National Oceanic and Atmospheric Administration (NOAA)

Grants Online

Privacy Impact Assessment Statement

July 2008

Reviewed by: Sarah Brabson, NOAA Office of the Chief Information Officer

NOAA Grants Online

Privacy Impact Assessment Statement

Unique Project Identifier: 006-48-04-00-01-3802-00-117-057

IT Security System: NOAA 1105

Project Description: The mission of the NOAA Grants Online Program Management Office (PMO) is to provide NOAA with a single unified grant processing and administration system, using an electronic solution that will reduce processing time and increase efficiency. This mission statement and other information about the PMO and the NOAA Grants Program may be found at the PMO Web site PMO Web site..

NOAA Grants Online is a different program, with a different purpose, than the government-wide Grants.gov, which allows grant-seeking organizations to electronically find and apply for federal grants. Grants.gov is the single access point for over 1,000 grant programs offered by all federal grant-making agencies.

NOAA Grants Online: 1) processes NOAA grant applications which have been submitted to grants.gov and forwarded by grants.gov to NOAA; 2) selects grant awardees from applications received and makes the grant awards; and 3) administers and monitors awarded grants throughout the life of the grant.

1. What information is to be collected (e.g., nature and source)?

Grants Online collects personally identifiable information (PII) in two ways.

Grant applicants, including non-profit and for-profit organizations, are required to provide personal information about themselves or key officials in their organization. This information is submitted on Commerce form CD-346, Applicant for Funding Assistance, in order that the Office of the Inspector General can conduct a name or identification check to determine if the applicant or any key individuals associated with the applicant have been convicted of or are presently facing criminal charges (e.g., fraud, theft, perjury), or other matters that significantly reflect on the applicant's management honesty or financial integrity. The information collected includes the name, address, date and place of birth, and three years' employment and residence history of the grant applicant or key official. Providing the individual's Social Security Number is voluntary. This collection has been approved by the Office of Management and Budget (OMB Approval Number 0605-0001), in accordance with the Paperwork Reduction Act.

The completed CD-346, which must be submitted as a signed paper form, resides in the Grants Online system as a scanned pdf, along with the other grant application information, described below, that is collected online. The completed CD-346 must be stored in the system to ensure that the electronic grant file is complete.

Additionally, the name and contact information for the individual who represents an organization and serves as the point of contact for management of the grant is collected

through the use of government-wide Standard Forms. In the case of awards to individuals, the "Application for Federal Assistance SF 424—Individual," requests Social Security Numbers on an optional basis. The "Application for Federal Domestic Assistance – Short Organizational," also requests Social Security Numbers from Project Directors and Primary Contacts/Grants Administrators on a voluntary basis. The SF 424 series of forms can be found at http://www.grants.gov.

The collection of Social Security Numbers is permitted under the authority of the Debt Collection Improvement Act of 1996, 31 U.S.C. 7701. Personal identifying information is not routinely made public, and is protected to the extent permitted under both the Freedom of Information Act, 5 U.S.C. 552, and the Privacy Act of 1974, 5 U.S.C. 552a. Further, Social Security Numbers are not used as award identifiers.

Business information collected includes Data Universal Numbering System (DUNS) numbers and financial institution information specific to institutions for the purposes of providing them their awarded grant funds. Other information that is collected (progress reports, final reports, etc.) is made available for public review following standard grants management practices.

2. Why is the information being collected (e.g., to determine eligibility)?

The information that is collected is used for purposes of reviewing grant applications, verifying the identity and capabilities of grant recipients, and distributing and administering grants.

3. What is the intended use of the information (e.g., to verify existing data)?

The information is used for verification of applicants' identity and capabilities so that effective grant-making and tracking of awardees' progress can occur. In addition, grantee progress reports, final reports, and similar publications and research findings are available for public viewing and comment, following standard grants management practices.

4. With whom will the information be shared (e.g., another agency for a specified programmatic purpose)?

The information is not shared with any third parties or unauthorized personnel, except for the public information noted above, or as authorized under the Privacy Act, 5 U.S.C. § 552a.

5. What opportunities do individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how may individuals grant consent?

All information collected is submitted by the parties involved as part of the grant application (through grants.gov, which forwards proposals for NOAA programs) and the grants administration process. Participation in the grant application process is itself voluntary. Within the application, specifically: submission of the Social Security

Number, if an individual is applying, is voluntary and not required.

An applicant cannot authorize dissemination to another party. Authorizing dissemination to a third party is not an option.

6. How is the information secured (e.g., administrative and technological controls)?

Management Controls

A Certification and Accreditation (C&A) was completed and is in force for this system. The C&A is the IT security review process that must be satisfactorily completed before a system may become operational. The IT Security Plan for this system is also current and in force.

Every two weeks the Grants Online team holds a Program Management Office meeting to discuss matters including the application of system updates and security patches. All updates and patches are run through a rigorous testing process to insure functionality and continued system availability. Management officials and technical representatives participate in all levels of the discussions to insure timely application of these updates and patches.

Operational Controls

The Grants Online system is located at the NOAA Information Technology Center (ITC) in Largo, Maryland. The ITC data center has key card controls limiting access to all production servers. Nightly backups are performed with backup media being stored approximately 17 miles from the production servers in a fire-proof media safe. Integrity checks of the backups are performed weekly.

All server sites have implemented the following minimum requirements. Access to all servers is controlled, with access limited to only those support personnel with a demonstrated need for access. Servers are kept in a locked room accessible only by specified management and system support personnel. Each server requires a specific log-on process. All entrance doors are identified and marked. A log is kept of all personnel who were issued a security card, key and/or combination that grants access to the room housing the server, and all visitors are escorted while in this room. All servers are housed in an area where appropriate environmental security controls are implemented, which include measures implemented to mitigate damage to automated information system resources caused by fire, electricity, water and inadequate climate controls.

Technical Controls

Access controls are used on the production equipment through the use of system usernames and passwords as well as database usernames and passwords. Logging of access is kept and reviewed for any improprieties. Password length and duration of validity follow Department of Commerce standards as outlined in Appendix G of the *IT Security Program Policy and Minimum Implementation Standards.*

7. How is the data extract log and verify requirement being met?

The Grants Online system is an Oracle and BEA/Weblogic based application. This application does not directly support a database extract by end-users. In those cases where an extract must be generated, the Grants Online user (extracts are limited only to personnel with certain access privileges) develops the extract routine and generates the data and formally transmits the data to the requesting party. Currently, this logging process is entirely manual. In those rare cases where an extract/report that contains personally identifiable information (PII) is required, the extract is tracked via manual entry and a determination is made to verify the duration of the extracted data. A notice is provided that the data must be destroyed after 90 days if it is no longer required. The manual logs of who currently has extracted PII data are reviewed monthly.

For any PII extracts from Grants Online that have not been destroyed after 90 days, an e-mail is sent requiring written or e-mail confirmation that either the PII data has been destroyed or that the need continues for an additional 90 days.

8. Is a system of records being created under the Privacy Act, 5 U.S.C. 552a?

No. Although it includes some personal information, the primary retrieval from an electronic file is not by a personal identifier, and it is not a system of records as defined by the Privacy Act.

9. How long are these records retained? The response should include the retention period and the applicable records controls schedule. If there is not a records schedule, the response should so indicate.

There is not yet an approved records control schedule authorizing the disposal of the electronic grants file on Grants Online. Pending the development and approval of a schedule by the National Archives and Records Administration, the electronic grants records must continue to retained.

Contact: Christopher Suzich, Project Manager
PH: (301) 444-2718 or chris.p.suzich@noaa.gov