Court Services and Offender Supervision Agency (CSOSA)

Emergency Notification System (ENS)
Privacy Impact Assessment

CONTROLLED UNCLASSIFIED INFORMATION

_____, 2020

Office of Director
Court Services and Offender Supervision Agency
Room 6131, 800 North Capitol St, NW, Washington, DC 20002

Overview of Emergency Notification System (ENS)

Court Services and Offender Supervision Agency (CSOSA) and the Office of Information & Technology (OIT) established the Emergency Notification System (ENS) to provide efficient and effective communication with CSOSA personnel. CSOSA, as a Federal agency employer, has a responsibility to ensure its employees, interns, and on-site contractors are provided pertinent information as quickly as possible to ensure they are kept safe during an emergency. In addition, as an integral part of the District's criminal justice system, CSOSA has a responsibility to keep its stakeholders informed of emergency conditions that may impact District criminal justice operations. In order to fulfil these responsibilities, the agency uses contact information from Agency records, from voluntary employee input, and from selected external stakeholders.

The purpose of this Privacy Impact Assessment (PIA) is to address the privacy risks associated with the collection, use, storage, dissemination, and disposal of PII in the ENS.

1. Description of the System

1.1. Describe the system, including the system name, system, acronym, and a brief description of the major functions.

The Emergency Notification System (ENS) provides for the efficient and effective communications with CSOSA employees, interns, selected on-site contractors, and selected external stakeholders (ENS participants) during emergencies or significant disruptions to Agency operations. This communication is possible due to the ENS participant's contact information stored in the vendor's cloud service. The participant's contact information is collected from existing Agency records, from voluntary employee input, and from selected external stakeholders. The vendor of the ENS is Everbridge, a Cloud Service Provider (CSP).

The CSOSA Continuity Manager is the Contracting Officer Representative (COR) and the ENS Account Administrator. The Continuity Manager and staff members from CSOSA's Office of Information Technology (OIT) work collaboratively with the vendor to establish the data collection, storage, maintenance, dissemination, and removal procedures.

The ENS participant's collected contact information is uploaded to the vendor's cloud storage automatically on a daily basis, or manually, as needed. The data contained in the ENS is replicated in accordance with Federal Risk and Authorization Management Program (FedRAMP)-compliant processes. Collectively, this combination of equipment and procedures provides CSOSA with the highest degree of reliable, accurate, and accessible contact information for use during an emergency, with or without an operational Agency network.

In the event of a wide variety of emergencies or significant disruptions to the

Agency's operations, the ENS allows a trained and authorized CSOSA staff member (ENS user) the ability to log into the ENS system, select relevant attributes from pre-defined and approved pull-down menus in order to create an emergency notification, and then send that notification to the intended ENS participants. Notification recipients may receive the notification by several communications methods, such as Agency office phone, mobile phone text or voice call, and email; and an opt-in personal phone and email. The ENS also allows for the notification authors to solicit responses from the message recipients. Finally, the ENS allows for the creation of notification status reports, which may be beneficial to determine employee accountability during a disaster.

1.2. Describe the purpose for which the personally identifiable information (PII) is collected, used, maintained, or shared.

The PII is collected, used, and maintained to ensure that its employees, interns, and on-site contractors are provided pertinent information as quickly as possible to ensure they are kept safe during an emergency. In addition, as an integral part of the District's criminal justice system, CSOSA has a responsibility to keep its stakeholders informed of emergency conditions that may impact District criminal justice operations. In order to fulfil these responsibilities, the agency uses contact information from Agency records, from voluntary employee input, and from selected external stakeholders.

1.3. Is this a new system or one that is currently in operation?

The ENS is a new system.

1.4. Is this privacy impact assessment (PIA) new, or is it updating a previous version? If this is an update, please include the publication date of the original.

This is a new PIA.

1.5. Is the system operated by the agency, by a contractor, or both?

The cloud-based system is operated by the vendor, but data management is performed by the agency.

2. Legal Authorities and Other Requirements

2.1. What specific legal authorities and/or agreements permit and regulate the collection, and use of the data by the system?

Authority for collecting this information includes:

- 5 U.S.C. § 7902, Safety Programs
- CSOSA Continuity of Operations Plan, Version 4.00, dated 5/8/19

- CSOSA Continuity of Operations Policy Statement, PS 1040, dated 6/19/20
- Federal Continuity Directive 1

2.2. System of Records Notice (SORN) Requirement: Is the information in this system retrieved by a name or a personal identifier? If so, this system will need to be covered by a Privacy Act SORN.

Yes, information is retrieved by a name or personal identifier. For authorized ENS users, the system will support a role-based search on notification recipients by:

- Last name
- First name
- Agency Desk Phone
- Agency Mobile Phone
- Agency Email Address
- Personal Home Phone (If voluntarily provided by the individual)
- Personal Mobile Phone (If voluntarily provided by the individual)
- Personal Email Address (If voluntarily provided by the individual)
- Organization (e.g. OCSIS, Office of the Director, External Stakeholder Agency Name, etc.)
- Component (e.g. OCSIS, Accountability & Monitoring Division, OIT Infrastructure, etc.)
- Employee type (e.g., employee, contractor, intern, external stakeholder, etc.)
- CSOSA Building and Floor
- Team (e.g. Emergency Evacuation Team, Emergency Relocation Group, Advance Team, Critical Incident Response Team, etc.)
- Skill/Certification (e.g. Foreign Language, First Aid, CPR, etc.)

2.3. Records Management Requirement: Does a records retention schedule, approved by National Archives and Records Administration (NARA), exist for the records contained in this system? If yes, please provide the NARA schedule number.

The General Records Schedule for this collection is GRS 5.3, *Continuity and Emergency Planning Records*. Disposition Authority DAA-GRS-2016-0004-0002. The disposition instructions are to destroy when superseded or obsolete, or upon separation or transfer of employee.

2.4. Is the PII contained in this system disposed of appropriately, and in accordance with the timeliness in the records disposition schedule?

Yes. Once an employee leaves the agency, his CSOSA contact information is marked as deleted. This information is then updated to the Agency's Everbridge account on a nightly basis through an automated process. The information is permanently deleted from the Everbridge account after 30 days.

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

Threats to privacy would be through compromise of the data in the CSOSA database and the vendor's cloud service. This data breach could expose an employee's work phone numbers, email address, building location, and personal phone numbers and email address if the individual opted in with their personal information.

CSOSA's OIT uses a number of controls: splitting of roles involved with granting user access; strong passwords; the encrypted internet communication protocol; Hypertext Transfer Protocol Secure (HTTPS); Activity Directory authentication; transparent data encryption; encrypted data exchanges; and other procedural and system controls to ensure that database information is handled, retained, managed and accounted for appropriately.

Potential privacy breaches are prevented and handled in three ways: CSOSA Information Technology equipment and procedures, the vendor's emergency notification system equipment and procedures, and CSOSA's ENS policy and procedures.

The ENS is authorized by the Federal Risk and Authorization Management Program (FedRAMP). As such, ENS is in compliance with a set of comprehensive and rigorous information technology security requirements. FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

CSOSA has established a policy that requires all users (notification senders) to undergo initial training and certification prior to operating the system, and recurring training and certification to continue permissions to operate. In addition, roles and responsibilities have been established that tightly control who has permissions for viewing and editing specific data.

3. Characterization and Use of Information

Collection

3.1. Select the specific personal information data elements (e.g. name, email, address, phone number, date of birth, social security number, etc.) that the system collects, uses, disseminates, or maintains.

Identifying Numbers					
Social Security		File/Case ID		Financial Account	
Taxpayer ID		Driver's License		Financial Transaction	

Employee ID		Credit Card			
Other identifying numbers (please specify): N/A					

General Personal Data					
Name	X	Date of Birth		Religion	
Maiden Name		Place of Birth		Financial Information	
Alias		Home Address		Medical Information	
Gender		Telephone Number	X	Military Service	
Age		Email address	X	Physical Characteristics	
Race/Ethnicity		Education			
Other general personal data (specify): Personal data, such as home phone, personal mobile phone, and personal email address is optional and is obtained by opt-in procedures. Additionally, skills and certifications, such as a current First Aid/CPR certification or a foreign language fluency would be voluntary, but would also require Agency verification.					

Work-related Data					
Occupation		Telephone number	X	Salary	
Job title	X	Email address	X	Work history	
Work address	X	Business associates			
Other work-related data (please specify): Other Agency-related data includes: Agency organization, Agency subcomponent(s), Teams (if applicable), Building, and Office Floor.					

Distinguishing Features/Biometrics					
Fingerprints		Photos		DNA profiles	
Palm prints		Scars, marks, tattoos		Retina/iris scans	
Video recording/signatures		Vascular scan		Dental profile	
Other distinguishing features/biometrics (please specify): N/A					

System admin/audit data					
User ID	X	Date/time of access	X	ID files accessed	X
IP address	X	Queries run	X	Contents of files	X
Other system admin/audit data (please specify):					

3.2. Indicate the sources of the information in the system (e.g., individual, another agency, commercial sources, etc.) and how the information is collected from stated sources (paper form, webpage, database, etc.).

The information is collected from the CSOSA Active Directory, OHR emails, Office of Facilities emails, employees (for opt-in data), and external stakeholders input.

Directly from individual about whom the information pertains					
In person	X	Hard copy: mail/fax	X	Online	X

Telephone	X	Email	X		
Other (please specify):					

Government Sources					
Within the Component	X	Other CSOSA components		Other federal entities	
State, local, tribal		Foreign			
Other (please specify):					

Non-government Sources					
Members of the public		Public media, internet		Private sector	
Commercial data brokers					
Other (please specify): N/A					

3.3. Where will the PII be stored in the system?

The PII will be stored within the vendor’s cloud-based infrastructure.

3.4. Now that you have identified the information collected and the sources of the information, please 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. Please describe the choices that the component 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.).

CSOSA selected the smallest data set possible to fulfil the requirement of being able to notify/advise the staff of an emergency event (naturally occurring or man-made) affecting them directly or indirectly. This dataset, if compromised, would give an attacker benign information of a staff member (name, work location, work telephone number, government furnished mobile.) An attacker’s motive is to get a large amount of immediately usable information which can be used for financial gain or increased status in their community. The data available would not provide that information readily and would require hours of research per user.

The data is stored on the vendor’s infrastructure and not in a CSOSA operated facility.

Purpose and Use of the System

3.5. Describe how and why the system uses the information to achieve the purpose stated in Question 1.2 above.

CSOSA, as a Federal agency employer, has a responsibility to ensure its employees, interns, and on-site contractors are provided pertinent information as quickly as possible to ensure they are kept safe during an emergency. In addition, as an integral part of the District's criminal justice system, CSOSA has a responsibility to keep its stakeholders informed of emergency conditions that may impact District criminal justice operations. In order to fulfil these responsibilities, the agency uses contact information from Agency records, from voluntary employee input, and from selected external stakeholders.

The information is limited to that required to ensure the best probability of communicating with an individual during an emergency situation. There are three types of data: Agency-provided, Individual Opt-In, and a combination of the two.

- Agency-provided data: Agency desk phone and mobile phone; Agency email address; Office building and floor; Agency component and sub-component(s) if applicable; and teams, if applicable.
- Personal information includes: Home phone, mobile phone, and email address.
- Agency and Personal information includes: Skills and certifications, such as first aid/CPR certification, and a foreign language fluency. This is a combined situation because the individual may volunteer to use his or her skills and certifications, but there needs to be some Agency oversight to ensure skill/certification currency and level of competence in order to maximize their contribution during an emergency.

The ENS is capable of reaching an individual using all communication devices at once, or in a cascading format.

3.6. Select why the information in the system is being collected, maintained, or disseminated.

The information is collected and maintained in order to quickly communicate with an individual during an emergency situation.

Social Security Numbers

3.7 Does the system collect Social Security Numbers? If so, explain the purpose of its collection, type of use, and any disclosures.

No, the system does not collect Social Security Numbers.

3.8 Specify any alternatives considered in the collection of SSN and why the alternatives were not selected.

N/A

4. Notice

4.1. How does the system provide individuals notice about the collection of PII prior to the collection of information (i.e. written Privacy Act notice, link to a privacy policy, etc.)? If notice is not provided, explain why not.

The ENS uses a link to the CSOSA Privacy Act Statement on the login page of the website, advising employees and contractors that their Agency information will be collected and used in this system. The system also provides the employee with the Privacy Act Notice on the Opt-In instruction page. Opt-In is the term used to describe an employee's ability to voluntarily provide personal phone numbers and email address so that the system can communicate with them even if the employee does not have an Agency-provided phone or computer at that time.

4.2. Provide the text of the notice, including where it can be found, or the link to the webpage where notice is posted.

The following language is included:

Authority: 49 U.S.C. §114 authorizes the collection of this information.
Purpose: CSOSA will use any private phone or email information collected to send out emergency notifications.
Routine Uses: This information will be used by and disclosed to CSOSA personnel and contractors or other agents who need the information to assist in activities related to emergency notifications. Additionally, CSOSA may share the information with facility operators, law enforcement or other agencies as necessary to respond to potential or actual threats to building and personnel security, or pursuant to its Privacy Act system of records notice."
Disclosure: Furnishing this information is voluntary; however, failure to furnish the requested information may delay or prevent notification of an emergency or security threat from reaching you in a timely fashion.

4.3. What opportunities are available for individuals to consent to uses, decline to provide information, or opt-out of this system/project?

The employee information contained in the ENS system already exists in the agency's Human Resources systems. The information is generally obtained in the application process for federal employment and in the ongoing tenure of an employee and is necessary for federal employment, The ENS system provides a backup storage for standard employee information necessary to continue operations in the event of an emergency.

CSOSA employees and interns do not have the option to decline to provide work contact information or opt out. They do have the ability not to provide personal information such as home phone number, personal mobile phone number, and personal email address. They also have the ability not to provide information on skills and certifications that may be helpful for the Agency to know in times of emergencies, such as first aid/CPR expertise and foreign language fluency. Other ENS notification recipients, such as selected contractor representatives and external stakeholders, are free not to participate; all of their information is considered voluntary.

If any individual determines that the Agency has inaccurate, incomplete, out of date, or irrelevant information, the individual will have an opportunity to submit new information to OHR so that the information can be updated and that information is what is used/inserted in the ENS by authorized CSOSA staff members.

5. Information Sharing

Internal

5.1. How do agency personnel gain access to the system and the PII (e.g., users, managers, system administrators, developers, contractors, etc.)?

The Account Administrator controls entry into the system. For all individuals, regardless of their role or responsibilities, the Account Administrator or authorized assistants, will enter the person's information into the system. The system, with the approval of the Account Administrator, will send an email to the individual. This email will include instructions, as well as a link to their log-in page.

Additionally, those who have responsibilities to send notifications or handle data will have training requirements, and will be provided privileges commensurate with their assigned role.

5.2. Will information be shared internally with other CSOSA program offices and/or components? If so, which ones?

The ENS information will not be shared with any other program office or components.

5.3 What information will be shared and with whom?

N/A

5.4 How will the information be shared?

N/A

5.5 What is the purpose of sharing the specified information with the specified internal organizations? Does this purpose align with the stated purpose in Question 1.2 above?

N/A

5.6 Describe controls that the program offices and/or components have put into place in order to prevent or mitigate threats to privacy in connection with the disclosure of information.

CSOSA requires employees to complete mandatory IT Security Awareness and Records Management training, both of which have sections on the proper handling, retention, and disposition of information, including personally identifiable information. Additionally, within the ENS, audit logs are available for review.

5.7 Is the access to the PII being monitored, tracked or recorded?

Yes. The ENS is a cloud-based application. The vendor will collect auditable data regarding access to the PII for review by CSOSA's Account Administrator in accordance with federal auditing responsibility controls. The Account Administrator reviews the audit logs to detect unauthorized access to PII data.

