Privacy Impact Assessment
for
Everbridge Mass Notification System (EMNS)

April 2025

Point of Contact
William Schroeder

Reviewing Official
Kellie Cosgrove Riley
Chief Privacy Officer

OVERVIEW

Everbridge is a global provider of Software as a Service (SaaS)-based unified critical communications solutions. During mission-critical business events or man-made or natural disasters, the Everbridge Mass Notification System (EMNS) platform enables the Commodity Futures Trading Commission (CFTC) to quickly and reliably deliver the right message to "Contacts" (CFTC employees and contractors (CFTC staff)) on the right device, in the right location, at the right time. The Security and Emergency Management Unit, along with the Division of Administration Information Technology (DAIT) Branch, Regional Administrators, and Cyber and Physical Security Branch within the Division of Administration (DA) will have primary responsibility for sending messages and managing the system. They are identified as "dispatchers" and "users" respectively. All CFTC staff will receive the mandatory mass emergency notifications from EMNS at their CFTC email addresses, and on their government furnished equipment (GFE) (to include mobile phones and tablets).

Within EMNS, the term "contact" refers to CFTC staff who receive the mass emergency notifications from the EMNS system. "Dispatcher" refers to individuals who have administrative access and will be the sender of the mass emergency notifications and "users" refers to those with administrative access who develop and amend the notification templates within EMNS.

EMNS collects, maintains, and uses information about CFTC staff in the following ways: CFTC staff's business information will be provided from CFTC Entra ID (Previously known as Active Directory) to EMNS for the purpose of sending out mass notifications. Entra ID username and password will also be used for single sign on (SSO) of the "dispatchers" (The Security and Emergency Management Unit, the DAIT Branch, Regional Administrators, and the Cyber and Physical Security Branch staff with administrative roles in EMNS) to gain access to the system to send out the mass emergency notifications. "Users" of the EMNS such as the Security and Emergency Management Unit with administrative roles in EMNS for the purpose of creating and amending notification templates, provide EMNS with a username and password (separate from Entra ID). Lastly, CFTC staff's personal information will be pulled from the Personnel Clearence System (PCS) solution within the Management and Administrative Enterprise Database (MAED) platform into the CFTC system Emergency Contact System (EContact) for the purpose of sending out mass notifications to CFTC staff's personal contact information.

1. AUTHORITIES AND OTHER REQUIREMENTS

1.1 What legal authority(ies) permit or require the CFTC to collect, use, maintain, or disseminate the information in the system, project, or program?

The CFTC's authority to have a mass notification system and collect CFTC staff's emergency contact information derives from the Department of Homeland Security/Federal Emergency Management Agency's Federal Continuity Directive 1 (2017) and the Commodity Exchange Act (CEA), 7 U.S.C. 1 et seq., and the rules and regulations promulgated thereunder.

1.2 Is there a Privacy Act System of Records Notice(s) (SORN(s)) that applies to the information in the system, project, or program? If yes, please identify it. If no, please explain why not.

Yes. The CFTC-9, Emergency Locator System, and the CFTC-35, General Information Technology Records, SORNs apply to information in EMNS.

1.3 Please identify the applicable accreditation boundary evaluated during the Authority to Operate (ATO) process. If the system is hosted by a Cloud Service Provider (CSP), please identify the CSP and state whether the system has Federal Risk and Authorization Management Program (FedRAMP) authorization.

Everbridge Mass Notification System is an Operational Major Application with an ATO Boundary authorized on August 14, 2024. ENMS is located within the Everbridge SaaS environment which is a FedRAMP® certified cloud environment hosted within AWS Commercial Cloud-East/West.

1.4 Is there a records retention schedule(s) approved by the National Archives and Records Administration (NARA) that governs the retention of the records maintained in the system, project, or program? If yes, please identify the schedule. If not, please explain.

Yes, the EMNS records retention schedule is governed by the following General Records Schedules:

- GRS5-3-010: Continuity planning and related emergency planning files
- GRS5-3-020: Employee emergency contact information

1.5 Please list all forms or other information collection instruments that are used to collect the information in the system. If the information collected is subject to the Paperwork Reduction Act, provide the name of the form or information collection and the applicable OMB control number.

EMNS does not receive information directly from the individual to whom the information pertains. EMNS receives information from other CFTC systems such as CFTC Entra ID and EContact.

2. INFORMATION

2.1 Identify the information that the system, project, or program collects, maintains, uses, or disseminates.

EMNS collects, maintains, and uses Name, Username, Business Email Address, Business Phone (Desk Phone), Business Mobile Number, Department, Employee Identification Number (ID), Employee type, and Duty Station for all CFTC staff. In addition, EMNS collects, maintains, and uses Personal Mobile Number, Personal Home Phone Number, and Personal Email Address for CFTC staff who voluntarily choose to provide that information for EMNS use.

The "users" and "dispatchers" of the system will have their Entra ID Username and Password collected for single sign on (SSO) to gain access into EMNS. A select number of users will also have to provide a Username and Password (separate from SSO) in order to create break glass accounts (a set of backup credentials that allow users to sign into the EMNS platform directly without using SSO).

2.2 Is the information collected directly from the individual and, if not, what are the sources of information collected. How is the information obtained?

EMNS does not collect information directly from the individual. CFTC staff's business information to include Name, Username, Business Email Address, Business Phone (Desk Phone), Business Mobile Number, Department, Employee ID, Employee Type, and Duty Station are pulled from CFTC Entra ID (Previously known as Active Directory) as mandatory fields into EMNS through an Application Programming Interface (API) connection that syncs daily.

Username and Passwords of the "dispatchers" (The Security and Emergency Management Unit, the DAIT Branch, Regional Administrators, and the Cyber and

Physical Security Branch staff with administrative roles in EMNS) are pulled from Entra ID for SSO. "Users" of the EMNS such as the Security and Emergency Management Unit with administrative roles in EMNS provide EMNS with a username and password (separate from Entra ID).

CFTC staff's personal information such as Personal Mobile Number, Personal Home Phone Number, and Personal Email Address will be pulled from PCS within the MAED platform into EContact, where the data can then be maintained or updated (in the EContact application). CFTC employees can use the notification tab within EContact to set whether or not they would like receive notifications at their personal contact methods. For contract staff, they can sign a waiver within the EContact system and then enter their personal contact information directly within EContact.

Once CFTC staff's personal contact information is within EContact, EContact provides an option for the individual to opt in to receiving emergency notifications via their Personal Mobile Number, Personal Home Phone Number, and/or Personal Email Address. In the case that the individual opts in to receiving emergency notifications via their Personal Mobile Number, Personal Home Phone Number, and/or Personal Email Address, EContact will populate those data elements within EMNS. If the individual opts out, no personal data for that individual will be provided to EMNS and the individual will not receive notifications via their Personal Mobile Number, Personal Home Phone Number, and/or Personal Email Address. At the outset, CFTC staff's personal information will be manually uploaded via Secure File Transfer Protocol (SFTP) to EMNS from EContact. In future phases of deployment of EMNS, there will be an API connection between EContact and EMNS that syncs daily.

2.3 What steps are taken to minimize the collection of information in the system, project, or program?

Through discussions held during deployment preparations, the Everbridge Vendor, the CFTC Security Team, CFTC Privacy Office, and the EMNS System Owner were able to identify the elements that are relevant and necessary to accomplish the legally authorized purpose of collection. All information from Entra ID is mandatory to be able to identify and send out the mass notifications to the right individuals at the right time. The information received from EContact is voluntary. If a CFTC staff member does not want to receive mass notifications from EMNS to their Personal Mobile Number, Home Phone Number, and/or Personal Email, that individual would "opt out" within EContact and EMNS would not receive that individual's personal information. The voluntary information from EContact is provided to EMNS to provide the option for the CFTC to be able to contact CFTC staff in an emergency and to inform them of potentially dangerous or other urgent situations that they may otherwise be unaware of.

2.4 Discuss how the accuracy, integrity, and/or quality of the information identified above are determined.

EMNS receives data from CFTC Entra ID, PCS, and EContact. EMNS does not include the functionality to check and correct inaccurate or outdated information. The API connection with CFTC Entra ID and EMNS is synced every day at midnight to ensure the accuracy of the data within EMNS. From the outset, CFTC staff's Personal Mobile Number, Home Phone Number, and Personal Email Address will be provided to EMNS via a manual upload from EContact. In future phases of deployment of EMNS, there will be an API connection between EContact and EMNS that syncs daily which will ensure the accuracy of the data. The CFTC system Management and Administrative Enterprise Database (MAED) will also be providing mandatory data element Employee ID to EMNS via manual upload to ensure the data being pulled from EContact is accurately matched to the right profile within EMNS.

2.5 Privacy Impact Analysis: Related to the Collection and Characterization of the Information

In limited circumstances (such as the need to evacuate a CFTC building) a notification may be sent to CFTC staff that request the CFTC staff member to reply. Given the notification is sent via text message, there is a risk that CFTC staff members may provide more than the requested response (such as a narrative response) and that could contain PII that the system does not need to process the response. There is no removal or redaction process in place for the unrequested narrative response if it were to be provided by CFTC staff. The responses to notifications are not saved by the individuals name but can be searched by administrators within EMNS by the specific notification that was sent out.

EMNS has mitigated this risk of over-collection by templating the request for a reply in polling format which creates a standardized reply of "yes" or "no" or typing a number to indicate an answer (in order to notify the CFTC if the individual is safe from the event or not). EMNS has further mitigated the risk of collecting more information than necessary by establishing effective policies to avoid unnecessary collection of information.

3. USE OF THE INFORMATION

3.1 Describe how the information is used internally at the CFTC to support a business purpose.

The primary use of CFTC staff's business and personal information is for the CFTC Security and Emergency Management Unit, along with the DAIT Branch, Regional Administrators, and Cyber and Physical Security Branch to send out mass notifications to CFTC staff by phone, email or text message in the event of an emergency or mission-critical business event.

3.2 Identify all programs or offices, and an approximate number of individuals, within the CFTC that have assigned roles and responsibilities with respect to the system, project, or program or with whom information is shared. Explain how each uses the information.

The Security and Emergency Management Unit, along with the DAIT Branch, Regional Administrators, and Cyber and Physical Security Branch within the DA will have primary responsibility for sending messages and managing the system. They are identified as "dispatchers" and "users" respectively. Dispatchers have administrative access and will be the sender of the mass emergency notifications. Users will be a more limited set of individuals who will have administrative access to develop and amend the notification templates within EMNS.

3.3 Privacy Impact Analysis: Related to the Internal Access and Use

There is a risk of misuse of the information through unauthorized access to the information and a related risk that information within EMNS may be used in a manner that is inconsistent with the purpose for which it is being collected and maintained in EMNS.

This risk is mitigated through the use of Role Based Access Controls (RBAC) comprised of user provisioning, permissions management, and access controls. "User" and "dispatcher" access is also mapped to organizational duties performed to ensure that users are only accessing data specific to their authorized functions. Individuals within the division must show a need to access the EMNS data for their work within their division. EMNS further secures the information within the system through continuous audit logs which log events that are significant and relevant to the security of the EMNS and the environment in which it operates. There is also an automated process in place to continuously review and monitor audit logs for suspicious or unusual activity. Additionally, all "users" and "dispatchers" must agree to Rules of Behavior prior to being granted access to the system.

4. INFORMATION SHARING

4.1 Is the information shared outside of the CFTC as part of usual agency operations? If so, identify the organizations or individuals with whom the information is shared, how and *why* it is shared, and how it is to be used.

Information from EMNS is not shared outside of CFTC as part of usual CFTC operations. In the event any external sharing is necessary in particular circumstances, the information will only be disclosed as permitted by the Privacy Act, including pursuant to the routine uses in the applicable SORN.

4.2 How is the information sharing described in 4.1 compatible with the purpose for which it was originally collected described in 3.1?

Information from EMNS is not shared outside of the CFTC.

4.3 Is the information sharing documented in a Memorandum of Understanding, other information sharing agreement, or a contract?

Information from EMNS is not shared outside of the CFTC.

4.4 Are there limitations on re-dissemination of the information by the third party in place, either in the documents identified in 4.2 or otherwise?

Information from EMNS is not shared outside of the CFTC.

4.5 Describe how the system, project, or program accounts for and maintains a record of disclosures outside of the CFTC.

Information from EMNS is not shared outside of the CFTC. If it becomes necessary to disclose information as permitted by the Privacy Act, including relevant routine uses in the applicable SORN, the system owner will discuss how to best account for disclosures with the Privacy Office.

4.6 Privacy Impact Analysis: Related to Information Sharing

Information from EMNS is not shared outside of the CFTC and, therefore, there are no identified risks or necessary mitigation steps related to external information sharing.

5. DATA RETENTION

5.1 Explain how long and for what reason the information is retained.

In accordance with the applicable retention schedules as identified in section 1.4 above, records in EMNS are maintained until an employee is offboarded from the CFTC and their CFTC Entra ID is deleted. EMNS (due to the API connection with Entra ID) has a process in place where the offboarded employee's profile and information will be automatically deleted from EMNS.

5.2 Describe how the information is disposed of at the end of its retention period.

Once an employee is offboarded from the CFTC and their CFTC Entra ID is deleted, EMNS (due to the API connection with Entra ID) has a process in place where the offboarded employee's profile and all of their information will be automatically deleted from EMNS. Deleted contacts are kept within EMNS for 30 days in case the contact needs to be restored. The date that the contact was deleted is recorded as "last modified date". After the 30 days, the contact will be securely and completely deleted (permanently) from EMNS as an automated process.

5.3 Privacy Impact Analysis: Related to Retention

There is risk that information in EMNS may be retained longer than is necessary to meet the business need for which it was collected.

This risk is mitigated by adhering to the applicable records schedule, which addresses the business need to retain the information. When records are scheduled for destruction based on the retention schedule, the information is deleted securely and completely as part of the automated deletion process where an offboarded employee's profile and information will be automatically deleted from EMNS.

6. NOTICE

6.1 How are individuals provided notice prior to the collection of their information? If they are not provided notice, please explain why.

EMNS does not provide direct notice to individuals because the system does not collect information directly from them. However, this PIA and the CFTC-9, Emergency

Locator System, and CFTC-35, General Information Technology Records, SORNs provide general notice about the collection of individuals' information.

Individual CFTC staff are presented with a Privacy Act statement when they enter their information into the EContact system and are informed that the information will be used to notify them in the case of an emergency or mission critical business event.

6.2 Do individuals have the opportunity to consent to the use of their information or decline to provide their information? Please explain.

The information within EMNS is received from CFTC Entra ID and from EContact. As a result, consent does not occur within EMNS but rather implicitly when an individual accepts employment with the CFTC and explicitly when they voluntarily provide their personal information within EContact. Within EContact, CFTC staff have the ability to decline to have their personal contact information entered into EMNS by indicating "yes" or "no." At this time however, there is no technical ability to honor the consent choices. In addition, the Privacy Act statement in EContact states that providing their information is voluntary.

6.3 Privacy Impact Analysis: Related to Notice

There is a risk that CFTC staff are not aware that EMNS collects and uses their information.

The risk that CFTC staff may not be aware that EMNS uses their information is addressed through the publication of this PIA and through notice provided at the points of collection by other systems such as EContact that have direct contact with CFTC staff.

There is also a risk that consent choices are not being honored. Currently, all CFTC employees and contractors' personal contact information is being pulled from PCS into EMNS causing CFTC staff to receive mass notifications regardless of consent choices to the use of their personal contact information for mass notifications.

This risk is unmitigated as there currently is no technical ability to honor the consent choices. DA-IT is working to mitigate this risk.

7. REDRESS

7.1 What procedures are in place that allow individuals to access their information?

CFTC staff do not have direct access to EMNS. However, CFTC staff are able to access their personal contact information by accessing EContact through CFTC Entra ID SSO. There, CFTC staff are able to edit or amend their information directly within EContact.

Individuals may also request access to records about themselves that are included in the relevant systems of records by following the procedures outlined in the applicable SORNs.

7.2 What procedures are in place to allow individuals to correct inaccurate or irrelevant information about themselves?

CFTC staff do not have direct access to EMNS. If a CFTC staff member needed to update their personal information, that CFTC staff member would need to update their information within EContact. EContact is designed to allow CFTC staff direct access to their voluntary personal contact information. CFTC staff access EContact using CFTC Entra ID SSO.

Individuals may also request that records about themselves be amended by following the procedures outlined in the applicable SORNs.

7.3 How are individuals notified about the procedures for correcting their information?

The procedures for submitting a request to correct information are outlined in the applicable SORNs.

7.4 Privacy Impact Analysis: Related to Redress

There is a risk that CFTC staff may not be able to access information about themselves that is within EMNS nor be afforded adequate opportunity to correct that information.

This risk is mitigated by providing CFTC staff with access to correct and amend their personal information within EContact and, more generally, by providing individuals an appropriate opportunity to access and request amendment of their records via the process outlined in the applicable SORNs.

8. AUDITING AND ACCOUNTABILITY

8.1 How is the information in the system secured?

EMNS is a FedRamp authorized Software as A Service (SaaS) and all physical and environmental security controls are managed by and inherited from the Cloud Service Provider (CSP). In addition, CFTC staff access EMNS using CFTC Entra ID credentials for single sign on (SSO). and CFTC employs a firewall and Virtual Private Network (VPN). Administrative controls are also in place including CFTC Rules of Behavior and a standing CFTC Contingency Plan.

8.2 Are audit logs generated reflecting access and use of the information in the system? If not, please explain. If so, please describe how often they are reviewed and for what purpose.

Audit logs are generated for all activity within EMNS by recording whenever an action is being taken and by whom. Audit logs contain username and user ID of the individual who accesses EMNS. There is an automated process in place to continuously review/monitor audit logs for suspicious or unusual activity.

8.3. What procedures are in place to determine who has access to the system, and are they documented?

The CFTC Account Administrator (EMNS system owner) has the responsibility of determining role-based access needs. The Account Administrator must review role assignments on an annual basis.

8.4 Describe what privacy training is provided to users, either general or specific to this system or project.

All CFTC staff are required to complete Cybersecurity and Privacy Awareness Training, which is a prerequisite and annual requirement for access to the CFTC network. In the case that a "user" and/or "dispatcher" did not complete required annual training, access to the CFTC network, including access to EMNS, would be disabled.

8.5 Privacy Impact Analysis: Related to Auditing and Accountability

There is a risk that audit logs are inconsistent or unreliable and that the CFTC information technology and security personnel are unaware of their responsibilities respective to reporting breaches or other incidents.

This risk is mitigated through robust audit logs. EMNS audit logs are created continuously whenever an action is taken within the system. The auditing and review of audit data is an automated process where audit logs are continuously reviewed for

suspicious or unusual activity. When audit logs indicate suspicious, abnormal or malicious activity, information technology and security personnel are aware of the procedures to report suspected and confirmed breaches and other incidences. All CFTC staff receive annual Cybersecurity and Privacy Awareness Training (CPAT) and Records Management training required to maintain access to CFTC information systems. CFTC staff are aware of how and when to report potential and actual incidents and breaches and are bound by the CFTC Rules of Behavior.