

**U.S. Department of Commerce
National Oceanic and Atmospheric Administration (NOAA)**



**Privacy Impact Assessment
For the
NOAA Information Technology Center**

Reviewed by: _____, Bureau Chief Privacy Officer

- Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
 Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Date

**U.S. Department of Commerce Privacy Impact Assessment
NOAA/ Information Technology Center**

Unique Project Identifier: 006-48-01-01-01-3801-00

Introduction: System Description

The NOAA1101 environment consists of application software components that support the NOAA Commerce Business System (CBS), Grants Online (GOL), the Economic Development Administration's (EDA's) Revolving Loan Fund Management System (RLFMS) and Operations Planning and Control System (OPCS) and multiple administrative and management applications. Of these myriad applications in NOAA1101 only CBS and GOL, RLFMS and OPCS contain Personally Identifiable Information and Business Identifiable Information (PII/BII). CBS, formerly known as NOAA1001, supports the NOAA integrated financial management system for NOAA and the cross-serviced bureaus, EDA and Bureau of Industry and Security (BIS). No other DOC organizations obtain their Accounting Services from NOAA or have applications under this system.

This is a non-public system. Access to this application is through the NOAA1101 General Support Systems (GSS) environment which is limited to authorized NOAA, BIS, and EDA staff. CBS and the other applications listed above include the production, training, test and development environments within the NOAA Information Technology Center System. (NOAA1101 ITC).

CBS consists of the Core Financial System (CFS) interfaced with standard Commerce-wide administrative systems for procurement (C.Award), bankcard (Commerce Purchase Card System (CPCS)), travel (Integrated Travel Manager (ITM)), relocation (Permanent Change of Station (PCS) moves), time reporting and labor cost distribution, NOAA data warehouse (NDW), and System for Award Management (SAM).

CBS supports the financial functions required to track financial events, provide financial information important for the financial management of Commerce and its operating units, and required for the preparation of financial statements, and to allow Commerce to continue receiving clean financial audit opinions. NOAA CBS financial systems modules support: CFS, NOAA Permanent Change of Station (PCS - Relocation Manager), Travel Manager (TDY Travel), and other reporting activities (NOAA Data Warehouse) that are unique to NOAA. The NOAA CBS is hosted in the NOAA Information Technology Center (ITC). The ITC is operated by the Office of the Chief Information Officer/Information Security Management Office (OCIO/SDD) Financial and Administrative Computing Division (FACD).

Information is shared with U.S. Department of Treasury for purposes of payment and tax processing related to 1099s and W2 data for non-payroll related payments. Note: NOAA CBS does not process payroll, nor timecard data. WebTA is the DoC system for timecards and that

system provides data to USDA /NFC. USDA/NFC process payroll and provide tax related information to Treasury.

CBS enables Commerce and NOAA to meet the requirements of the Chief Financial Officers Act (CFOs Act) of 1990, P.L. 101-576; the Federal Managers' Financial Integrity Act of 1982, P.L. 97-255 (31 U.S.C. 3512 et seq.); and Office of Management and Budget (OMB) Circular A-127, Financial Management Systems. The authorities for these Systems of Records also apply:

COMMERCE/DEPT-1: Attendance, Leave, and Payroll Records of Employees and Certain Other Persons is an applicable SORN. Title 5 U.S.C., Title 31 U.S.C. 66a, 492, Title 44 U.S.C. 3101, 3309.

COMMERCE/DEPT-9: Travel Records (Domestic and Foreign) of Employees and Certain Other Persons. Budget and Accounting Act of 1921; Accounting and Auditing Act of 1950; and Federal Claim Collection Act of 1966.

COMMERCE/DEPT-2: Accounts Receivable. 5 U.S.C. 5701-09; 31 U.S.C. 951-953, 4 CFR 102.4, FPMR 101-7; Treasury Fiscal Requirements Manual.

The mission of the **GOL 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:

<http://www.corporateservices.noaa.gov/~grantsonline/index.html>. This is a non-public system.

NOAA GOL 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](http://www.grants.gov) is the single access point for over 1,000 grant programs offered by all federal grant-making agencies. GOL: 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. Award information is recorded in the U.S. Government's System for Award Management (SAM).

Information is received from Grants. Gov. Only staff who are reviewing grant applications have access to this information.

The statutory authority for the GOL is P.L. 106-107, the Federal Financial Assistance Management Improvement Act of 1999. It has expired, but is still in effect per the Grants Policy Committee (GPC), a committee of the U.S. Chief Financial Officers Council.

The RLFMS tracks Revolving Loan Fund (RLF) data. EDA issues funds to the RLF Operator (formally known as grantee). The RLF operator disburses money from the fund to small businesses or businesses that cannot otherwise borrow capital. The RLF Operators are non-profit

organizations that are in Economic Development Districts. These loans are provided at an interest rate that is at or below current market rate. As the loans are repaid, the RLF operator uses a portion of the interest earned to pay administrative expenses as well as replenish available capital for additional loans. *The RLF operator applies as a grantee, through Grants.gov; this information is downloaded by the 1101 system. The operator must report to NOAA1101 on the funds issued to small businesses or other businesses. The reports are submitted semi-annually via e-mail (the document is password protected with encryption) or via secure file transfer, and stored on the users' computers or the file share server provided by DOC Office of Secretary Network (OSNet). The reports contain PII and BII The semi-annual reports are converted from a PDF document to a .csv file and imported into the application.*

The **OPCS** is the EDA grant information, proposal processing and project tracking system. *The grant request forms are downloaded from Grants.gov.* The grant applications are reviewed to determine eligibility. Once the grant applicant is considered eligible, some of the information from the grant applications is entered in the OPCS application. This application consists of five (5) modules which are OPCS, Security, CBS Import, Federal Funding Accountability and Transparency Act (FFATA) and Congressional District Zip Codes. The OPCS module provides the capability to track the grant project from pre-application through approval to project closeout. OPCS combines proposal tracking documentation with a variety of other information about proposals, applications and approved projects, the areas in which they are located, and the proposed and actual impacts of such projects. The following are description of the supporting modules that are associated with OPCS:

SECURITY - System Security module grants appropriate access rights to groups of users and individual users based on login and password.

CBS Import – This module imports data from the NOAA CBS system. Files are manually exported from CBS and the module imports the required data for the OPCS database. The data that are tracked in OPCS are reservation, obligation, and disbursement.

FFATA - This module provides the capability to extract certain information from the OPCS database, allows the user to review the data for quality assurance, and provides the data in the format needed to meet the guidance provided by the Office of Management and Budget (OMB) for data submission to the USASpending web site under the Federal Financial Accountability and Transparency Act (FFATA).

Congressional District Zip Codes - This module provides the capability to upload the congressional district data.

The collection and maintenance of the PII and BII for the OPCS grants and RLFMS are authorized by the Public Works and Economic Development Act of 1965, as amended by the Economic Development Administration Reauthorization Act of 2004 (Pub. L. 108-373).

GOL, OPCS and RLFMS files are not retrieved by the name of an individual or by some other identifying particular assigned to the individual.

For both OPCS and RLFMS, the PII and BII are mainly data at rest. *The PII and BII data are accessed only by EDA authorized users and not shared outside the programs.*

Summary of information sharing for the four applications:

CBS: Information is shared with U.S. Department of Treasury for purposes of payment and tax processing related to 1099s and W2 data for non-payroll related payments.

GOL, RLFMS and OPCS: Information is received from Grants. Gov. Only staff who are reviewing grant applications have access to this information. The selected RLFMS operator submits reports to NOAA1101.

Role(s) of Contractors: Contractors may be performing any duties for which they have been cleared.

This is a moderate impact system.

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system

- This is a new information system.
 This is an existing information system with changes that create new privacy risks.
(Check all that apply.)

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify): Addition of two EDA applications					

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)					
a. Social Security*		e. File/Case ID		i. Credit Card	
b. Taxpayer ID	X	f. Driver's License		j. Financial Account	X
c. Employer ID		g. Passport		k. Financial Transaction	
d. Employee ID		h. Alien Registration		l. Vehicle Identifier	
m. Other identifying numbers (specify):					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form:					

General Personal Data (GPD)					
a. Name	X	g. Date of Birth	X	m. Religion	
b. Maiden Name		h. Place of Birth	X	n. Financial Information	X
c. Alias		i. Home Address	X	o. Medical Information	
d. Gender		j. Telephone Number		p. Military Service	
e. Age		k. Email Address	X	q. Physical Characteristics	
f. Race/Ethnicity		l. Education		r. Mother's Maiden Name	
s. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation		d. Telephone Number	X	g. Salary	
b. Job Title	X	e. Email Address	X	h. Work History	
c. Work Address	X	f. Business Associates			
i. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		d. Photographs		g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	
j. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
--	--	--	--	--	--

a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	
b. IP Address		d. Queries Run		f. Contents of Files	
g. Other system administration/audit data (specify):					

Other Information (specify)

2.2 Indicate sources of the PII/BII in the system. (Check all that apply.)

Directly from Individual about Whom the Information Pertains					
In Person		Hard Copy: Mail/Fax	X	Online	X
Telephone		Email	X		
Other (specify):					

Government Sources					
Within the Bureau	X	Other DOC Bureaus		Other Federal Agencies	X
State, Local, Tribal		Foreign			
Other (specify)					

Non-government Sources – Loan or grant applicants					
Public Organizations	X	Private Sector	X	Commercial Data Brokers	
Third Party Website or Application					
Other (specify):					

2.3 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. (Check all that apply.)

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)					
Smart Cards		Biometrics			
Caller-ID		Personal Identity Verification (PIV) Cards			
Other (specify):					

X	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.
---	--

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

X	There are not any IT system supported activities which raise privacy risks/concerns.
---	--

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
To determine eligibility		For administering human resources programs	
For administrative matters	X	To promote information sharing initiatives	
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify): 1) Payment processing via Treasury Financial Management System, Internal Revenue Service 1099 / W2 processing.			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

The CBS information is used to support the administrative and financial management requirements of NOAA, including, but not limited to, making payments to employees and vendors (members of the public). The information is used to ensure that financial transactions are conducted in a timely and correct manner, to protect against fraudulent transactions, and to generate and maintain financial management data adequate to meet acceptable accounting and auditing standards. Entitlement determination (in support of employee relocation / Permanent Change of Station (PCS)) and tax processing also require this information. The PII identified is for federal employees. BII is required for companies providing services to NOAA for payment processing via U.S. Department of Treasury.

The GOL information is used for verification of applicants' identity and capabilities so that effective grant-making and tracking of awardees' progress can occur. The PII collected is for applicants and awardees who are primarily members of the public, including those associated with academic institutions.

The PII and BII for OPCS is collected by the Grants.gov system. The forms are downloaded from Grants.gov. The required data are manually entered into OPCS by EDA users. Only the eligible grant applicant information is entered into OPCS. The information is collected and used to ensure that financial transactions are conducted in a timely and correct manner, to protect against fraudulent transactions. Information collected is from members of the public.

The PII in RLFMS is collected from the RLF operators that have been awarded the RLF grant and from businesses that apply for and have been awarded RLF loan. The BII data are from businesses that apply for and have been awarded RLF loan. The information collected from the RLF Operator is contained in the grant request and the required program semi-annual report. Information is used to determine grant awards and to determine that the grant is being managed properly. Information is collected from members of the public.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau			X
DOC bureaus			
Federal agencies (Treasury)			X
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

	The PII/BII in the system will not be shared.
--	---

6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

X	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage: GOL, RLFMS and OPCS receive information from Grants.gov. Only cleared authorized users approved to receive HSPD-12/CAC cards gain access to PII/BII data; this helps to prevent leakage.
	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.3 Identify the class of users who will have access to the IT system and the PII/BII. (*Check all that apply.*)

Class of Users			
General Public		Government Employees	X
Contractors	X		
Other (specify):			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII 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.
X	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: http://www.noaa.gov/protecting-your-privacy _____.