Additionally, all computer systems at CSOSA, including the ENS, are monitored through computer security software programs. All CSOSA staff members (employees, contractors, anyone with access to CSOSA computer systems and/or the CSOSA network) are notified that computer use is subject to monitoring and use of the network and systems, and consents to that monitoring. There is a warning on the log in screen for the ENS that tells authorized users that use of the system may be monitored, intercepted, recorded, read, copied or captured.

External

5.8 Will the information contained in the system be shared with external entities (e.g. another federal agency, District of Columbia agency, etc.)?

No; this information will not be shared.

5.9 What information will be shared and with whom?

N/A

5.10 What is the purpose of sharing the specified information with the specified external entity? Does this purpose align with the stated purpose in Question 1.2 above?

N/A

5.11 How is the information accessed and used by the external entity?

N/A

5.12 What controls are in place to minimize risk and protect the data?

Controls used to minimize risk and protect the data include administrative, technical, and physical safeguards. These safeguards are responsibilities that are shared between CSOSA and the vendor.

The administrative safeguards include, but are not limited to, training and access control management, for which CSOSA is responsible.

Access control includes the request, approval, provisioning, and disabling of accounts; and writing and maintaining policies, plans, and procedures. Users (those who send messages) and contacts (those who receive messages) will use Single Sign On by entering the vendor's portal by way of their normal secure CSOSA log in procedures. Single Sign On means the individual does not need to enter a user ID and password multiple times. Once the person enters their CSOSA user ID and password, they are also logged into the vendor's system. Also, authorized users sending notifications from their Agency mobile phone will do so by way of the vendor's application. For external stakeholders, the Continuity Manager will manually enter their information into the system. The external stakeholders will have no direct access to the system.

Concerning physical controls, the vendor is a cloud-based system and uses Amazon Web Services. Therefore, the vendor is responsible for working with the Amazon Web Services for implementing all federally-mandated physical security controls. Security controls that have been implemented are as follows:

(1) Security Perimeter for physical protection, including information handling facilities and equipment with physical barriers such as fences, gates, exterior walls and doors as applicable;
(2) Human security such as standing guard, sitting guard, and patrolling guard; and
(3) Mechanical security such as entry and exit control, intruder monitoring and detection.

The vendor also ensures entry and exit security controls are in place in order to permit only authorized individuals' entrance to server rooms within secure perimeters of business premises including:

Visitor records (visitor book or electronic log): One year or longer from date of recording.

- Access logs (building / room entry and exit control system (electronic log)): One year or longer from date of recording,
- Surveillance camera video recordings: Three months or longer from date of recording, and
- Restrictions on bringing recording equipment.

5.13 Is the external information sharing pursuant to a Computer Matching Agreement (CMA), Memorandum of Understanding (MOU), or other type of approved sharing agreement with another agency?

N/A

6 Consent and Redress

6.1 How will individuals be notified if there are any changes regarding how their information is being collected, maintained, or disseminated by the system?

The CSOSA Account Administrator is responsible for notifying ENS participants, by email and within three business days, that there has been a change in their information collection, maintenance, or dissemination.

6.2 What are the procedures that will allow individuals to access their own information?

CSOSA employees will have continual access to their information by logging in to the vendor's portal by way of the Agency network. Employees will have the ability to change their Opt-In/Opt-Out status; edit their personal phone numbers and email addresses, if applicable; and view their Agency-provided information.

6.3 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Periodically, ENS participants are reminded to review their data to ensure accuracy. Corrections are then emailed to the Account Administrator, who makes the changes.

6.4 How does the project notify individuals about the procedures for correcting their information?

There are three methods by which CSOSA notifies individuals about the procedures for correcting their information: 1) Initial and refresher training, 2) Periodic reminder instructions and 3) Instructions within the portal.

6.5 How will individuals have the opportunity to consent or dissent to particular uses of the information?

ENS participants will have continual access to their information by logging in to the vendor's portal. Within their password-protected portion of the portal, individuals will have the ability to change their Opt-In/Opt-Out status.

6.6 How will the agency provide notice to individuals that their PII information may be shared with other agencies or entities (both internal and external)?

N/A. CSOSA will not share their PII with other agencies or entities.

