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

Privacy Impact Assessment
For the
NOAA Information Technology Center (ITC)
[NOAA1101]

Reviewed by:

Mark Graff

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

MICHAEL TOLAND

Digitally signed by MICHAEL TOLAND
DN: c=US, o=U.S. Government, ou=Department of Commerce, ou=Office of the Secretary, cn=MICHAEL TOLAND, 0.9.2342.19200300.100.1.1=13001000249566
Date: 2017.07.06 07:44:36 -04'00'

for Catrina Purvis 7/6/17

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

[PAGE INTENTIONALLY BLANK]

NOAA Information Technology Center (ITC) [NOAA1101]
Privacy Impact Assessment

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

Introduction: System Description

NOAA1101

The **NOAA1101** General Support System (GSS) is an interconnected set of information resources under the management and control of Service Delivery Division (SDD) within the NOAA Office of the Chief Information Officer (CIO). The NOAA1101 GSS includes hardware, software, information, data, applications, communications, facilities, and people.

NOAA1101 provides Infrastructure As A Service (IAAS), Data Center colocation, Application Support services that are instrumental to obtaining the objectives of the President's Management Agenda; achieving the goals of the Office of Management and Budget for effective and efficient government; and NOAA's goal for excellence in the technical operational support of NOAA's financial, management, and administrative systems. Support activities of the GSS include direct, technical, and operational support of financial and administrative systems.

In general, the NOAA1101 GSS boundary encompasses the NOAA instance of Commerce Business System (CBS), including the CBS Major Application, formerly NOAA1001; CBS Support Systems, formerly NOAA1000; Grants Online (GOL), formerly NOAA1105; the Economic Development Administration's (EDA's) Revolving Loan Fund Management System (RLFMS) and Operations Planning and Control System (OPCS); and a myriad of other administrative and management applications. The CBS and GOL systems are separately documented as subsystems within NOAA1101 and are identified as FISMA children of the GSS.

The NOAA1101 GSS has been identified as a High Value Asset by the DOC Office of Cyber Security due to the Critical Systems Management Information it contains. The operational support of these systems is a critical factor in the functionality and benefit of these systems to NOAA employees and consequently to the achievement of NOAA's mission.

NOAA1101 NOTE: ONLY CBS and GOL, RLFMS and OPCS contain Personally Identifiable Information and Business Identifiable Information (PII/BII).

NOAA1101 is a FISMA MODERATE system.

For any system, contractors may be performing duties for which they have been cleared.

Commerce Business System (CBS)

CBS, formerly NOAA1001, 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 NOAA integrated financial management system for NOAA and 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.

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/Service Delivery Division (OCIO/SDD) Service Delivery and Hosting Services (SDHSB).

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:

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.

Grants OnLine (GOL)

The GOL Program Management Office (PMO) provides 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 Website. This is a non-public system.

PMO Website: http://www.corporateservices.noaa.gov/~grantsonline/index.html.

NOAA **Grants OnLine** (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 is the single access point for over 1,000 grant programs offered by all federal grant-making agencies.

GOL does the following:

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).

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.

Only staff who are reviewing grant applications have access to this information.

Revolving Loan Fund Management System (RLFMS)

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.

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.

The collection and maintenance of the PII and BII is 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).

Contractors may be performing any duties for which they have been cleared.

Operations Planning and Control System (OPCS)

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.

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.

The collection and maintenance of the PII and BII is 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).

Contractors may be performing any duties for which they have been cleared.

[PAGE INTENTIONALLY BLANK]

Section 1: Status of the Information System

1.1. New or Existing System

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.

[X] This is an existing information system with no 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):		

Section 2: Information in the System

2.1. Privacy Information Collected

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*	X	e. File/Case ID		i. Credit Card	
b. Taxpayer ID	X	f. Driver's License		j. Financial Account	X
c. Employer ID	X	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 SSN, including truncated form:**
Financial account information and grant/loan applications require Tax ID Numbers. These could be either SSNs or EINs. In some cases, in NOAA1101, the Tax ID is an SSN.

AUTHORITIES: FFATA; Federal Managers' Financial Integrity Act of 1982; Federal Financial Assistance Management Improvement Act of 1999; 16 USC 6109(a)(4), 3402; 8 USC 1324a; 41 CFR 60-4.3, E.O. 11246.

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	X
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):					

2.2. PII and BII Sources

Indicate sources of the PII/BII in the system.

(Check all that apply.)

Directly from an 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	X	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. Technologies that Contain PII

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 no technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

3.1. Activities that raise Privacy Concerns

Indicate IT system 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. Why information is Collected

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)	
Details: 1. Payment processing via Treasury Financial Management System 2. Internal Revenue Service 1099 / W2 processing. 3. Loan administration. 4. Grant administration.			

Section 5: Use of the Information

5.1. How Information is Collected

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).

CBS
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.

GOL
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.

OPCS
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.

RLFMS
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.

There is no computer matching used for any of these applications.

