Template Version Number: 01-2021

U.S. Department of Commerce
Office of the Secretary (OSY)

Privacy Impact Assessment (PIA)
Emergency Notification System (ENS)

Reviewed by: Tahira Murphy, 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

Tahira Murphy Digitally signed by Tahira Murphy
Date: 2022.08.31 16:54:25 -04'00'

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

8/31/2022
Date

U.S. Department of Commerce Privacy Impact Assessment
OSY/ENS

Unique Project Identifier: OS 2862

Introduction: System Description

Provide a brief description of the information system.

Department of Commerce (DOC) is implementing the ENS which relies on Everbridge before, during, and after critical events of any kind, including ongoing pandemics, active shooter situations, terrorist attacks, severe weather incidents, network outage and cyberattack incidents, and the management of day-today security and life safety incidents. As part of the ENS system Everbridge's CEM (Critical Event Management) enables DOC to manage, control, and automate responses to these incidents to keep people safe, limit damage, and reduce recovery time and cost. Everbridge CEM data primarily contains basic contact information for all DOC personnel.

(a) Whether it is a general support system, major application, or other type of system
Major Application – Software as a service (SaaS)

(b) System location
ENS is a SaaS cloud-based system, managed, maintained, and hosted on Everbridge-Suite platform which is located on AWS East/West.

(c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)
ENS is interconnected with National Oceanic and Atmospheric Administration (NOAA) Identity, Credential and Access Management (ICAM) Single Sign-On (SSO) and Identity Management (IDM) – NOAA ICAM SSO and IDM

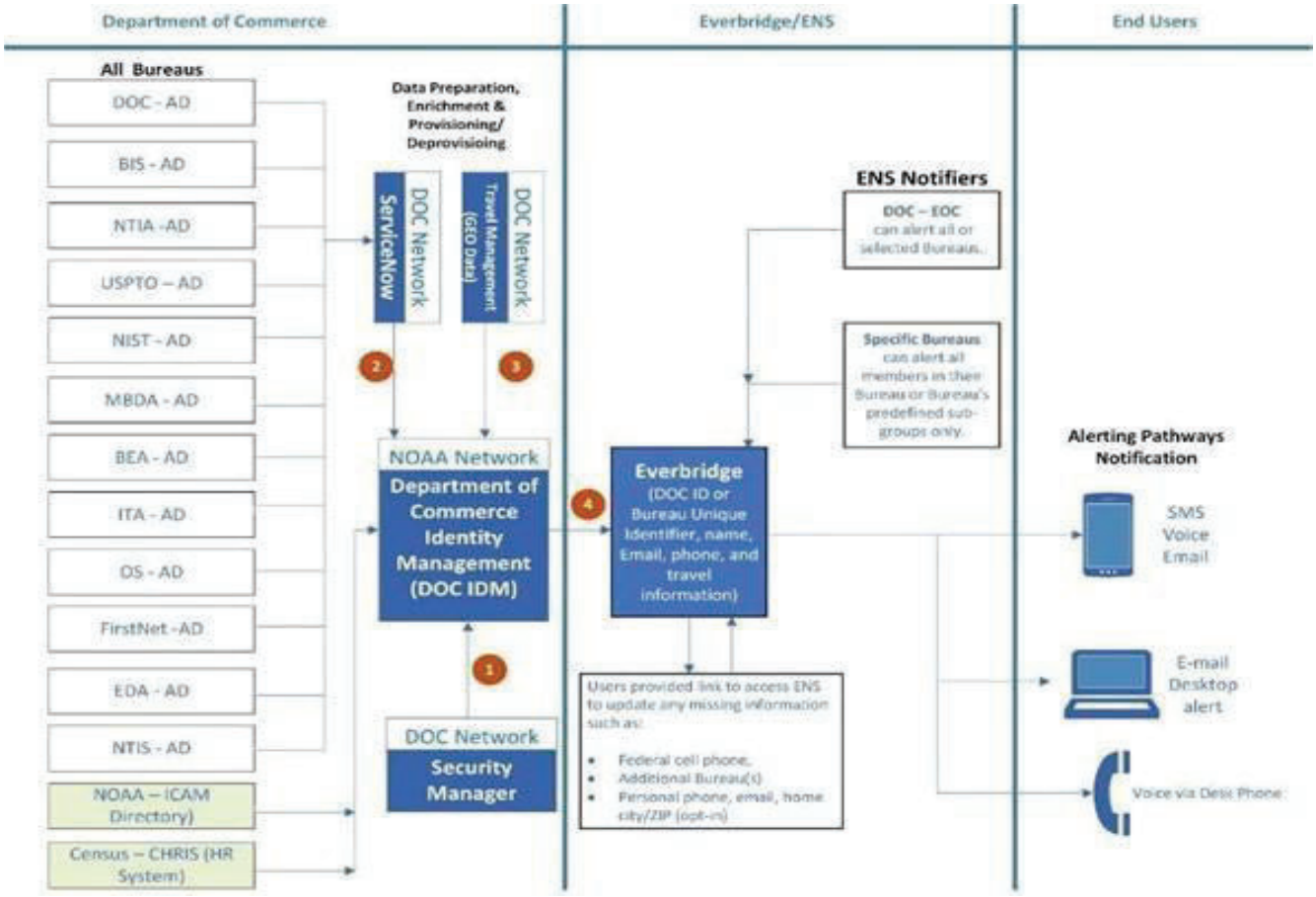
(d) The way the system operates to achieve the purpose(s) identified in Section 4

ENS is a SaaS cloud-based system. ENS would send notifications to DOC employees. The message is delivered in various delivery formats (e.g., voice call, email, SMS message, TTY call).

(e) How information in the system is retrieved by the user

The Everbridge Manager Portal contains and controls access to user information and can only be accessed if the user is in the required permissions role. Admin and Manager level based roles will have access to see the information and send out alerts, where as other users will only be able to send alerts, but not see the actual user info.

(f) How information is transmitted to and from the system



Overall Flow of Contact Information from DOC to ENS (Everbridge) and DOC notifications delivery from ENS to Contacts

In figure 1 DOC IDM will consume contact information from the following sources

Step 1: Security Manager – provides primary contact information from all the bureaus including DOC ID

Step 2: ServiceNow - enriches contact information from all the bureaus

Step 3: Travel Management – provides contact's travel information from all the bureaus

Step 4: DOC IDM - pushes information to ENS by encrypted CSV over SFTP

Initial load (see figure 4 on page 18 for details):

1. Security Manager
2. NOAA and Census (export from bureau's ENS admins)
3. ServiceNow
4. Travel Management

Ongoing contact synchronization:

1. Security Manager – Automates the provisioning and deprovisioning of Contacts (via DOC IDM)
2. ServiceNow - Enriches contact information from all the bureaus (does not override existing contact profile data in ENS that contact personally entered in)
3. Travel Management – provides contact's travel information from all the bureaus
4. NOAA and Census – Contact information enriched at source

(f) Any information sharing

ENS is interconnected with NOAA ICAM SSO and IDM. ENS only ingests information, and sends out alerts to users, it does not share information with other systems.

(g) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information

Includes the following, with all revisions and amendments: 5 U.S.C. 301; 44 U.S.C. 3101; E.O. 12107, E.O. 13164, 41 U.S.C. 433(d); 5 U.S.C. 5379; 5 CFR Part 537; DAO 202-957; E.O. 12656; Federal Preparedness Circular (FPC) 65, July 26, 1999; DAO 210-110; Executive Order 12564; Public Law 100-71, dated July 11, 1987. (https://www.osec.doc.gov/opog/PrivacyAct/SORNs/DEPT-18.html)

(h) The Federal Information Processing Standards (FIPS) 199 security impact category for the system

Moderate

Section 1: Status of the Information System

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

__X___ 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):					

_____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment.

_____ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment.

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

General Personal Data (GPD)					
a. Name	x	h. Date of Birth		o. Financial Information	
b. Maiden Name		i. Place of Birth		p. Medical Information	
c. Alias		j. Home Address	x	q. Military Service	
d. Gender		k. Telephone Number	x	r. Criminal Record	
e. Age		l. Email Address	x	s. Marital Status	
f. Race/Ethnicity		m. Education		t. Mother's Maiden Name	
g. Citizenship		n. Religion			
u. Other general personal data (specify): Work Travel Itinerary (No Passport)					

Work-Related Data (WRD)					
a. Occupation		e. Work Email Address	x	i. Business Associates	

b. Job Title		f. Salary		j. Proprietary or Business Information	
c. Work Address	x	g. Work History		k. Procurement/contracting records	
d. Work Telephone Number	x	h. Employment Performance Ratings or other Performance Information			
l. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		f. Scars, Marks, Tattoos		k. Signatures	
b. Palm Prints		g. Hair Color		l. Vascular Scans	
c. Voice/Audio Recording		h. Eye Color		m. DNA Sample or Profile	
d. Video Recording		i. Height		n. Retina/Iris Scans	
e. Photographs		j. Weight		o. Dental Profile	
p. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID		c. Date/Time of Access		e. ID Files Accessed	
b. IP Address		f. 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		Online	
Telephone		Email			
Other (specify):					

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

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

2.3 Describe how the accuracy of the information in the system is ensured.

Information is ingested from multiple authoritative sources (SecurityManager, Travel Manager, and ServiceNow instances) based on the HR Personnel files.

2.4 Is the information covered by the Paperwork Reduction Act?

	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection. When figuring out if PRA clearance is needed, consider the following: • What type of information are you collecting, • Who are you collecting it from, • How will you be collecting it, and • Why you are collecting this information. If you're only collecting information from federal employees or military personnel as part of their job, then you don't need PRA clearance. If the information isn't part of their work-related duties, you may need PRA clearance. (https://pra.digital.gov/do-i-need-clearance/)]
X	No, the information is not covered by the Paperwork Reduction Act.

2.5 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			
For a Computer Matching Program		For administering human resources programs	
For administrative matters		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): For Emergency Notification of employees, contractors, and other Federal employees.			

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 information contained in the Everbridge ENS system will be used to contact federal employees and contractors in the event of an emergency with pertinent details and/or guidance from the Emergency coordinators. Personnel will be contacted based on the contact information available within the ENS system (call, email, text, etc). Information will be stored as long as that person is an employee or contractor within DOC.

5.2 Describe any potential threats to privacy, such as insider threat, as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

The system only contains personnel contact information, and majority of that information is available in public documents. Standard DOC security practices are implemented and are required to use/access the system. Individuals' information will be automatically purged upon exit from DOC employment. There are always insider threats, and the department has IT Security Awareness Training sessions for its users. There is a Rule of Behavior (RoB) that user sign before assessing the information system. https://connection.commerce.gov/agreements/office-secretary-general-rules-behavior-users

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	X		
Federal agencies			
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 Does the DOC bureau/operating unit place a limitation on re-dissemination of PII/BII shared with external agencies/entities?

	Yes, the external agency/entity is required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
	No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
X	No, the bureau/operating unit does not share PII/BII with external agencies/entities.

6.3 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: Information is received from the DOC Identity Management System (IDM). Security controls to prevent leakage and unauthorized access are inherited from the Everbridge FedRAMP system and are enforced by DOC cybersecurity standards and requirements.
	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.4 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.)* Please ensure the response to this question is complete (i.e. provide the link to the Privacy Act statement if notice is provided by Privacy Act Statement and/or privacy policy.]

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
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: Provide login banner and link if possible; see attachment A https://www.commerce.gov/about/policies/privacy https://osec.doc.gov/opog/PrivacyAct/PrivacyAct.html	
X	Yes, notice is provided by other means.	Specify how: General notice about this system will be sent to users, asking them to update their contact information. Additionally see attachment A for Commerce Federation Broker Privacy Statement
	No, notice is not provided.	Specify why not:

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

	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how:
X	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: Individuals' information is automatically collected based on their HR profile.

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

	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how:
X	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: Individuals' information is automatically collected from systems that are included in their HR profile.

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.	Specify how: Individuals will be able to update their information via their respective HR offices.
	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.
	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: System access and system usage is automatically recorded and can be viewed via Everbridge audit logs.
X	The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements. Provide date of most recent Assessment and Authorization (A&A): _____ ☒ This is a new system. The A&A date will be provided when the A&A package is approved.
	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 controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
	A security assessment report (SAR) has been reviewed for the information system and it has been determined that there are no additional privacy risks. This statement should usually be checked if an A&A was completed. The BCPO needs a copy of the most recent SAR.]
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 DOC ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.

	Other (specify): If there are any additional controls that should be noted here to ensure the protection of PII and/or BII for this system, include here.]

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system. *(Include data encryption in transit and/or at rest, if applicable).*

Everbridge's security framework is governed by ISO/IEC 27001:2013 Information Security Standard and utilizes the comprehensive set of security requirements and controls within US National Institute of Standards and Technology (NIST) Special Publication 800-53 – Security and Privacy Controls for Information Systems.

Section 9: Privacy Act

9.1 Is the PII/BII searchable by a personal identifier (e.g., name, or Social Security number)?

__X__ Yes, the PII/BII is searchable by a personal identifier.

_____ No, the PII/BII is not searchable by a personal identifier.

9.2 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, number, and link. *(list all that apply)*: DEPT-18, Employees Personnel Files Not Covered by Notices of Other Agencies
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, this system is not a system of records and a SORN is not applicable.

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: https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-commerce/rg-0040/nc1-040-79-01_sf115.pdf. Schedule Number: NC1-040-79-01
	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		Overwriting	
Degaussing		Deleting	X
Other (specify):			

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

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. *(The PII Confidentiality Impact Level is not the same, and does not have to be the same, as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

X	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 Indicate which factors were used to determine the above PII confidentiality impact level. *(Check all that apply.)* For each criterium selected, explanations must be included in

accordance with NIST SP 800-122, describing how each item was a determining factor for identifying the confidentiality impact rating.]

X	Identifiability	Provide explanation: System only uses the first and last name, and possibly personal phone and email addresses to identify users.
X	Quantity of PII	Provide explanation: Limited to just DOC and Contractors information such as first name, last name, email address
	Data Field Sensitivity	Provide explanation: Does not contain sensitive PII
X	Context of Use	Provide explanation: In case of emergency the data is used by DOC emergency contact staff to notify affected personals
X	Obligation to Protect Confidentiality	Provide explanation: The Privacy Act of 1974 (5 USC 552a) and OMB Memorandum provide the obligation to the US Government to protect this information
X	Access to and Location of PII	Provide explanation: Hosted on an Everbridge SaaS platform and all users have access to their own records. Access to additional information is based on least privileged principle
	Other:	Provide explanation:

Section 12: Analysis

12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

Individual's contact information may be revealed. This information is required for the system to function as designed.
The system only contains personnel contact information, and majority of that information is available in public documents. Standard DOC security practices are implemented and are required to use/access the system. Individuals' information will be automatically purged upon exit from DOC employment. There are always insider threats, and the department has IT Security Awareness Training sessions for its users.
If the system was to be accessed by an unauthorized user, the main threat would be possible receipt of a false notification to users of an emergency situation.

