

U.S. Department of Commerce
National Oceanic and Atmospheric Administration
Office of the Chief Information Officer



Privacy Impact Assessment
CORPORATE SERVICES
LOCAL AREA NETWORK
NOAA1200

Reviewed by: _____, Bureau Privacy Officer or Designee

Approved by: , DOC Chief Privacy Officer

Date approved: 12/15/2014

**U.S. Department of Commerce Privacy Impact Assessment
National Oceanic and Atmospheric Administration (NOAA)
Office of the Chief Information Officer (OCIO)
Corporate Services Local Area Network
(CORP SRV LAN)**

Unique Project Identifier: 006-000351100 00-48-02-00-01-00

Introduction: System Description

CORPSRV LAN, NOAA1200, is a General Support System consisting of Windows file and print servers, desktop and laptop user workstations, network infrastructure components that support NOAA's executive offices and corporate financial and administrative services Program Support Units located at twelve sites across the country: Silver Spring, MD (1) Headquarters (HQ) and 2) HQ/Commissioned Personnel Center; 3) Germantown, MD; 4) Washington, DC; 5) Norfolk, VA; 6) Kansas City, MO; 7) Boulder, CO; 8) Newport, OR; 9) Tampa, FL; 10) Seattle, WA; 11) Fairmont, WV; and 12) Largo, MD.

All sites are bound under an active directory domain structure (CorpSrv.NOAA.local). NOAA1200 supports a user base of approximately 1,700 users.

System Purpose - NOAA1200 provides connectivity to the NOAA network for both local and remote access to the following basic administrative services: file, print, and communication sharing; file backup and restoration; account management and storage. In addition, NOAA1200 provides support for desktops, laptops and servers.

Statutory authorities:

5 U.S.C 301

National Marine Sanctuaries Amendments Act of 2000 (Public Law 106-513 Section 318)
America Creating Opportunities to Meaningfully Promote Excellence in Technology, Education, and Science (COMPETES) Act (Public Law 110-69, Section 4002).

This system has a moderate impact level.

See the table on the follow page for information on sharing.

System Sharing – All users of these systems are internal to the system owner’s organization. No information is shared outside the bureau.

Business Function	Application/Resource	Type of PII	Comments
AGO (Acquisition and Grants Office)	Procurement, Grants, and Contract Data; N: Drive	Date of Birth (DOB); Address; Social Security number (SSN)	Applications, Grant, Vendor and procurement information.
CAO - SECO (Office of the Chief Administrator - Safety and Environmental Compliance Office)	Local disk; \\hq5-is-fsvr1\dcao budget; SharePoint: Google: Drive	Personal information, i.e., name, address, DOB, SSN on DD-214, SF-50; employment documents	Resumes, transcripts, employment documents; Accident/Incident reports; Passport Applications
CAO – CivRights (Office of Civil Rights)	NOAA Complaints of Discrimination; NOAA Demographic Data Reports; Complaint Investigator Reports; Civil Rights Office Personnel Information; Internally generated reports and databases	Name; address; SSN; age; race; national origin; disability; gender, religion; performance evaluation; etc.	
CAO – BAIPS (Business Analysis & Investment Planning Staff)	Local disk; \\hq5-is-fsvr1\dcao budget; SharePoint: Google: Drive	Names & Employee Salary Information	
OCIO (Office of the Chief Information Officer)	Performance Reviews, SF-52, Telework Applications, SF-182, CD-137, CD-505, OGE 450 Financial Disclosure Reports, Various applications in GTOWN	Ratings, DOB, Addresses, SSN	Applications: NRS, Clearance Data, CAC, Epledge, NFC, COD, NOAA CORPS Payroll, POL/SF113, HR Reports, CAMS/BXA/Labor
EPP/OED (Educational Partnership Program-Office of Education)	Scholarship Applications on N: Drive	Address, DOB, School & Other PII	
Security	C-Cure	SSN	SSN used for identity check
	M: Drive (shared drive for each division)	DOB, Place of Birth (POB), SSN, FBI Name Checks and arrest records, foreign travel forms	
WFMO (Workforce Management Office)	SharePoint Site	Address, Phone Numbers, SSN, User ID, DOB, Passcodes	Resumes, hiring letters, insurance forms, eOPF documents
PPI (Planning, Policy and Integration)	N: Drive	SSN, DOB, POB	Personnel actions, CAC documents, Equipment and badging information
DUS (Department of Undersecretary, CROM (Chief, Resource & Operations Management), EXSEC (Office of the Executive Secretary)	N: Drive	Personal information, i.e., name, address, DOB, SSN on DD-214, SF-50; employment documents	Resumes, transcripts, employment documents; Accident/Incident Reports; Passport Applications
GC (General Counsel)	N: Drive	DOB, POB, SSN	Security Cover Sheets
CFO (Office of the Chief Financial Officer)	CBS vendor, grant conversion/issue resolution, internal and external data call support	Taxpayer Identification Number (TIN), ABA number, SSN, DOB, bank information	Most files are Secure Zipped, Encrypted, and password protected
GC – SSMC (Silver Spring Metropolitan Campus)	N: and C: Drives	SF-50s, OPFs with DOBs and SSN	

NOTE Re shared drives: Access controls are applied to all systems and applications per DOC CITR-022 Access and Use Policy, NOAA Rules of Behavior, and NOAA IT Security Manual Section 16.0 Access Controls.

Section 1: Information in the System

1.1 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*	X	e. Alien Registration		i. Financial Account	X
b. Taxpayer ID	X	f. Driver's License		j. Financial Transaction	X
c. Employee ID	X	g. Passport	X	k. Vehicle Identifier	
d. File/Case ID	X	h. Credit Card		l. Employer ID Number	X
m. Other identifying numbers (specify): *Storage is not duplicative among hosted offices; Workforce management, financial, and security collect and store SSNs from different populations: employees, contractors, non-NOAA					

General Personal Data (GPD)					
a. Name	X	g. Date of Birth	X	m. Religion	X
b. Maiden Name	X	h. Place of Birth	X	n. Financial Information	X
c. Alias	X	i. Home Address	X	o. Medical Information	X
d. Gender	X	j. Telephone Number	X	p. Military Service	X
e. Age	X	k. Email Address	X	q. Physical Characteristics	
f. Race/Ethnicity	X	l. Education	X	r. Mother's Maiden Name	
s. Other general personal data (specify): Education level, school transcripts, field of study, references, performance measure results while in scholarship program, and postgraduate activities, national origin, disability.					

Work-Related Data (WRD)					
a. Occupation	X	d. Telephone Number	X	g. Salary	X
b. Job Title	X	e. Email Address	X	h. Work History	X
c. Work Address	X	f. Business Associates			
i. Other work-related data (specify): Performance information, FBI Name Checks and arrest records, foreign travel forms, accident/incident reports.					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints	X	d. Photographs	X	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	X
b. IP Address	X	d. Queries Run	X	f. Contents of Files	
g. Other system administration/audit data (specify): Passcodes					

Other Information (specify)

1.2 Indicate sources of the PII/BII in the system. Check all that apply.

Directly from Individual about Whom the Information Pertains					
In Person	X	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					
Public Organizations		Public Media, Internet		Private Sector	
Commercial Data Brokers					
Other (specify):					

Section 2: Purpose of the System

2.1 Indicate why the PII/BII in the system is being collected, maintained, or disseminated. Check all that apply.

Purpose			
To determine eligibility	X	For administering human resources programs	X
For administrative matters	X	To promote information sharing initiatives	
For litigation	X	For criminal law enforcement activities	
For civil enforcement activities	X	For intelligence activities	
Other (specify): Financial	X	Other: Education/training	X

Section 3: Use of the System

3.1 Provide an explanation of how the bureau will use the PII/BII to accomplish the checked purpose(s), e.g., to verify existing data. Describe why the PII/BII that is collected, maintained, or disseminated is necessary to accomplish the checked purpose(s) and further the mission of the bureau and/or the Department. Indicate if the PII/BII identified in Section 1.1 of this document is in reference to a federal employee/contractor, member of public, foreign national, visitor or other (specify).