Section 6: Information Sharing and Access

6.1. Sharing Information

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			X
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. Sending and Receiving Information

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 system connects with or receives information from another system authorized to process PII/BII.

Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:

CBS
For purposes of payment and tax processing related to 1099s and W2 data for non-payroll related payments. NOAA CBS does not process payroll, or 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 connects to and transfers data between the US Department of Treasury, Bureau of Fiscal Service.
An encrypted VPN tunnel using AES-256 encryption is used to connect the NOAA1101 system to the Bureau of Fiscal Service and protect the PII/BII data.

GOL
DOWNLOAD information from Grants.gov.
Only cleared authorized users can gain access to PII/BII data; this helps to prevent leakage.
This information is secured using SHA-2 Certificates and TLS v1.2.

OPCS
DOWNLOAD information from Grants.gov.
Only cleared authorized users can gain access to PII/BII data; this helps to prevent leakage.
This information is secured using SHA-2 Certificates and TLS v1.2.

[ ] **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. Access to Information

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. Notifications of Disclosure

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.	**Where is it:** The Privacy Act statement and/or privacy policy for Grants on Line can be found at: https://grantsonline.rdc.noaa.gov.
[X] Yes, notice is provided by other means.	**Specify how:** **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." *The code references are included in the CBS training required for all users.* **GOL** 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 (EIN). A GOL privacy act statement is also provided here: http://www.corporateservices.noaa.gov/grantsonline/pdfs/Grants_Online_Privacy_Act_Statement.pdf **OPCS** 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 (EIN).
[ ] No, notice is not provided.	**Specify why not:**

7.2. Opportunity to Decline

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.	**Specify how:** **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. **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). **OPCS** The individual may decline to provide the data on the Grants.gov forms, by not completing the fields. However, the individual must provide information on the form in order for the grant request to be processed. **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.
[ ] No, individuals do not have an opportunity to decline to provide PII/BII.	**Specify why not:**

7.3. Consent to Use

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

[X] Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	**Specify how:** **CBS** Employees may decline, in writing to their supervisors, 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. **GOL** When an individual or entity completes an application, he/she effectively gives consent for it to be used to determine whether he/she qualifies for a grant. There are no other uses for this information than the application itself. **OPCS** When an individual or entity completes an application, he/she effectively gives consent for it to be used to determine whether he/she qualifies for a grant. There are no other uses for this information than the application itself. **RLFMS** When an entity completes an application, he/she effectively gives consent for it to be used to determine whether he/she qualifies for a loan. There are no other uses for this information.
[ ] No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	**Specify why not:**

7.4. Opportunity to Review/Update

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.	**Specify how:** **CBS** Employees may review/update information on their Employee Personal Page via the National Finance Center, while vendors can access the SAM to update their data, which then flows into CBS. **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. **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. **OPCS** The grantee must contact the EDA point of contact to update the information.
[ ] 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. Controls

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] Access to the PII/BII is being monitored, tracked, or recorded.

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-IR-01 NOAA ITC Incident Response Policy, and ITC-AU-01 NOAA ITC Auditing 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.

[X] The information is secured in accordance with FISMA requirements.

Provide date of most recent Assessment and Authorization (A&A): 6/15/2017

-OR-

[ ] This is a new system. The A&A date will be provided when the A&A package is 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. Protection of Privacy Data

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 the Common Access card, unique system usernames and passwords as well as database (application) usernames and passwords to authenticate each user. NOAA 800-53 rev 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. System of Record Notice (SORN)

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 *(list all that 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.
OPM GOVT-1:	General Personal Records. 5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347, and Executive Order 9397 as amended by E.O.13478, E.O 9830, and E.O. 12107,

[ ] Yes, a SORN has been submitted to the Department for approval on (date).

[ ] No, a SORN is not being created.

Section 10: Retention of Information

10.1. Records Control Schedule

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:
For GOL, a records control schedule will be developed and submitted to NARA for approval. Pending the development and approval of a schedule by NARA, 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. Disposal

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 SP 800-122 PII Confidentiality Impact Levels [NEW]

11.1. Impact of Disclosure

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.

☐ **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. Determination Factors

Indicate which factors were used to determine the above PII confidentiality impact levels.

(Check all that apply.)

☒ **Identifiability**	**Provide explanation:** CBS collects personal information for employees, vendors, and customers. GOL collects personal information from customers.
☒ **Quantity of PII**	**Provide explanation:** CBS collects a moderate amount of PII. The OPCS and RLFMS applications include a few PII data fields.
☒ **Data Field Sensitivity**	**Provide explanation:** CBS contains sensitive PII and BII. The OPCS and RLFMS applications contain sensitive BII.
☒ **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 Business Process Changes

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

☐ Yes, the conduct of this PIA results in required business process changes.

☒ No, the conduct of this PIA does not result in any required business process changes.

12.2 Technology Changes

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

☐ Yes, the conduct of this PIA results in required technology changes.

☒ No, the conduct of this PIA does not result in any required technology changes.