7 Information Security and Safeguards

7.1 Does the component office work with their Chief Information Officer (CIO) to build privacy and security into the system and build privacy extension to the extent feasible?

The Agency's Office of the Director works in collaboration with the Chief Information Officer to build information privacy and security into the system. The vendor's emergency notification system is a FedRAMP-authorized cloud-based application, with industry-leading technical controls. Additionally, privacy is maintained through Agency and vendor access control policies and procedures.

7.2 Do contractors have access to the system?

The vendor's representatives have access only to the system application, and not the data.

7.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

The system employs role-based access control (RBAC). Using RBAC, the Account Administrator ensures that accounts have been given only those privileges required for the execution of their role, and no higher. RBAC also includes provisions that individuals cannot execute or perform unauthorized actions.

7.4 What administrative, technical, and physical safeguards are in place to protect the information?

The administrative, technical, and physical safeguard responsibilities are shared between CSOSA and the vendor.

The administrative safeguards include, but are not limited to, the training and access control management portion, for which CSOSA is responsible.

Access control includes the request, approval, provisioning, and disabling of accounts; and writing and maintaining policies, plans, and procedures. Users (those who send messages) and contacts (those who receive messages) will use Single Sign On by entering the vendor's portal by way of their normal secure, CSOSA log in procedures. Single Sign On means the individual does not need to enter a user ID and password multiple times. Once the person enters their CSOSA user ID and password, they are also logged into the vendor's system. Also, authorized users sending notifications from their Agency mobile phone will do so by way of the vendor's application. For external stakeholders, the Continuity Manager will manually enter their information into the system. The external stakeholders will have no direct access to the system.

Concerning physical controls, the vendor's ENS is a cloud-based system and uses

Amazon Web Services. Therefore, the vendor is responsible for working with the Amazon Web Services for implementing all federally-mandated physical security controls. These security controls that have been implemented are as follows:

- Security Perimeter for physical protection, including information handling facilities and equipment with physical barriers such as fences, gates, exterior walls and doors as applicable;

(2) Human security such as standing guard, sitting guard, and patrolling guard; and
(3) Mechanical security such as entry and exit control, intruder monitoring and detection.

The vendor also ensures entry and exit security controls are in place in order to permit only authorized individuals' entrance to server rooms within secure perimeters of business premises including:

- Visitor records: (visitor book or electronic log) for the duration of One year or longer from date of recording.
- Access logs: (building / room entry and exit control system (electronic log)): One year or longer from date of recording,
- Surveillance camera video recordings: Three months or longer from date of recording, and
- Restrictions on bringing recording equipment.

7.5 Is an Authority to Operate (ATO) required? Has one been granted?

Yes, an ATO is required. Yes, an ATO was granted on 5/30/19.

7.6 Is the system able to provide an accounting of disclosures?

The ENS provides the Audit Logs for the Account Administrator to review and identify unauthorized activities.

7.7 What controls are in place to prevent the misuse (e.g., browsing) of data by authorized users who have access to the data?

Controls in place to prevent the misuse of data by authorized users with access to the data include two information security best practices: Least Privilege and Separation of Duties.

Least privilege is a technique that restricts data access rights for applications, servers, etc. to only those permissions absolutely required to perform authorized and necessary operational or maintenance activities.

Separation of duties is a classic information security method to manage conflict of interest, the appearance of conflict of interest, and fraud by restricting the amount of power held by any one individual.

7.8 Is there a way to identify unauthorized users? If so, what controls are in place to prevent a data breach?

Each user has unique credentials and access is logged. The risk of a data breach is minimized through the use of auditing control. An example of an auditing control would be the ability of an authorized account administrator to review the database to look for abnormal activity, such as odd-hour attempts at database querying. Access controls prevent an unauthorized user from logging in and gaining access to the system. Additionally, non-administrative users can only access their own data.

7.9 Does the agency provide annual security and privacy training for agency employees and contractors?

Yes, the agency provides annual security and privacy training. IT security training is covered in the agency's annual IT Security Awareness training that is required for all CSOSA staff members. Annual privacy training is provided through the Office of the General Counsel.

7.10 Who is responsible for assuring safeguards for PII in the system?

All authorized users of the ENS, authorized staff in the Office of Information Technology, the Account Administrator, and the vendor are all responsible for ensuring the correct use and safeguarding of the PII.

7.11 How will owners of the PII be harmed if privacy data is unlawfully disclosed?

The disclosure of personal phone numbers and email addresses may require individuals to change the numbers and addresses to prevent or stop harassing phone calls and spam emails from those who acquired the information. Agency operations and assets would not be adversely affected.

7.12 If contractors have access to the system, has the agency provided the contractor, who works on the system, a confidentiality agreement or a Non-Disclosure Agreement (NDA)?

Because of the vendor permissions in place, the vendor's access to data is prohibited except in rare and tightly controlled situations. Consequently, a Non-Disclosure Agreement is not needed.

7.13 What other IT security measures has the agency implemented to protect PII in the system?

The administrative, technical, and physical safeguard responsibilities are shared between CSOSA and the vendor. The administrative safeguards include, but are not limited to, training and access control management for which CSOSA is responsible. Access control includes the request, approval, provisioning, and disabling of accounts; and writing and maintaining policies, plans, and procedures.

8 Auditing and Accountability

8.1 How does the system owner ensure that the information is used in accordance with the stated practices in this PIA?

The System Owner is the Agency's Continuity Manager, who is also the Contracting Officer's Representative (COR) and the Account Administrator. The Continuity Manager ensures that the information is used in accordance with the procedures described within this PIA by: 1) Establishing a policy and procedures that govern this system, 2) Establishing a training and certification program for any system user (those who will be potentially sending notifications), 3) Establishing roles, responsibilities, and permissions for all users, and 4) Establishing and maintaining a review and approval process for all notifications.

8.2 What are the privacy risks associated with this system and how are those risks mitigated?

Audits of ENS by third parties (e.g. annual FISMA audit, annual financial audit), completed as scheduled by CSOSA Office of Information Technology, mitigate risk through external review of the system and associated procedures for data handling and risk mitigation.

9 Data Quality and Integrity

9.1 How will the information that the agency collects be verified for accuracy and completeness when it is entered into the system?

PII accuracy and completeness will be verified four ways: 1) Initial information from OHR and Facilities will be verified at the originating office, 2) Data Managers and the Account Administrator will be continually monitoring and auditing system data, verifying against documents such as Office of Facilities emails regarding employees and their office locations, OHR employee lists, and component organization lists, 3) ENS participants will be periodically reminded to log in to the system to view their personal data as well as Agency-provided data, and 4) ENS built-in data input validation.

9.2 Are there any privacy risks for individuals whose information is collected or used by the project that relate to data quality and integrity? If so, how will CSOSA mitigate these risks?

The disclosure of personal phone numbers and email addresses may require individuals to change the numbers and addresses to prevent or stop harassing phone calls and spam emails from those who acquired the information. Agency operations and assets would not be adversely affected.

10 Privacy Policy and Statement

10.1 Has the agency provided a Privacy Act Statement or policy for this system and is it provided to all individuals whose PII is collected, maintained or stored?

Yes.

10.2 Is the privacy policy publicly viewable? If so where?

Yes. CSOSA's privacy policy is publicly viewable on the agency's public website at:

https://www.csosa.gov/privacy-policy

Authorizing Signatures

This Privacy Impact Assessment has been conducted by the Office of the Director and has been reviewed by Sheila Stokes, the Senior Agency Privacy Official, for accuracy.

___Richard Magners_______________
System Owner Name (Please Print)

9/17/2020

X Richard A. Magners

Richard Magners

Signed by: RICHARD MAGNERS

_____Johnathan Raford______________
Privacy Program Manager Name (Please Print)

X JOHNATHAN RAFORD

Digitally signed by JOHNATHAN RAFORD
Date: 2020.09.30 08:58:40 -04'00'

Johnathan Raford

Sheila Stokes, Esq.

Digitally signed by Sheila Stokes, Esq.
Date: 2020.10.02 09:29:27 -04'00'

_____Sheila Stokes_________________
Senior Agency Official for Privacy (Print)

X

Sheila Stokes