page before closing this window.

Pre-Review Nondisclosure Certification

This is a Certification of Non-Disclosure and the Lack of Conflict of Interest in your activities in conjunction with this Peer Review.

You certify that you will not disclose any of the applicant, application and other information that you will access during your participation in this review. If you are not totally objective and free from bias, you should not review participate in the Peer Review process.

Applicants need to be assured their proposals are transmitted without prejudice to a peer review and that the reviews contain accurate, unbiased, supportable comments. Proposals are submitted to the Office of Justice Programs in confidence; you must respect that confidentiality and ensure that there are no potential conflicts of interest. Your comments enjoy a similar confidentiality, and applicants never receive any report that contains your name. In addition to peer reviewers' identities, all oral and written communications created in or resulting from the peer review process are confidential.

By accepting, you certify that:

- I have been briefed on DOJ Standards of Conduct and policies concerning divulging sensitive procurement information. I am aware that disclosure of trade secrets and other confidential information (18 USC 1905) is a crime. I understand that certain conflicts of interest (18 USC 203-209) constitute crimes.
- I will not communicate, transmit, or otherwise divulge any of the data that may come into my possession as a part of my duties or about which I gain knowledge during the course of my duties without specific authority of appropriate officials.
- If I am listed as a staff member, consultant, or advisor on a proposal I will contact the Office of Justice Programs immediately.
- If I have a close personal or familial relationship with the author(s)/staff on a proposal I will contact the Office of Justice Programs immediately.
- If I recently had a financial relationship with the author(s)/staff on a proposal involving grants, publications, presentations, etc I will contact the Office of Justice Programs immediately.
- If I have recently been a faculty/staff member of the department, school, or university/institution submitting the proposal I will contact the Office of Justice Programs immediately.
- I can review a proposal objectively or do not feel others would view such actions to be a problem.

If you choose not to accept this certification, you will not be able to continue on this panel. Please contact your peer review contact to discuss your choice and any other questions you might have.

APPENDIX B. GMS PRIVACY NOTICE

Applicant Sign In

Page 1 of 1



Grant Management System



OVW Grantees: Please note that some changes have been made to the progress reports module. Please review the updated Quick Start Guide or online job aids for new uploading and downloading procedures. For questions please contact the GMS Helpdesk at 888-549-9901, option 3.

Applicant Sign In

User ID:
Password:

[First Time User?](#)

[Forgotten your password?](#)

NOTICE TO USERS This is a Federal computer system and is the property of the United States Government. It is for authorized use only. Users (authorized or unauthorized) have no explicit or implicit expectation of privacy. Any or all uses of this system and all files on this system may be intercepted, monitored, recorded, copied, audited, inspected, and disclosed to authorized site, Department of Justice, and law enforcement personnel, as well as authorized officials of other agencies. By using this system, the user consents to such interception, monitoring, recording, auditing, inspection, and disclosure at the discretion of authorized site or Department of Justice personnel. Unauthorized or improper use of this system may result in administrative disciplinary action and civil and criminal penalties. By continuing to use this system, you indicate your awareness of and consent to these terms and conditions of use. LOG OFF IMMEDIATELY if you do not agree to the conditions stated in this warning. [Privacy, Security and Disclaimers](#)