1. Names, addresses, e-mail addresses, age, race, national origin, disability, gender, maiden name, alias, SSNs, photographs, place of birth, and date of birth are collected and maintained to enable NOAA to identify to whom we are issuing a badge (employees and contractors).
2. Names, addresses, e-mail addresses, SSNs, place of birth and date of birth, photographs, fingerprints, FBI Name Checks and arrest records, foreign travel forms and passport numbers are used to create and support records for the submission of security investigations, for potential employees or contractors (members of the public).
3. Names, addresses, e-mail addresses, race, national origin, disability, gender, home phone number, education, medical information, military service, work history, email address, and SSNs are used for eligibility for hiring employees (members of the public).
4. Names, occupations, job titles, salaries and performance information are used to create and maintain federal employee performance reviews.
5. Names, addresses, e-mail addresses, age, race, religion, national origin, disability, gender, employee ID, employee case number and SSNs are collected for labor issues, civil enforcement activities and litigations (federal employees).
6. Names, addresses, age, financial account, financial transactions and SSNs are collected and maintained to facilitate payroll information and records (federal employees).
7. Names, addresses, e-mail addresses, age, race/ethnicity, gender, DOB, citizenship, education level, school transcripts, field of study, references, performance measure results while in program, and postgraduate activities are used to determine awards and track students in the (1) Office of Education, Educational Partnership Program; (2) Ernest F. Hollings Undergraduate Scholarship Program; (3) Dr. Nancy Foster Scholarship Program; and (4) National Marine Fisheries Service Recruitment, Training, and Research Program (members of the public).
8. User ID, IP Address, Date/Time of Access, Queries Run, ID Files Accessed and Passcodes are collected for system administration, including system security (federal employees).

Section 4: Information Sharing

4.1 Indicate with whom the bureau intends to share the PII/BII in the system and how the PII/BII will be shared.

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

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

Section 5: Notice and Consent

5.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. Check all that apply.

<input type="checkbox"/>	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 6.	
X	Yes, notice is provided by other means.	Specify how: Owners of the hosted systems send notifications to individuals when information is required. For scholarship applicants, scholarship awardees and grantees, notice is given on the Web site and on the application and tracking forms, regarding the purposes and uses of the information given, along with both security and privacy notices.
<input type="checkbox"/>	No, notice is not provided.	Specify why not:

5.2 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.	Specify how: On scholarship applications, not all information is required, and optional fields are marked as such. If required information is not given, applications will be declined. Members of the public may decline to provide PII/BII directly to the application owners; however, they cannot be employed by NOAA/receive applicable services. Federal employees and contractors may decline to provide the information, but must provide the information as a condition of employment. In general, information is required for the effective administration of the center, including continuity of operations in case of an emergency. Links to the NOAA privacy policy are provided to employees, contractors and members of the public.
---	---	--

	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:
--	---	------------------

5.3 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.	Specify how: Individuals are given an explanation in writing, on the applicable forms, from the application owners, as to why the required information must be provided (i.e. specific uses), as well as a link to the NOAA Privacy Policy. Per the privacy policy, completion of a form or otherwise providing the information implies consent to the particular uses of the information.
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

5.4 Indicate whether and how individuals have an opportunity to review/update PII/BII that pertains to them.

X	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	For scholarship programs, students may request to review their information from their supervisors and submit updates to them at any time. On the Web sites of all other hosted applications/offices, contact information for the staff office manager is given, with the stated purpose of requesting to review and update information.
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 6: Administrative and Technological Controls

6.1 Indicate the administrative and technological controls for the system. Check all that apply.

	All users signed a confidentiality agreement.
X	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	Staff received training on privacy and confidentiality policies and practices.
X	Access to PII/BII is restricted to authorized personnel only.
X	The information is secured in accordance with FISMA requirements. The most recent Assessment and Authorization is 12/4/2013.
X	The Federal Information Processing Standard 199 security impact category for this system is moderate or higher.
X	NIST 800-122 recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones. See Appendix A.
X	Contractors that have access to the system are subject to information security provisions in their contracts as required by the DOC policy.
	Other (specify):

Section 7: Privacy Act

7.1 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 existing system of records notices, Department #1, Attendance, Leave, and Payroll Records of Employees and Certain Other Persons, Department #18, Employees' Personnel Files Not Covered by Notices of Other Agencies, as well as NOAA #14, Dr. Nancy Foster Scholarship Program, which has been revised to include Ernest F. Hollings Undergraduate Scholarship Program and the National Marine Fisheries Service Recruitment, Training, and Research Program alumni survey. This revision was sent to DOC for review on 8-22-14.
	Yes, a system of records notice has been submitted to the Department for approval on (date).
	No, a system of records is not being created.

Section 8: Retention of Information

8.1 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: Requirements for record retention are found in the <u>NOAA Records Schedules 100-24 Information Technology Operations and Management Records and 100-27 Records of the Chief Information Officer p.12 and the (GRS) 24 and 27.</u>
	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:
X	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation: