U.S. Department of Commerce
National Oceanic and Atmospheric Administration

Privacy Impact Assessment
for the
CORPORATE SERVICES LOCAL AREA NETWORK
(CorpSrv), NOAA1200

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

Catrina D. Purvis

Digitally signed by Catrina D. Purvis
DN: cn=Catrina D. Purvis, o=Office of the Secretary, Office of Privacy and Open Government, ou=US Department of Commerce, email=cpurvis@doc.gov, c=US
Date: 2017.03.24 17:20:18 -04'00'

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

U.S. Department of Commerce Privacy Impact Assessment
NOAA/NOAA1200, CorpSrv

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

Introduction: System Description

CORPSRV LAN, NOAA1200, is a General Support System consisting of multiple subsystems as described below:

The NOAA1200 core system consists of Microsoft 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 sites within the United States.

1. Boulder, CO;
2. Fairmont, WV;
3. Germantown, MD;
4. Honolulu, HI.
5. Kansas City, MO;
6. Largo, MD; and
7. Newport, OR;
8. Norfolk, VA
9. Norfolk, VA;
10. Seattle, WA;
11. Silver Spring, MD;
12. Tampa, FL;
13. Washington, DC

NOAA1200 supports a user base of approximately 1,700 users, and. 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.

Google Apps for Government (GAfG)

Google Services is comprised of Google's multi-tenant public and hybrid Google Apps cloud instances and multi-tenant public cloud Google App Engine. These services are built atop the Google Common Infrastructure. Google Apps is a Software-as-a-Service (SaaS) cloud deployment model that allows customers the ability to communicate, store files and collaborate with Gmail, Hangouts, Talk, Calendar, Drive, Docs, Sheets, Slides, Vault, Sites, Groups, Contacts and Classroom while managing their domain with the Admin Console. Google App Engine is a Platform-as-a-Service (PaaS) cloud deployment model, providing customers an environment to easily build, run and manage their applications on Google's infrastructure.

GAfG is assessed and authorized (A&A) under the FedRAMP program, administered by the US GSA. It is authorized as a MODERATE Impact system which is adequate for the NOAA owned data processed and stored there. NOAA1200 users are not authorized to use GAfG for processing and storage of sensitive PII/BII, which is covered in the annual NOAA Information Technology Security Awareness Course (cyber security training).

Mobile Device Management (MDM)

The IBM MaaS360 is a comprehensive, cloud-based security and management platform for NOAA mobile devices, applications and content. NOAA uses MaaS360 to protect data and optimize productivity, enabling employees to work anytime and anywhere through trusted mobile interactions. MaaS360 provides a cloud based, on-demand software-as-a-service (SaaS) delivery model, built on a secure, multi-tenant architecture. MDM Federal Information Security

Management Act (FISMA) Risk Management Framework (RMF) Assessment and Authorization (A&A) requirements are met via the Federal Risk and Authorization Management Program (FedRAMP)

Amazon Web Services (AWS) Cloud Service Provider

The AWS GovCloud (US) is an Infrastructure as a Service (IaaS). It is an isolated AWS region designed to host sensitive data and regulated workloads in the cloud, supporting NOAA's compliance requirements, including the International Traffic in Arms Regulations (ITAR) and the FISMA/RMF A&A via FedRAMP. AWS GovCloud (US) is operated by employees who are vetted "U.S. Persons" and root account holders of AWS accounts must confirm they are U.S. Persons before being granted access credentials to the region.

Statutory authorities:

1. 5 U.S.C 301, which authorizes the operations of an executive agency, including the creation, custodianship, maintenance and distribution of records.
2. National Marine Sanctuaries Amendments Act of 2000 (Public Law 106-513 Section 318)
3. America Creating Opportunities to Meaningfully Promote Excellence in Technology, Education, and Science (COMPETES) Act (Public Law 110-69, Section 4002).

This system has a FIPS 199 moderate impact level.

Information will be shared only within the bureau, with the case by case exception that information may be disclosed to another Federal agency in connection with the assignment, hiring or retention of an individual, the issuance of a security clearance, the reporting of an investigation of an individual.

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):					

___X__ This is an existing information system in which changes do not create new privacy risks.

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*	X	e. File/Case ID	X	i. Credit Card	
b. Taxpayer ID (TIN)	X	f. Driver's License		j. Financial Account	X
c. Employer ID		g. Passport	X	k. Financial Transaction	
d. Employee ID	X	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: Storage is not duplicative among hosted offices: acquisition and grants, workforce management, financial, and security collect and store SSNs in their different capacities, from different populations: employees, contractors, non-NOAA customers.

Sensitive information is stored and processed in NOAA1200 as a result of routine business processes within the NOAA organizations supported, authorized under 1. 5 U.S.C 301.

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		e. ID Files Accessed	
b. IP Address	X	d. Queries Run		f. Contents of Files	
g. Other system administration/audit data (specify): Passcodes Audit data specific to when sensitive PII/BII is processed or stored in NOAA1200 is not collected. Audit information should be collected by applicable privacy systems of records when NOAA1200 users access those systems using NOAA1200 workstations.					

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	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	
State, Local, Tribal		Foreign			
Other (specify					

Non-government Sources					
Public Organizations		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):			
There are not any technologies used that contain PII/BII in ways that have not been previously deployed.			X

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

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	X
For administrative matters	X	To promote information sharing initiatives	
For litigation	X	For criminal law enforcement activities	X
For civil enforcement activities	X	For intelligence activities	
To improve Federal services online	X	For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify): Financial, education/training			

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).

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 (federal employees)
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 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	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.

	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:
X	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.)*

The only collection conducted within the boundaries of NOAA1200 consists of the PII collected for the scholarship application program. All other PII collections are conducted within the respective system boundaries of the Staff and Line Offices that own the data which may then be stored and/or processed by that office using NOAA1200. As such, the respective Privacy Act Statements pertaining to those Staff and Line Office collections are maintained within their originating FISMA systems, from which the information may then be stored and/or processed within the NOAA1200 system.

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
	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: https://oedwebapps.iso.noaa.gov/uspa/Default.aspx https://oedwebapps.iso.noaa.gov/USPA https://oedwebapps.iso.noaa.gov/SSTR/ https://oedwebapps.iso.noaa.gov/studentstracker/VAUS/ https://oedwebapps.iso.noaa.gov/studentstracker/_____ _.	
X	Yes, notice is provided by other means.	Specify how: Owners of the hosted systems send notifications to individuals when information is required. Please refer to the Appendix for these owners. 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. (A procedure required by the system of record and is not specific for NOAA1200)
	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.	Specify how: 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. NOAA1200 implements necessary controls to protect PII/BII. Information owners are responsible for implementing necessary, operational controls regarding collection, maintenance, and dissemination. Each collection procedure under the respective and applicable SORNs will have the prescribed notification procedures regarding opportunity to decline. The following applies to collection processes supported by NOAA1200: 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. 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. 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:

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.	Specify how: NOAA1200 implements necessary controls to protect PII/BII. Information owners are responsible for implementing necessary, operational controls regarding collection, maintenance, and dissemination. Each collection procedure under the respective and applicable SORNs will have the prescribed notification procedures regarding consent for use of their PII/BII. The following applies to collection processes supported by NOAA1200: 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:

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	Specify how:

	review/update PII/BII pertaining to them.	NOAA1200 implements necessary controls to protect PII/BII. Information owners are responsible for implementing necessary, operational controls regarding collection, maintenance, and dissemination. Each collection procedure under the respective and applicable SORNs will have the prescribed notification procedures regarding review and update of their PII/BII. The following applies to collection processes supported by NOAA1200: 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 8: Administrative and Technological Controls

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

	All users signed a confidentiality agreement or non-disclosure agreement.
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.
	Access to the PII/BII is being monitored, tracked, or recorded. Explanation:
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 4/1/2016 ☐ 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 security and 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.
	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.

1. Multifactor authentication
2. Anti-virus protection
3. Intrusion prevention and detection systems
4. Forensic analysis tools
5. Log analysis tools

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 *(list all that apply)*: 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. Also, OPM/GOVT-1, General Personnel Records, OPM-2, Employees Performance File Records would cover the personnel related records created and maintained by Supervisors, and WFMO, both those that go in the eOPF, and those held by the chain of command.
	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 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 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.
	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:

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

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: Some individuals could be identified based on the information stored.
X	Quantity of PII	NOAA1200 includes the workstation disks and server file stores for the NOAA headquarters staff, who use their workstations on a daily basis to process and store PII/BII.
X	Data Field Sensitivity	Provide explanation: The confidentiality impact level is set at moderate because sensitive PII is present: e.g. SSN, biometrics, etc. in combination with additional non-sensitive PII.
	Context of Use	Provide explanation:
	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: Addition of Privacy Act Statements on all scholarship forms/sites.
	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: Addition of Privacy Act Statements on all scholarship forms/sites.
	No, the conduct of this PIA does not result in any required technology changes.

Appendix

System Sharing – All users of these systems are internal to the system owner's organization.

Business Function	Application / Resource	Type of PII	Comments
AGO (Acquisition and Grants Office)	Procurement, Grants, and Contract Data; N: drive	DOB; Address; SSN	Applications, Grant, Vendor and procurement information.
CAO - SECO (Office of the Chief Administrator - Safety and Environmental Compliance Office)	Local disk; \\hqs-is-fsvr1\dcao budget; SharePoint:	Personal information, i.e., name, address, DOB, SSN on DD-214, SF-50; employment documents	Resumes, transcripts, employment documents; Accident/ Incident reports; Passport Application
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; \\hqs-is-fsvr1\dcao budget; SharePoint.	Names & Employee Salary Information	
OCIO	Performance Reviews, SF52, Telework Apps, SF182, CD137, CD505, OGE 450 Financial Disclosure Reports, Various applications in GTOWN	Ratings, DOB, Addresses, SSN	Apps: 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	
Office of Security	C-Cure	SSN, photographs, finger prints	SSN, photographs, and finger prints used for identity check on a single computer in that office for FBI SOR.
	M: drive (shared drive for each division)	DOB, 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 docs (copies)
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	TIN, ABA, SSN, DOB, Bank Info	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 per DOC CITR-022 Access and Use Policy, NOAA Rules of Behavior, and NOAA IT Security Manual Section 16.0 Access Controls. See DOC / NOAA SORNs that may be applicable at the following weblink: (http://www.corporateservices.noaa.gov/audit/privacy_act/systems-of-records/).