X	Yes, notice is provided by other means.	<p>Specify how:</p> <p>1) CBS - Information for personnel, and tax transactions and reports is provided to the employee when they are given the W-4 to complete. Also, general notice for other uses of CBS is provided in the Internal Revenue Code sections 3402(f)(2) and 6109: "Internal Revenue Code sections 3402(f)(2) and 6109 and their regulations require you to provide this information; your employer uses it to determine your federal income tax withholding." <i>The code references are included in the CBS training required for all users.</i></p> <p>2) GOL, OPCS and RLFMS – A specific Grants. Gov notice is given in a privacy link on the initial screen of Grants.gov, as part of the Grant application process. Also, on this page: http://www.grants.gov/web/grants/applicants/organization-registration.html, notice is given to organizations that they must provide an Employer ID Number.</p> <p><i>The notices are attached at the end of this PIA, before the signature page.</i></p>
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

X	Yes, individuals have an opportunity to decline to provide PII/BII.	<p>Specify how:</p> <p>CBS - Employees may refuse to provide information, either verbally or in writing, to their HR contacts, but this information is required data as part of their employment, for processing payroll and tax forms.</p> <p>GOL - Grantees may choose not complete required fields, but this will prevent consideration of their applications. Grantees are not required to enter taxpayer ID or DUNS numbers (the fields are not marked as required).</p> <p>OPCS - The individual may decline to provide the data on the Grants.gov forms, by not completing the</p>
---	---	---

		<p>fields. However, the individual must provide information on the form in order for the grant request to be processed.</p> <p>RLFMS – RLF Operators may decline by not submitting a report, but they would not meet the reporting requirement and would be considered delinquent in this requirement.</p>
	No, individuals do not have an opportunity to decline to provide PII/BII.	

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

X	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	<p>Specify how:</p> <p>CBS - Employees may decline, in writing to their supervisors, consent to the use of their PII for payroll and taxes but the CBS – Treasury Fiscal Requirements Manual states that applicable information is required for processing payments.</p> <p>GOL/OPCS – When an individual or entity completes an application, he/she effectively gives consent for PII/BII to be used to determine whether he/she qualifies for a grant. There are no other uses for this information than the application itself.</p> <p>RLFMS - When an entity completes an application, consent is effectively given for PII/BII to be used to determine whether he/she qualifies for a loan. There are no other uses for this information.</p>
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

X	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	<p>Specify how:</p> <p>CBS - Employees may review/update information on their Employee Personal Page via the National Finance Center, while vendors can access the SAM to</p>
---	---	---

		<p>update their data, which then flows into CBS.</p> <p>GOL - Applicants enter all PII at the time of completing the Grant application and it can be modified by contacting the GOL Help Desk which verifies updates against the SAM before making the update in GOL.</p> <p>RLFMS: The BII and PII is accessed and updated via the RLF program reporting process which is semi-annual. The RLF Operator submits updates for the semi-annual report and can change the information at that time.</p> <p>OPCS: The grantee must contact the EDA point of contact to update the information.</p>
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. (*Check all that apply.*)

X	All users signed a confidentiality agreement or non-disclosure agreement. (EDA systems, contractors only)
X	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
X	Access to the PII/BII is restricted to authorized personnel only.
X	<p>Access to the PII/BII is being monitored, tracked, or recorded.</p> <p>Explanation: NOAA ITC System Administrators identify the various logs on each supported system or devices that require monitoring to identify any security incidents as identified in ITC-SA-03 System Monitoring and Security Policy. The administrator implements automated alert monitoring tools that are set to send email alerts so the responsible administrator is notified of the problem immediately. Auditable events include logon (successful and failed), remote connections, audit log failures, and access violations at a minimum.</p>
X	<p>The information is secured in accordance with FISMA requirements.</p> <p>Provide date of most recent Assessment and Authorization (A&A): 6/30/2015</p> <p><input type="checkbox"/> This is a new system. The A&A date will be provided when the A&A package is</p>

	approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended privacy controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POAM).
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish ownership rights over data including PII/BII.
X	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system.

Access controls for authorized users are implemented on production systems through the use of the Common Access card, unique system usernames and passwords as well as database (application) usernames and passwords to authenticate each user. NIST SP 800-53 revision 4 access controls are enforced for access to all applications. User accounts are obtained through the application account managers. Upon log-in the user is prompted to change his/her initially assigned password. For system accounts, the user is required to contact the ITC account managers to receive his or her initial password.

Currently, all individuals at NOAA and the various NOAA centers utilizing NOAA subsystems are in possession of a Homeland Security Presidential Directive 12 (HSPD-12) compliant NOAA Identification Card. This verification of personal information is utilized to generate and validate via the HSPD-12 chip used in each card. HSPD-12 cards/Common Access Cards (CACs) are manufactured for individuals whose personal information has been validated by a background investigation conducted by the NOAA Office of Security Division. CAC readers are installed on all Corporate Services Local Area Network (CORPSRV) domain member workstations and servers. All ITC support personnel have valid CACs and are required to utilize the CACs as part of the two-factor authentication to access CORPSRV domain workstations and servers.

This process is also additionally supplemented by two factor authentications utilizing the Virtual Private Network (VPN) Server, RSA* tokens and other factors for remote administration and log on. At this point in time, all NOAA systems utilized are in process of being provided card readers for the HSPD-12 compliant ID Cards.

Users or processes acting on behalf of users are uniquely identified through user accounts. Password authentication is in place and required for all user accounts, applications, and system access. This level of authentication meets NIST Special Publication 800-63 guidance. Passwords must adhere to current NOAA guidelines (minimum length, aging, history, combination of character types, etc.) before access is granted.

Access logs are kept and reviewed for any anomalies.

CBS data is encrypted at rest, in an Oracle Table Space.

*This is a brand, not an acronym.

Section 9: Privacy Act

9.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. (A new system of records notice (SORN) is required if the system is not covered by an existing SORN).

As per the Privacy Act of 1974, “the term ‘system of records’ means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.”

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name and number (<i>list all that apply</i>): COMMERCE/DEPT-1: Attendance, Leave, and Payroll Records of Employees and Certain Other Persons; COMMERCE/DEPT-2: Accounts Receivable; COMMERCE/DEPT-9: Travel Records (Domestic and Foreign) of Employees and Certain Other Persons.
	Yes, a SORN has been submitted to the Department for approval on <u>(date)</u> .
	No, a SORN is not being created.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. (*Check all that apply.*)

X	There is an approved record control schedule. Provide the name of the record control schedule: CBS: NOAA Records Management Handbook Chapter 400, specifically Section 404-11 Accounting Files. OPCS and RLFMS -The General Record Retention schedule is used. For BII and PII, the record control schedule is EDA DAA-0378-2014-0413.
X	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule: GOL: A records control schedule will be developed and submitted to NARA for approval. Pending the development and approval of a schedule by the

	National Archives and Records Administration, the electronic grants records must continue to be retained.
X	Yes, retention is monitored for compliance to the schedule.
X	No, retention is not monitored for compliance to the schedule. Provide explanation: GOL does not yet have a records schedule.

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding	X	Overwriting	
Degaussing	X	Deleting	X
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Levels - NEW

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed.

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
X	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels. *(Check all that apply.)*

X	Identifiability	Provide explanation: CBS collects personal information for employees, vendors, and customers. GOL collects personal information from customers.
X	Quantity of PII	Provide explanation: CBS collects a moderate amount of PII.

		The OPCS and RLFMS applications include a few PII data fields.
X	Data Field Sensitivity	Provide explanation: CBS contains sensitive PII and BII. The OPCS and RLFMS applications contain sensitive BII.
X	Context of Use	Provide explanation: CBS uses PII to support payment processing and tax reporting. GOL uses PII to assist with determining an applicant's financial integrity.
	Obligation to Protect Confidentiality	Provide explanation:
	Access to and Location of PII	Provide explanation:
	Other:	Provide explanation:

Section 12: Analysis

12.1 Indicate whether the conduct of this PIA results in any required business process changes.

x	Yes, the conduct of this PIA results in required business process changes. Explanation: Encryption of non-CBS data.
	No, the conduct of this PIA does not result in any required business process changes.

12.2 Indicate whether the conduct of this PIA results in any required technology changes.

x	Yes, the conduct of this PIA results in required technology changes. Explanation: Encryption of non-CBS data.
	No, the conduct of this PIA does not result in any required technology changes.

GRANTS.GOV PRIVACY POLICY

Please Review our Privacy Policy for Your Protection

Thank you for visiting Grants.gov and reviewing our privacy and security policy. The Grants.gov privacy policy protects the rights of individual users under section [552a of title 5, United States Code](#) (commonly referred to as the "Privacy Act"), and other laws relevant to the protection of the privacy of an individual. All information is gathered, stored, and used in accordance with the above-mentioned Privacy Act.

NOTE: Our privacy and security policy is clear: *We will collect no personal information about you when you visit our website unless you choose to provide that information to us.*

Information Collected and Stored Automatically

Grants.gov does not require a user to submit information to browse the Grants.gov site. The only users who are required to submit contact information are those users who wish to be authorized submitters on behalf of their organization, or users who wish to receive information directly from Grants.gov.

Grants.gov collects personal information about you (e.g., name, email address, phone number, title, username) only if you specifically and knowingly give it to us. If you consent to provide us with personal information (by providing feedback or by asking a question), we use that information to respond to your message and to help us get you the information you have requested. We only share the information you give us with other government agencies if your inquiry relates to that agency, or as otherwise required by law. Moreover, we do not create individual profiles with the information you provide or give it to any private organizations. We do not collect information for commercial marketing.

Grants.gov collects information to allow access for two types of users:

- Agency Users
- Authorized Organization Representatives

NOTE: All information collected and stored is in compliance with the [Paperwork Reduction Act](#). Any information submitted to Grants.gov through the application process will be stored in the Grants.gov system for a period of six months. Additionally, no one from Grants.gov will ever ask you for personal information, such as your Social Security number, banking, or credit card information.

When you browse, read pages or download information on Grants.gov, we automatically gather and store certain technical information about your visit. This information never identifies who you are. The information we collect and store about your visit is listed below:

- The Internet domain (e.g., "xcompany.com" if you use a private Internet access account, or "yourschool.edu" if you connect from a university's domain) and IP address (an IP address is a number that is automatically assigned to your computer whenever you are surfing the Web) from which you access our website;
- The type of browser (e.g., Firefox, Internet Explorer) and operating system (e.g., Windows, OS X) used to access our website;
- The date and time you access our website;
- The pages you visit; and,
- If you clicked on a link to the Grants.gov website from another website, the address of the website.

This information is only used to help us make the site more useful for you. With this data we learn about the number of visitors to our site and the types of technology our visitors use. We never track or record information about individuals and their visits.

Site Security

For site security purposes and to ensure that this service remains available to all users, this government computer system is housed in a secure government facility and employs commercial software programs to monitor network traffic to identify unauthorized attempts to upload, view, change information, or otherwise cause damage.

Except for authorized law enforcement investigations, no other attempts are made to identify individual users or their usage habits. Unauthorized attempts to upload, view, or change information on this site are strictly prohibited and may be punishable under the Computer Fraud and Abuse Act of 1986 and the National Information Infrastructure Protection Act.

Links to Other Sites

This website has links to other websites. When you click on one of these links to another site, you are subject to the privacy policy of the new site. These webpages are provided as a tool to help visitors explore the wide range of options and information available, and to help them make informed choices about how to prepare for and pursue grant application opportunities. As such, the organization, services, advice, or products are not endorsed or guaranteed in any way by Grants.gov and are entirely the responsibility of the sponsor of the site visited.

Cookies

To use this website, you must enable cookies support in your web browser. Cookies will only be used for the duration of the individual session to allow you easy navigation within the website. A cookie is a small piece of information that is sent to your browser, along with a webpage, when you access a website. There are two kinds of cookies. A session cookie is a line of text that is stored temporarily in your computer's RAM. Because a session cookie is never written to a drive, it is destroyed as soon as you close your browser. A persistent cookie is a more permanent line of text that gets saved by your browser to a file on your hard drive. Depending on your browser settings, you may receive notification that a given site is requesting cookie information, possibly with an expiration date. Persistent cookies have an expiration date in the future. Session cookies have no date associated with them. The Grants.gov website will create a session cookie whenever you access the website. The session cookie is automatically destroyed as soon as you close your browser. We do not create any persistent cookies.

Unsubscribe

NOTE: If you choose to unsubscribe from Grants.gov email notifications, please click [Unsubscribe from Grant Notices](#) and submit your email address. For further assistance please [contact Grants.gov](#).

Grants.gov Registering as an Organization Applicant


Before applying for a funding opportunity, you need to register as an applicant associated with an organization. Registering with Grants.gov allows you to create an account and connect it with the organization you either work for or otherwise contribute to their grant applications.

Registering as an organization applicant submits a request to your organization's EBiz POC for Grants.gov roles. One of these roles is the Authorized Organization Representative (AOR) role, which, if authorized to you, allows you to submit applications on behalf of your organization. An organization is an entity that submits grant applications on behalf of the group, such as a state government, nonprofit organization, or a private business. Registering as an organization applicant has five main steps. Below is an overview of the registration process. Click one of the steps to view more detailed instructions.

Please make sure to begin registration early, as the process takes between three business days and three weeks. If you do not complete your registration by the submission deadline, then you are unlikely to be allowed to submit an application. You should contact the agency point of contact listed on the grant opportunity to discuss that agency's policy.

1. Obtain a DUNS Number

How do I get a DUNS number?

Call 1-866-705-5711 or access the Dun & Bradstreet website <http://fedgov.dnb.com/webform>.

→ **How long does this step usually take?**

1-2 business days

2. Register with SAM

How do I register with the System Award Management (SAM)?

Access <https://www.sam.gov>. You will also need the authorizing official of your organization and an Employer Identification Number (EIN).

→ **How long does this step usually take?**

7-10 business days (2 more weeks to acquire an EIN)

Points of Contact and Signatures

<p>Information System Security Officer or System Owner Name: Office: Phone: Email:</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p>Signature: _____</p> <p>Date signed: _____</p>	<p>Information Technology Security Officer Name: Office: Phone: Email:</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p>Signature: _____</p> <p>Date signed: _____</p>
<p>Authorizing Official - NEW Name: Office: Phone: Email:</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p>Signature: _____</p> <p>Date signed: _____</p>	<p>Bureau Chief Privacy Officer (NOAA) Name: Office: Phone: Email:</p> <p>I certify that the PII/BII processed in this IT system is necessary, this PIA ensures compliance with DOC policy to protect privacy, and the Bureau/OU Privacy Act Officer concurs with the SORNs and authorities cited.</p> <p>Signature: _____</p> <p>Date signed: _____</p>

<p>Bureau Chief Privacy Officer (EDA) Name: Office: Phone: Email:</p> <p>I certify that the PII/BII processed in this IT system is necessary, this PIA ensures compliance with DOC policy to protect privacy, and the Bureau/OU Privacy Act Officer concurs with the SORNs and authorities cited.</p> <p>Signature: _____</p> <p>Date signed: _____</p>	
--	--

This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to publication of the PI