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

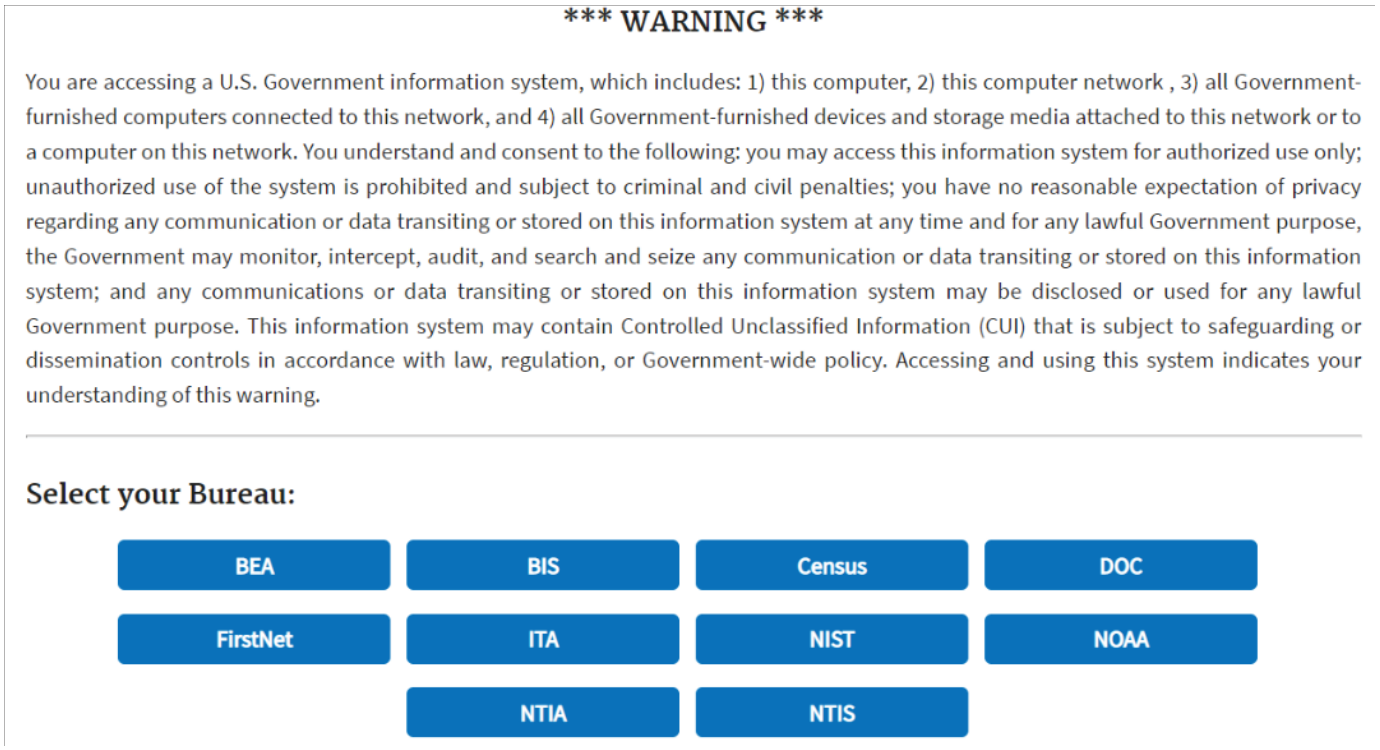
	Yes, the conduct of this PIA results in required business process changes. Explanation:
X	No, the conduct of this PIA does not result in any required business process changes.

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

	Yes, the conduct of this PIA results in required technology changes. Explanation:
X	No, the conduct of this PIA does not result in any required technology changes.

Attachments:

Attachment A:



Points of Contact and Signatures

System Owner
Name: Prabhjot Bajwa
Office: Office of the Chief Information Officer
Phone: 202-748-4252
Email: pbajwa@doc.gov

Signature: PRABHJOT BAJWA
Date signed: Digitally signed by PRABHJOT BAJWA 06:46:07 -07'00' Date: 2022.08.08

Information Technology Security Officer

Name: Densmore Bartly
Office: Office of the Chief Information Officer
Phone: 202.482.3186
Email: dbartly@doc.gov

Signature: DENSMORE BARTLY
Date signed: Digitally signed by DENSMORE BARTLY Date: 2022.08.24 22:14:59 -04'00'

Privacy Act Officer
Name: Tahira Murphy
Office: Office of Privacy and Open Government
Phone: 202.482.8075
Email: tmurphy2@doc.gov

Signature: Tahira Murphy
Date signed: Digitally signed by Tahira Murphy Date: 2022.08.29 15:38:19 -04'00'

Authorizing Official
Name: Zachary Schwartz
Office: Authorizing Official
Phone: 202.577-1769
Email: zschwartz@doc.gov

Signature: ZACHARY SCHWARTZ
Date signed: Digitally signed by ZACHARY SCHWARTZ Date: 2022.08.25 11:24:02 -04'00'

Bureau Chief Privacy Officer
Name: Tahira Murphy
Office: Office of Privacy and Open Government
Phone: 202.482.5153
Email: mdumas@doc.gov

Signature: Tahira Murphy
Date signed: Digitally signed by Tahira Murphy Date: 2022.08.29 15:38:48 -04'00'

Information System Security Officer
Name: Tierry Fornishi
Office: Office of the Chief Information Officer
Phone: 240-223-7192
Email: tfornishi@doc.gov

Signature: TIERRY FORNISHI (Affiliate)
Digitally signed by TIERRY FORNISHI (Affiliate) Date: 2022.08.08 10:07:12 -04'00'

Date signed: