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

Privacy Threshold Analysis (PTA)
for the
Emergency notification System (ENS)

U.S. Department of Commerce Privacy Threshold Analysis

OSY/ENS

Unique Project Identifier: OS 2862

Introduction: This PTA is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based on the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system: *Provide a brief description of the information system*

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

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.

Address the following elements:

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 purpose that the system is designed to serve***
The Department of Commerce (DOC) 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-to-day security and life safety incidents. 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. The purpose of Emergency Notification System (ENS) is to quickly communicate with all DOC employees and associates during emergency situations. This is critical to meeting our emergency preparedness goal of assuring the safety, protection, and security of all staff.

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

f) ***A general description of the type of information collected, maintained, used, or disseminated by the system***

Personally Identifiable Information (PII) as defined in OMB Memorandum M-07-16 refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. Information that could be tied to more than one person (date of birth) is not considered PII unless it is made available with other types of information that together could render both values as PII (for example, date of birth and street address). A non-exhaustive list of examples of types of PII includes:

- Full Name
- Employee ID
- Home address
- Telephone number
- Email address
- Work address
- Work email address
- Work Telephone number
- Work Travel Itinerary (Limited)

* PII refers to information that can be traced back to an individual person.
* For more examples of PII, refer to section 2.2 of NIST SP 800-122.

g) Identify individuals who have access to information on the system

Access to data will be controlled based on Least Privilege principal, only those authorized and system administrators will have access to actual user data.

h) How information in the system is retrieved by the user

The Manager Portal (https://manager.everbridge.net/accUpload) contains a template that can be downloaded to enter *Contact Data* for bulk upload. The Manager Portal also contains a template that can be downloaded to enter *Account Data* for bulk upload.

The unique fields within the *'Contact Data'* template is listed in table below:

Organization Name	First Name	Middle Initial	Last Name
Suffix	External ID	Country	Business Name
Record Type	Groups	SSO User ID	Group Remove
Travel Arranger	Location 1	Street Address 1	Apt/Suite/Unit 1
City 1	State/Province 1	Post Code 1	Country 1
Latitude 1	Longitude 1	Location Id 1	Extension Phone
Extension	Extension Phone Country	Email Address	Plain Text Email -1 way
Plain Text - 1 way Pager Service	Plain Text Email - 2 way	SMS 1	SMS 1 Country

FAX 1	FAX Country 1	TTY 1	TTY Country 1
Numeric Pager	Numeric Pager Country	Numeric Pager Pin	TAP Pager
TAP Pager Country	Tap Pager Pin	One Way SMS	One Way SMS Country
Custom Field 1	Custom Value 1		

The unique fields within the *'Account Data'* template are listed below:

First Name	Middle Initial	Last Name	Suffix
Email	SSO User ID	External ID	External ID ORG
Org Name 1	Role Names 1	Org Name 2	Role Names 2

The SOS connector in Safety Connection which is part of Everbridge Suite, gets itinerary data directly from TravelTracker (International SOS SaaS portal). The connector pulls information from travel itineraries, travel agencies and booking sites to track dynamic location. The unique fields of data collected as part of the SOS connector are listed below:

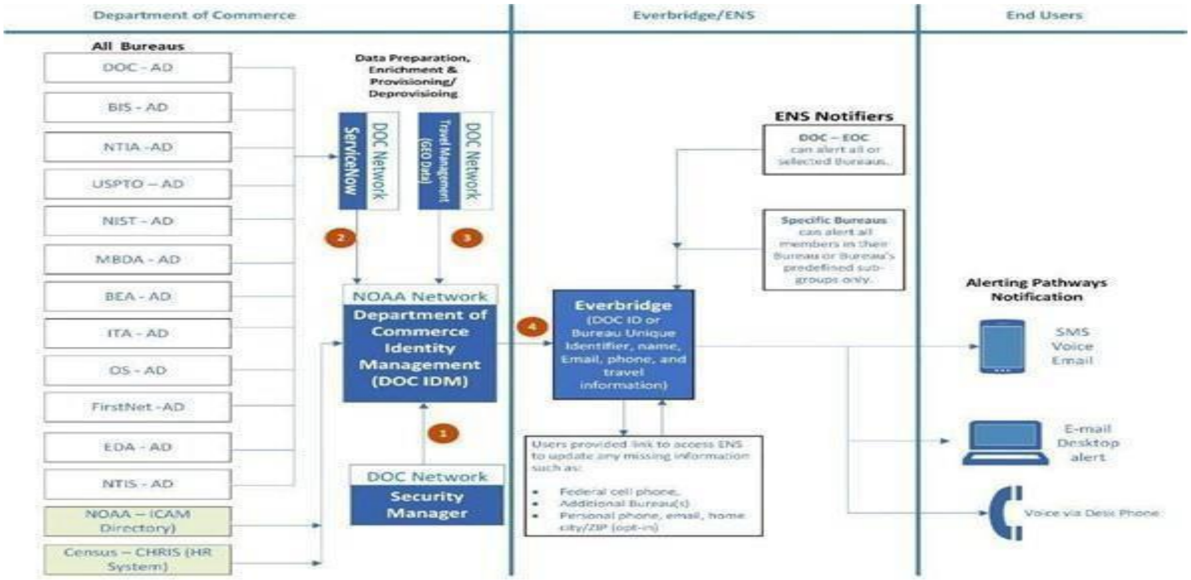
Employee ID	First Name	Last Name	Location Name
Date Range	Country	Address	Apt/Suite/Unit
City	State/Province	Postal Code	Latitude
Longitude	Source		

The Member Portal (https://member.everbridge.net/) is utilized for Member Registration. Registering members through the portal can be public or private. The following information is collected by from members during the registration process:

- First Name (mandatory)
- Last Name (mandatory)
- Middle Initial (optional)
- Suffix (optional)
- External ID (optional)

Department of Commerce has full control over which types of data are introduced and shared within the ENS system. The ENS System is fully configurable to DOC.

i) *How information is transmitted to and from the system*


Department of Commerce
Everbridge/ENS
End Users
All Bureaus
DOC - AD
BIS - AD
NTIA -AD
USPTO – AD
NIST - AD
MBDA - AD
BEA - AD
ITA - AD
OS - AD
FirstNet -AD
EDA - AD
NTIS - AD
NOAA – ICAM Directory)
Census – CHRIS (HR System)
Data Preparation, Enrichment & Provisioning/ Deprovisioing
DOC Network
ServiceNow
DOC Network
Travel Management (GEO Data)
2
3
NOAA Network
Department of Commerce Identity Management (DOC IDM)
1
DOC Network
Security Manager
4
Everbridge (DOC ID or Bureau Unique Identifier, name, Email, phone, and travel information)
Users provided link to access ENS to update any missing information such as:
• Federal cell phone,
• Additional Bureau(s)
• Personal phone, email, home city/ZIP (opt-in)
ENS Notifiers
DOC – EOC can alert all or selected Bureaus.
Specific Bureaus can alert all members in their Bureau or Bureau's predefined sub-groups only.
Alerting Pathways Notification
SMS Voice Email
E-mail Desktop alert
Voice via Desk Phone

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

Per the Everbridge Privacy policy, it may be necessary to share client contact information with third parties for Everbridge to provide the services requested by DOC. For example, we will need to transmit an individual's cell-phone number to a telecommunications provider in order to deliver a customer-initiated notification designated for that individual and others. Under such circumstances we will only transmit the information needed to fulfill the obligations described in our customer's service contract.

These third parties are also bound by contractual obligations to keep personal information confidential and use it only for the purposes for which we disclose it to them. Transfers to these third parties are covered by the provisions in this privacy policy regarding notice and choice, as well as applicable contractual agreements.

The Everbridge Information Handling and Document Control Policy and the Everbridge Legal team establishes the criteria for what PII can be shared.

Questionnaire:

1. Status of the Information System

1a. What is the status of this information system?

__X__This is a new information system. *Continue to answer questions and complete certification.*

_____ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

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. *Continue to answer questions and complete certification.*

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

1b. Has an IT Compliance in Acquisitions Checklist been completed with the appropriate signatures?

___X_ Yes. This is a new information system.

_____ Yes. This is an existing information system for which an amended contract is needed.

____ No. The IT Compliance in Acquisitions Checklist is not required for the acquisition of equipment for specialized Research and Development or scientific purposes that are not a National Security System.

_____ No. This is not a new information system.

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

_____ Yes. *(Check all that apply.)*

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

__x___No.

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

_____ Yes, the IT system collects, maintains, or disseminates BII.

__X__No, the IT system does not collect any BII

4. Personally Identifiable Information (PII)

4a. Does the IT system collect, maintain, or disseminate PII?

As per OMB 17-12: "The term PII refers to information that can be used to distinguish or trace an individual's identity either alone or when combined with other information that is linked or linkable to a specific individual."

_X_Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

__X__DOC employees
__X__Contractors working on behalf of DOC
__X__Other Federal Government personnel
_____ Members of the public

_____ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate Social Security numbers (SSNs), including truncated form?

_____ Yes, the IT system collects, maintains, or disseminates SSNs, including truncated form.

Provide an explanation for the business need requiring the collection of SSNs, including truncated form.
Provide the legal authority which permits the collection of SSNs, including truncated form.

_X_No, the IT system does not collect, maintain, or disseminate SSNs, including truncated form.

4c. Does the IT system collect, maintain, or disseminate PII other than user ID?

__X__Yes, the IT system collects, maintains, or disseminates PII other than user ID.

_____ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4d. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

_____ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

_X_No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, 4c, and/or 4d are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the SAOP approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

_X_____ The criteria implied by one or more of the questions above **apply** to the [replace this language here with the IT SYSTEM NAME] and as a consequence of this applicability, a PIA will be performed and documented for this IT system.

______The criteria implied by the questions above **do not apply** to the [whether or not this response is selected, replace this language here appearing in red with the IT SYSTEM NAME] and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

System Owner Name: Prabhjot Bajwa Office: Office of the Chief Information Officer Phone: 202-478-4252 Email: pbajwa@doc.gov Signature: PRABHJOT BAJWA PRABHJOT BAJWA Digitally signed by 06:46:58 -07'00' Date: 2022.08.08 Date signed:	**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 Digitally signed by DENSMORE BARTLY Date signed: Date: 2022.08.24 22:15:30 -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 Digitally signed by Tahira Murphy Date signed: Date: 2022.08.29 15:34:53 -04'00'	**Authorizing Official** Name: Zachary Schwartz Office: Authorizing Official Phone: 202-577-1769 Email: zschwartz@doc.gov Signature: ZACHARY SCHWARTZ Digitally signed by ZACHARY SCHWARTZ Date signed: Date: 2022.08.25 11:22:59 -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 Digitally signed by Tahira Murphy Date signed: Date: 2022.08.29 15:35:25 -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 10:08:54 -04'00' Date signed: