Emergency Notification System Handbook

September 2019

FEMA

CONTENTS

List of Figures

List of Tables

CHAPTER 1: ORGANIZATION

Purpose

The purpose of the *Emergency Notification System Handbook* is to provide a comprehensive collection of information regarding the proper and effective use of the Emergency Notification System (ENS). The direction provided in the *Emergency Notification System Handbook* should be used to guide operational policy.

The Federal Emergency Management Agency (FEMA) Operations Center (FOC), as executive agent responsible for directing and managing the ENS, must be prepared to perform alerts, notifications, warnings, and other similar operations during all threats and emergencies and be able to effectively resume essential operations if they are interrupted. The FOC supports FEMA headquarters (HQ) and interagency alerting and notification for disaster response and continuity of operations. In addition, ENS is available for use by regional watch centers (RWC) and Mobile Emergency Response Support (MERS) operations centers (MOC) to support notification within their areas of responsibility. The Department of Homeland Security (DHS) HQ and other DHS components also use ENS to varying degrees to notify their teams and personnel. The *Emergency Notification System Handbook* provides overall DHS organizational program guidance for the ENS to help these organizations perform their operational duties as efficiently as possible.

Effective notification is simply a "good business practice," part of the fundamental mission of agencies as responsible and reliable public institutions. Today's changing threat environment and recent emergencies, including localized acts of nature, accidents, technological emergencies, and military- or terrorist attack-related incidents, have increased the need for emergency alert and notification capabilities and an effective ENS that enables agencies to continue their essential functions across a broad spectrum of emergencies.

The following ENS objectives have been established for all DHS components, as defined in the DHS Continuity of Operations (COOP) plan:

- Ensure the continuous performance of the component's essential functions/operations during an emergency.
- Protect essential facilities, equipment, vital records, and other assets.
- Reduce or mitigate disruptions to operations.
- Reduce loss of life, minimizing damage and losses.
- Ensure a timely and orderly recovery from an emergency and resumption of full service to customers.

Scope and Applicability

ENS is capable of sending notifications to individuals and groups as defined by each DHS operational program to support alerting requirements. The messages are intended to be critical in nature but may also be sent for testing critical notification processes. All messages are sent to personnel via documented communication devices (i.e., home telephone, work telephone, mobile telephone, short message service [SMS]/text messaging, and email). The guidance provided in the Emergency Notification System Handbook is applicable to all DHS organizational components and FEMA elements, as required.

Approved Uses

ENS consists of multiple redundant platforms and robust telecommunications and network resources; however, system capacity is not unlimited. For this reason, ENS use should be reserved for its intended purposes of **disaster response support** and **continuity of operations**. Use for routine administrative notifications of a nonemergency nature or for logistics management should be avoided. ENS is not functionally designed for use as a personnel accountability system and, unless unusual circumstances exist, should not normally be used for this purpose. Employee notices and human resource-oriented information should also be distributed using other systems. In addition, while notifications are delivered to interagency disaster response and continuity partners, activation of ENS is reserved for FEMA and DHS operations centers and watches.

Scope of ENS Activities

ENS has become a very valuable tool for emergency management within FEMA. As noted in other sections of the *Emergency Notification System Handbook*, there are several other DHS components that use the FEMA-owned and -managed ENS.

The wide customer base also includes a variety of operational objectives. This means that all must all share this resource and manage it in such a manner that it will not negatively affect the operational missions. Therefore, all must recognize the level of cooperation, participation, and compliance required to maintain this critical success.

Authorities and Foundational Documents

- Executive Order 12656, Assignment of Emergency Preparedness Responsibilities
- Federal Executive Branch National Continuity Program and Requirements (October 2012)
- National Security Presidential Directive (NSPD)-51/Homeland Security Presidential Directive (HSPD)-20: *National Continuity Policy*

- Federal Continuity Directive 1: Federal Executive Branch National Continuity Program and Requirements
- FEMA Directive 262-3, *Web 2.0 Policy*
- FEMA Directive 262-3 ENS Directive, 2019
- FEMA P-1001, *FEMA Watch Guide* (January 2019)

CHAPTER 2: FEMA OPERATIONS CENTER ACTIVITIES

Overview

FEMA's Response Directorate, specifically the FOC, has been designated as DHS' executive agent for oversight and management of the ENS. The FEMA Alternate Operations Center East (FAOC-E) in Thomasville, GA, and the FEMA Alternate Operations Center West (FAOC-W) in Denver, CO, will serve in a backup capacity to the FOC for all ENS and other operational requirements. Inherent in this role is the responsibility to formulate guidance for all DHS components to use in developing viable, executable ENS policies (such as data, groups, contacts, and scenario policies) to facilitate orientation and training, as appropriate, and to oversee and assess the operation of the ENS to support disaster response and critical continuity programs.

The FOC is also the activation point for FEMA HQ-based disaster response teams and for FEMA and interagency continuity notifications. Requests for FOC support for other types of notification support or for use of ENS should be vetted through FEMA's Response Directorate and Operations Division. Figure 1 shows the implementation of the ENS at the FOC.

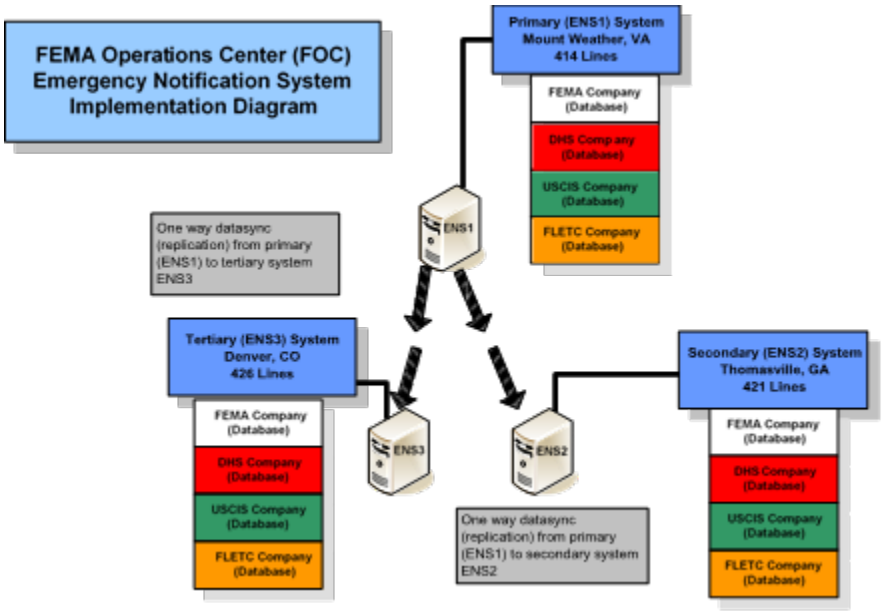


Figure 1: FEMA Operations Center Emergency Notification System Implementation

Operations

The ENS has internal security safeguards, which are managed by the FOC ENS-Administration (ENS-Admin) team. Additionally, the ENS is a component of FEMA's information technology (IT) infrastructure, which is managed by the FEMA Office of the Chief Information Officer (OCIO). Responsibility for maintaining a secure environment is the dual requirement of the FOC and FEMA IT and is a responsibility of every ENS user.

Specific instructions for the ENS components, such as messages, scenarios, and other features, are documented in the *ENS Standard Operating Procedures*, and are available to authorized system users who request them.

DHS is committed to a rapid response and recovery for all of its organizational components in the event of an emergency or threat to national security. The decision to activate the ENS will be made by the appropriate authorizing official for each supported program or team. If an emergency affects an individual DHS component, the leadership of that component can make the decision to activate their individual scenarios in accordance with established ENS procedures and component policies. The Secretary of Homeland Security or his/her designee can direct activation of scenarios for all DHS components. The operations center performing the actual ENS activation will verify that the requesting official has the required authority.

ENS-Administration Team

An ENS-Admin team has been developed to ensure that system administration and maintenance are performed in a standardized method. As expansion of ENS continues, the roles and responsibilities of ENS-Admin team members will also expand. Contact information for the ENS-Admin team members is in Appendix D: ENS POC Contact and Information.

The ENS-Admin team is the authority for all ENS technical matters. The ENS-Admin team administers and maintains the ENS servers, hardware, and software and performs operational management and policy development.

Because of the large number of programs using ENS, the ENS-Admin team provides training and system credentials to DHS and FEMA program points of contact (POC) so that they can manage their program's ENS contacts and groups. End users should contact their respective POCs for questions, issues, support, etc. Only POCs should contact the ENS-Admin team if they have issues they are unable to resolve.

The ENS-Admin team will assist POCs and other operations centers to refine scenarios toward their specific mission requirements. This may include group, contact, and scenario

creation. This effort may also involve developing tests for the individual groups and assistance with follow-up reporting. The ENS-Admin team will also coordinate these efforts with the FOC operations teams prior to implementation.

Contact Information

- Email: ENS-admin@fema.dhs.gov
- ENS SharePoint site: https://intranet.fema.net/org/orr/collab/response/omd/rcb/foc/ens/Pages/default.aspx
- FOC Intranet site: https://intranet.fema.net/org/orr/response/foc/Pages/default.aspx

CHAPTER 3: OFFICE OF CHIEF INFORMATION OFFICER ROLES AND RESPONSIBILITIES

Enterprise Service Desk

The Enterprise Service Desk (ESD), FEMA's technical support element, serves as the 24-hour POC for ENS technical support. Although ESD is the first point of contact for ENS users, it does not generally have the ability to provide support or guidance regarding issues related to the system, specifically. The ESD can, however, notify the ENS-Admin team about the problem and relay the associated information received from the component POC. This procedure enables after-hours logging of ENS issues.

Users should also address system issues with their program's ENS POC and should not contact the ESD directly. POCs can provide training and assistance to end users, or, when necessary, the POC may contact the ENS-Admin team or ESD for support. Chapter 5: ENS POC Responsibilities provides details regarding POC responsibilities.

Enterprise Network

The ENS relies on the DHS/FEMA enterprise network for connectivity. The ENS-Admin team must coordinate with the OCIO and several IT organizations for proper access and configuration. When these services become unavailable, some or all of the ENS features or functions may also be unavailable. The network services provided by the OCIO include the following:

- Telecommunication services for telephone messages;
- Microsoft Outlook for email and email qualification;
- Data network for account management, application interface, reports, and database management;
- Firewalls and other security devices; and
- Personal Identity Verification (PIV) authentication (Security Assertion Mark-up Language [SAML]).

CHAPTER 4: COMPONENTS OVERVIEW AND FEMA NOTIFICATION STRATEGY

In order to manage contact data and provide assistance to component users, each component will designate a POC, who will assign and manage administrator rights for his/her respective component. This will ensure maximum efficiency of administration and operation for the 15,000-plus contacts. Further, each component should comply with the guidance established within the *Emergency Notification System Handbook*.

Figure 2 shows the relationship among these components.

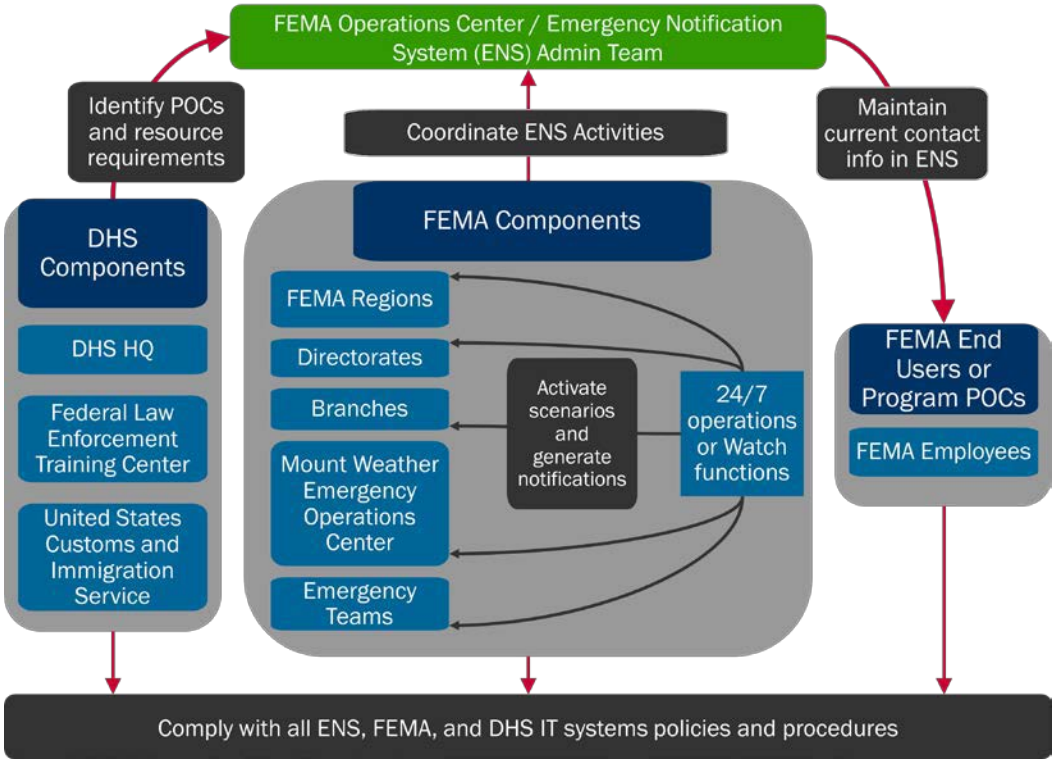


Figure 2: Component Relationships

As shown in Figure 2, there are three classes of ENS users, as defined next.

DHS Components

DHS components must comply with all ENS, DHS, and individual component IT systems policies and procedures. Each component has designated one or more POCs, who will manage ENS data within their respective components. DHS components include the following:

- DHS HQ
- Federal Law Enforcement Training Center (FLETC)
- U.S. Customs and Immigration Service (USCIS)

FEMA Components

FEMA regions, directorates, branches, the Mount Weather Emergency Operations Center (MWEOC), and emergency teams are examples of FEMA components. These components have assigned a POC to manage their respective information within ENS. In addition, each FEMA component is served by a 24/7 operations or watch function, with responsibility for activating scenarios (generating notifications) for that component. These elements and POCs must comply with all ENS, FEMA, and DHS IT systems policies and procedures.

FEMA End Users (Contacts)

FEMA end users are all employees who receive a notification from ENS or log into ENS to manage their contact information. All FEMA users must comply with all ENS, FEMA, and DHS IT systems policies and procedures.

Component Activities

ENS usage rules and policies generally apply to all users; however, these may be modified to conform to the situation and component policies. For example, FEMA-specific requirements will not apply to other DHS components. All DHS organizational components must be prepared to activate and manage scenarios and all other data related to their respective operational requirements.

Component ENS activities must be coordinated through the FOC/ENS-Admin team using established operational guidelines. To assist with this, all DHS components must become familiar with the guidance provided in the *Emergency Notification System Handbook*.

Each DHS component will provide rosters and scenario requirements to the FOC/ENS-Admin team and then periodically update them, as directed, in addition to notifying the FOC/ENS-Admin team of personnel changes within its component.

FEMA Notification Strategy

Notification scenarios within FEMA are activated by FEMA's network of operations centers in response to specific events, as directed by checklists or standard operating procedures.

Checklists may prompt the activation of scenarios directly or they may have steps that first involve contacting decision makers who can direct various activations or other notifications. In addition, program managers or POCs may contact their supporting operations center to request activation of specific scenarios for tests or exercises or during real-world events. In general, the FOC activates specific scenarios for FEMA HQ teams and programs and for the MWEOC. MOCs or RWCs activate specific scenarios for their regions and areas of responsibility (AOR).

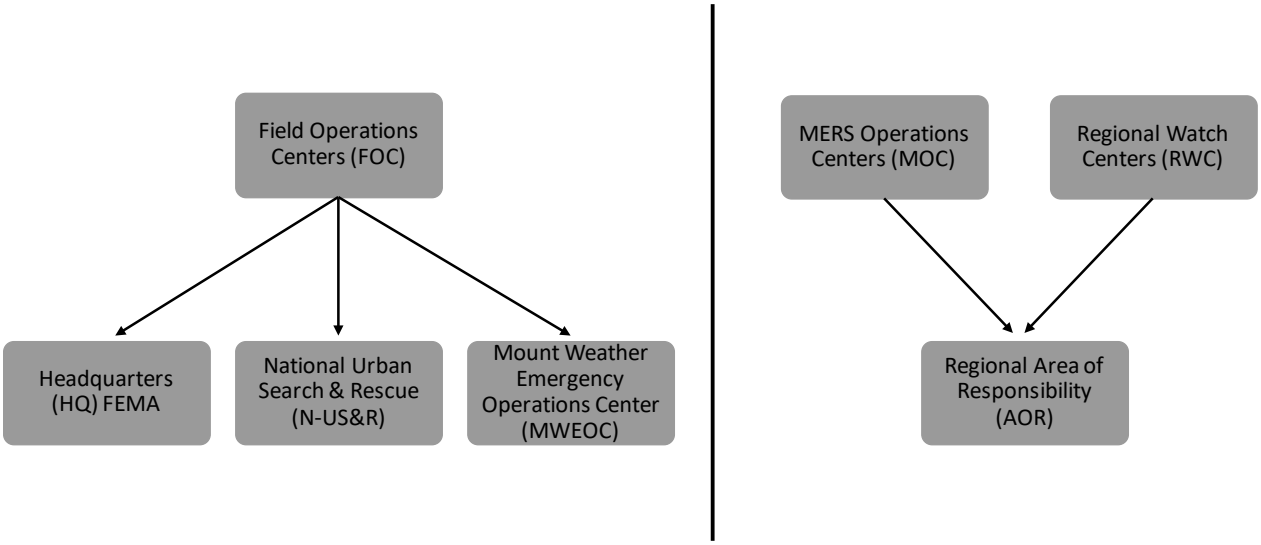


Figure 3: Notification Strategy

As shown in Figure 3, for FEMA-wide notifications the FOC will notify FEMA HQ elements and the National Urban Search and Rescue (US&R) teams and will direct the MOCs and RWCs to disseminate notifications regionally. The MOCs and RWCs will subsequently notify US&R teams within their regional areas of responsibility, as required.

MERS Operations Center Description

MOCs activate on behalf of one or both of the regions that their detachments support. MOCs are the POCs for the US&R teams and activate the US&R teams. MOCs provide Tier 1 support for ENS issues and questions within their area of responsibility.

Regional Watch Center Description

Like the MOCs, RWCs are staffed 24/7 and manage the data and activate scenarios in

accordance with the *FEMA Watch Guide* and their regional policies and procedures. The RWCs can also provide Tier 1 ENS support. A list of regional POCs is in the ENS POC roster in Appendix D: ENS POC and Contact Information.

Training

A number of training topics and documents can be found on the ENS collaboration site: https://intranet.fema.net/org/orr/collab/response/omd/rcb/foc/ens/Pages/default.aspx.

Additional training may be available by contacting the ENS-Admin team.

CHAPTER 5: ENS POC RESPONSIBILITIES

Table 1 lists the responsibilities of each ENS POC.

Table 1: ENS POC Responsibilities

Responsibility / Restrictions	Details
Each component must develop its own internal Emergency Notification System (ENS) policies and plan for operational use based on its specific requirements.	• This plan must be provided to the ENS-Administrative (ENS-Admin) team. • Each component must understand and agree that system usage during an emergency situation may warrant a shutdown of test scenarios to proceed with real-world activations.
Members of the Federal Emergency Management Agency (FEMA) Operations Center (FOC)/ENS-Admin team must be granted administrator rights to all companies.	• Members assist individual Points of Contact (POC) with administrative tasks. • Members facilitate support from the ENS-Admin team. • Members allow the FOC to monitor and manage scenario activations.
Information for non-Department of Homeland Security (DHS) team members receiving ENS notifications must be entered or imported via a DHS POC.	• Most contacts from each program have access to the FEMA network and can update their own contact information in ENS. • The accuracy of the contact data is the responsibility of the POC.
Text and speech segments of all messages must be professional in nature.	• Inflammatory language must not be used. • Messages should remain as brief as possible.
Include only small attachments in email messages.	• The size of these attachments could negatively affect performance and resources.
Lists of component POCs must be provided to the FOC.	• Each component and its designated POC are responsible for maintaining and managing their individual rosters, groups, contacts, etc., as defined by operational requirements. • Only authorized POCs and designated program personnel may request activation of individual teams for testing or operational purposes. The authorized activation requestor must properly complete the “Request for Activation” form in Appendix E: Request for Activation and submit it to the FOC.

Responsibility / Restrictions	Details
All component POCs must sign the ENS rules of behavior and are responsible for ensuring that their users abide by these rules.	• Refer to Appendix F: Ensures Rules of Behavior.
Components should limit their administrative accounts to the extent that this limitation does not interfere with the component's mission.	• Component-shared accounts are not permitted.
Messages for profit activity or personal use or advertising of a product or service or political messages or to obtain telephone numbers of individuals or businesses are strictly prohibited.	• The only exception to this would be telephone calls made to personnel to update their contact information.
No additional software must be installed on the ENS.	• Installation of software may violate the ENS warranty and support and maintenance agreement.
Persons authorized to operate (activate scenarios) ENS must not reveal how to activate ENS or broadcast improper or erroneous information.	N/A
Each component must create a technical support structure.	• The following are example support structures: o Tier 1 support will handle common basic requests, such as changing/adding a telephone number or resetting a password. o Tier 2 support will assist with scenario creation and activation, group management, and report reviews.
POCs and administrators of each component must attend formal training conducted by the ENS-Admin team.	N/A

Note: These tasks are not a comprehensive list of support requirements but represent the types of tasks that may be performed. Each component should carefully review all reports and other related information before continuing to Tier 3 support.

Appendix G: Point of Contact Duties for ENS POC Program contains specific requirements regarding the various duties of the POCs. In order to successfully manage and operate the ENS, these tasks must be accomplished regularly. By incorporating these duties into the POC's responsibilities, all users will have a better understanding of the ENS; therefore, a higher level of notification response will be achieved.

Note: No component or user is authorized to contact the vendor directly for support or for other questions or issues. All inquiries must be directed to the appropriate POC. POCs may contact the FOC ENS-Admin team.

CHAPTER 6: ENS CONTACTS

A contact is a recipient of an ENS alert or notification message. Contacts are considered the ENS end-user. Each contact has his/her device information loaded into the ENS database. ENS uses this contact device information to send or receive alerts and notifications.

Roles and Responsibilities

All contacts must comply with the rules and policies defined in the *Emergency Notification System Handbook*.

- Contacts must know who their POC is and should coordinate with the POC regularly.
- Contacts should notify their POC of changes within their contact profile, such as a change in name, new or updated device contact information, etc.
- Contacts are not authorized to request support from the ENS-Admin team, but should first consult with their POC for questions or support issues.

Training/Procedures

If the secondary or tertiary (FAOC-E/W) systems are used for scenario activation, users will receive notification via another toll-free telephone number.

All response procedures remain the same. For FEMA contacts, the telephone number for ENS2 is 877-216- 2044 (FAOC-E); the telephone number for ENS3 is 888-540-2682 (FAOC-W). There is no difference in the activation or call-back sequence. The only difference end users will see is the telephone number itself.

The ENS relies upon a unique user identification (ID) number to ensure that only authorized persons are allowed access to the messages contained within it. For FEMA, the user ID is typically the user's home telephone number, including the area code; for example: 123-456- 7890, followed by the pound (#) sign.

Note: Until "qualified" by the ENS, users will continue to be notified (via phone, e-mail, etc.). Adherence to the following instructions is the only way to successfully qualify.

Users should review the following steps to become familiar with the notification and response procedures. Users should pay close attention to Step 5 in order to properly complete the notification sequence.

1. When contacted via telephone by the ENS, answer in a loud, clear voice or ENS may assume it has reached an answering machine or fax and will hang up. If notified by

the ENS, a toll-free telephone number will display to call 800-713-6125 (primary system ENS1), 877-216-2044 (secondary system ENS2), or 888-540-2682 (tertiary system ENS3).

2. Users will be prompted to identify themselves to ENS by entering their user ID followed by the pound (#) sign.
    a. The user ID is typically the contact's home phone number.
    b. The user ID must not contain personally identifiable information (PII) such as SSN. The use of PII is a security violation, and the contact may be removed from ENS.
3. After entering the user ID correctly, a recorded message will deliver information and instructions relevant to the alert, activation, or notification.
4. Listen carefully to the message. The last part of the message will state, "Please stay on the line for further instructions." If the user hangs up at this point, the message will end and the user will not be qualified. (The ENS will continue to call). Remain on the line as instructed. The message will state, "Would you like to have the message repeated? Press 1 for yes and 2 for no." To acknowledge receipt of the message, press 2 or press 1 to repeat the message. After pressing 2, the user will then be qualified and will not be contacted again by the ENS.
5. Hang up only after the recording states: "Thank you. Goodbye."
6. Users may also qualify via email. After receipt of an email qualification message from ENS, click "Reply," type "Yes," and click "Send."
7. Users may receive a notification that asks for an estimated time of arrival (ETA). After the message is delivered, ENS will ask if the user can respond. Press 1 if able to respond. Instructions will be given to enter the ETA in military time. For example, an entry of 1300 is 1 p.m. Follow the remaining prompts, as instructed.

Key Points to Remember

- Respond quickly. Most scenarios last a maximum of 90 minutes.
- Accurately enter the user ID.
- Listen to the entire message.
- Call the POC or local MOC toll-free telephone number if experiencing problems.

CHAPTER 7: POLICIES AND BEST PRACTICES

The ENS will be utilized to notify FEMA, DHS personnel, and other related agencies of emergency situations. These messages will serve as a notification to prompt immediate action to resolve or mitigate the situation at hand and further communicate the status of the situation. Operational control and administration of ENS will be the responsibility of the FOC. The FOC director will guide daily operation of ENS.

Each component will designate a POC, who will assign and manage administrator rights for his/her respective component. In addition, each component should comply with the following policies:

ENS Standards

The standards and best practices listed below will help ensure a uniform application of system processes and procedures. They will help in the administration and maintenance of ENS as well as assist in proper usage. Please contact the ENS Admins at ens-admin@fema.dhs.gov for questions, issues, or to report misuse.

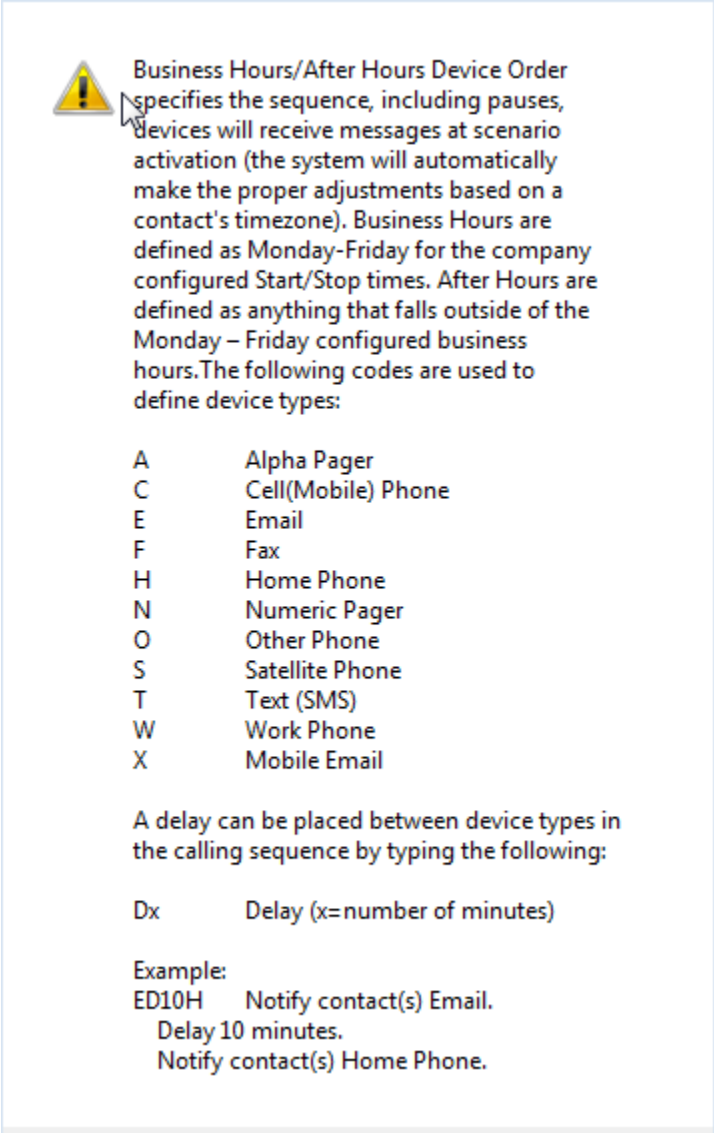
- A contact's Login Name should match their FEMA email address.
- A contact's UserID should be either a 10-digit home phone, or if a home phone is unavailable use a personal cell phone number.
- Include the FOC Communicator Quality Assurance (QA) group in all non-in house test scenarios. They should be first on the list of groups contacted.
- All **email messages** should include:
    - Identify the sending entity (e.g., This is the **FEMA Operations Center** with an important message…) and for whom the message is intended (e.g., **for the National Response Coordination Center [NRCC]**.)
    - At the end of the message make sure to include the duration of the scenario (e.g., This notification will **expire 90 minutes** from %StartTime% EST.), and include the %CompanyCallBack% Autotext.
- In the **voice recorded** messages include:
    - Identify the sending entity (e.g., This is the **FEMA Operations Center** with an important message…) and for whom the message is intended (e.g., **for the NRCC**.)
    - At the end of the recorded message state: "Please stay on the line for further instructions."
- Clean up **only** your messages and copied scenarios within a day after they are activated, unless directed otherwise by the ENS-Admin team.

- Clean up reports **only** you generate within the day you have pulled them from ENS.
- ***Remove individuals upon their departure from FEMA.*** Leaving them in the system is a security issue, and they may still be contacted by the system.
- Utilize the custom fields "Notes" and "Position" for other contact information or an individual's title.
- Do not list a call center or common phone number for a contact's device. This will create confusion during an activation as the system will be looking for different UserIDs.
- The Secondary (ENS2) and Tertiary (ENS3) systems are **not to be utilized unless directed otherwise by the ENS-Admin team or the FOC**. During emergency situations you may be directed to utilize either.
- Adhere to the ENS testing period schedule, unless directed otherwise:
    - ENS 2 – Every Wednesday from 0800 to 1500
    - ENS 3 – Every Thursday from 0800 to 1500
- When activating a scenario:
    - Verify the volume of the voice recording is audible.
    - Double check the message to make sure it is accurate.
    - If there is a problem (incorrect message, wrong email attachment, etc.) stop the scenario immediately and correct the issue. If it is a system issue, alert the ENS-Admin team.
- Create an in-house test scenario for testing purposes. Do not create instant activations for the purposes of testing the program.
- Stay within your set 3-digit scenario range. Do not deviate from that range as it will create confusion amongst others utilizing the system.
- Do not check the box "Send selected Voice message as an email attachment" when assigning messages to a scenario.
- Do not contact the vendor for anything related to the FEMA ENS. Only ENS-Admin team should be notified of an issue (ens-admin@fema.dhs.gov).
- Do not assign administrator rights without prior authorization from the ENS-Admin team. See ENS Admin Checklist and Rules of Behavior.
- Personally Identifiable Information (PII)
    - All use of PII data within ENS is strictly confined to emergency alerting, warning, notification, and official informational purposes only.
    - ENS PII data must NOT be shared either internally or externally to the agency.
    - All ENS PII data must be protected to the greatest extent possible by the operating office.
    - Misuse of PII data must be immediately reported to ens-admin@fema.dhs.gov.

Best Practices

- Utilize the email qualification method. Begin the device notification order with ED3 (email, delay three [3] minutes) to allow contacts time to reply. This allows more available phone lines since many contacts qualify by email.
- Create template scenarios on ENS for known events (Disaster Declarations, Incident Management Assistance Team [IMAT], Emergency Relocation Group [ERG], etc.), and create a general notification scenario for other events.
- Copy the template using copy scenario and rename it to reflect the event. Templates and instant activations are not for normal use.
- Use the following naming convention when working with a copied scenario in ENS: < 3-digit number series > < name of location activating scenario > < name of event > < initials of the individual who built the scenario > . For example: 000 FOC Disaster Declaration DLH . This is not required for in house test scenarios.
- Also, when using a copied scenario have the scenario ID reflect the date and time the scenario will be activated. This allows for awareness on the scenario, as well as an idea of when the scenario can be cleaned up. For example, a copied scenario that is to be activated on August 13, 2012 at 8:36pm would look like 101320122036.
- In an effort to recognize which activations are coming up, we recommend you use the first number in your number set. For instance, Thomasville is 100-199, so they should use 100 when activating copied scenarios.
- Use the same naming convention on the messages for a scenario. This will allow for easier recognition of the messages for clean-up.
- Utilize dynamic groups for long-term use, and static groups for one-time activations where a dynamic group will not suffice.
- Create voice messages for scenarios rather than using text to speech, if capable. This is easier to generate and much easier to understand when the message is sent out.

Figure 4 shows the ENS device codes.



Business Hours/After Hours Device Order specifies the sequence, including pauses, devices will receive messages at scenario activation (the system will automatically make the proper adjustments based on a contact's timezone). Business Hours are defined as Monday-Friday for the company configured Start/Stop times. After Hours are defined as anything that falls outside of the Monday – Friday configured business hours.The following codes are used to define device types:

A	Alpha Pager
C	Cell(Mobile) Phone
E	Email
F	Fax
H	Home Phone
N	Numeric Pager
O	Other Phone
S	Satellite Phone
T	Text (SMS)
W	Work Phone
X	Mobile Email

A delay can be placed between device types in the calling sequence by typing the following:

Dx	Delay (x=number of minutes)

Example:
ED10H Notify contact(s) Email.
Delay 10 minutes.
Notify contact(s) Home Phone.

Figure 4: ENS Device Codes

CHAPTER 8: ENS SECURITY

Overview of ATO and C&A Activities

The ENS-Admin team is responsible for maintaining the ENS authority to operate (ATO) as required by the *Federal Information Security Management Act* (FISMA). However, every ENS user is responsible for compliance with all DHS/FEMA security requirements.

The ENS-Admin team has completed all the necessary FISMA requirements. The ENS is fully compliant with all certification and accreditation (C&A) mandates and has a valid ATO.

Requirements

ENS is approved for unclassified information only. In addition, personal contact information in ENS is to be used for notification purposes only. ENS should not be used as a "phonebook" and numbers should not be shared or copied to other documents. All ENS security concerns or issues must be immediately reported to the ENS-Admin team. Every user is responsible for protecting ENS data. This means compliance with all security requirements and maintaining a high security posture is important.

CHAPTER 9: ENS PHYSICAL DESCRIPTIONS

The FEMA ENS located within the FOC at MWEOC serves as the primary system. The critical data is replicated to a secondary system located in the FAOC-E in Thomasville, GA, and a tertiary system in Denver, CO (FAOC-W). The FAOCs serve as the backup systems for all FOC ENS and operational functions and responsibilities.

Data changes are replicated every four (4) hours, and a full replication takes place daily. When a user logs into the secondary or tertiary systems, the replication is automatically stopped. Furthermore, changes made to information while in the secondary and/or tertiary systems will not replicate to the primary system therefore, no data changes should be made while on these backup systems. The secondary and/or tertiary systems should only be used for sending notifications.

The advantages of secondary and tertiary systems and the role of the FAOCs are as follows:

- Redundancy of data
- Load balancing of scenarios
- Offsite operators are able to activate scenarios

The use of ENS2 and ENS3 is permitted in the following circumstances:

- Every Wednesday from 8 a.m. to 3 p.m.: ENS2;
- Every Thursday from 8 a.m. to 3 p.m.: ENS3; and
- As directed by the FOC or ENS-Admin team.

Logging onto the backup systems for another reason is not authorized.

ENS1: Primary system (ENS1) (FOC) – Server A: Web server, Server B: Structured Query Language (SQL) server/controller, three (3) additional nodes that host the T-1 lines. Primary system line configuration – 400 T-1 lines total.

ENS2: Secondary system (ENS2) (FAOC-E) – Server A: Web server, SQL server, and NITE XML Toolkit (NXT) controller and four (4) nodes host the T-1 lines. Secondary system line configuration – 400 lines total.

ENS3: Tertiary system (ENS3) (FAOC-W) – Server A: Web server, Server B: SQL server/controller, two (2) additional nodes that host the T-1 lines. Tertiary system line configuration – 400 lines total.

All three systems reside on the FEMA network and use the resources of that network.

CHAPTER 10: SUMMARY

Each organizational component within DHS must plan for, train, test, and evaluate its ENS implementation. In order to accomplish this, the direction provided in the *Emergency Notification System Handbook* should be used as a guide for operational policy. This policy must be modified as the operational requirements change.

Each component must take the responsibility of system management very seriously, so everyone can share in its success.

The ENS will be utilized to notify FEMA, DHS personnel, and other related agencies of emergency situations and all-hazard notifications according to *the National Response Framework* (NRF). These messages will serve as a notification to prompt immediate action to resolve or mitigate the situation at hand and further communicate the status of the situation. Operational control and administration of ENS will be the responsibility of the FOC. The FOC director will direct daily operation of ENS.

APPENDIX A: LIST OF ACRONYMS

AOR	Area of Responsibility
ATO	Authority To Operate
C&A	Certification and Accreditation
COOP	Continuity of Operations
DHS	Department of Homeland Security
ENS	Emergency Notification System
ERG	Emergency Relocation Group
ESD	Enterprise Service Desk
ETA	Estimated Time of Arrival
FAOC-E	FEMA Alternate Operations Center East
FAOC-W	FEMA Alternate Operations Center West
FEMA	Federal Emergency Management Agency
FISMA	Federal Information Security Management Act
FLETC	Federal Law Enforcement Training Center
FOC	FEMA Operations Center
HQ	Headquarters
HSPD	Homeland Security Presidential Directive
ID	Identification
IMAT	Incident Management Assistance Team
IT	Information Technology
MERS	Mobile Emergency Response Support
MOC	MERS Operations Center
MWEOC	Mount Weather Emergency Operations Center
NOC	National Operations Center
NRCC	National Response Coordination Center
NRF	National Response Framework
NSPD	National Security Presidential Directive
NXT	NITE XML Toolkit

OCIO	Office of the Chief Information Officer
PII	Personally Identifiable Information
PIV	Personal Identity Verification
POC	Point of Contact
QA	Quality Assurance
RWC	Regional Watch Center
SAML	Security Assertion Mark-up Language
SMS	Short Message Service
SQL	Structured Query Language
USCIS	U.S. Customs and Immigration Service
US&R	Urban Search and Rescue

APPENDIX B: GLOSSARY

Activation of the Continuity of Operations (COOP) plan: The activation of the COOP plan is the initiation of the process of executing the COOP plan.

Company: A company is a separate database for each component. Therefore, each component's data is completely separate from all others. However, all companies use the same collective resources (T-1 lines, etc.)

Continuity of operations (COOP): COOP comprises internal organizational efforts to ensure that a viable capability exists to continue essential functions across a wide range of potential emergencies through a notification system and procedures that delineate essential functions. COOP specifies succession to office and the emergency delegation of authority, provides for the safekeeping of vital records and databases, identifies alternate operating facilities, provides for interoperable communications, and validates the capability through tests, training, and exercises.

Emergency Notification System (ENS): ENS provides alerts, notifications, warnings, and other similar operations during all hazards, threats, and emergencies to designated FEMA personnel, DHS employees, detailees, contractors, and employees of other participating federal, state, and local agencies and non-governmental organizations in the event of a scheduled exercise or an actual emergency.

ENS contact: An ENS contact is a recipient of an ENS alert or notification message. ENS contacts are considered the ENS end user. Each ENS contact has his/her device information loaded into the ENS database. ENS uses this contact device information to send or receive alerts and notifications.

Enterprise Service Desk (ESD): ESD is FEMA's technical support element. The ESD may notify the ENS-Admin team about problems and relay the associated information received from the component POC.

Executive agent: FEMA is the appointed executive agent for the federal executive branch for all ENS activities and planning.

FEMA Alternate Operations Centers (FAOC): The FAOC in Thomasville, GA (FAOC-E), hosts the secondary notification system, and the FAOC in Denver, CO (FAOC-W), hosts the tertiary notification system.

FEMA Operations Center (FOC): The FOC is located at Mount Weather, VA, and hosts the

primary notification system and is the ENS owner and steward.

Incident Management Assistance Team (IMAT): IMATs are full-time, rapid-response teams with dedicated staff who deploy within two (2) hours and arrive at an incident within 12 hours to support the local incident commander. IMATs support the initial establishment of a unified

command and provide situational awareness for federal and state decision makers crucial to determining the level and type of immediate federal support that may be required.

Mobile Emergency Response Support (MERS) Operations Centers (MOC): MOCs are the POCs for and activate the US&R teams. MOCs provide Tier 1 support for ENS issues and questions within their area of responsibility.

National Operations Center (NOC): NOC is DHS' primary operations center and is the operations and coordination central point for DHS.

Non-specific threat: A non-specific threat refers to a threat condition being implemented for a national declaration.

Point of contact (POC): POCs are the staff designated by the leadership of an organizational component who would be the main point of contact for all ENS-related issues.

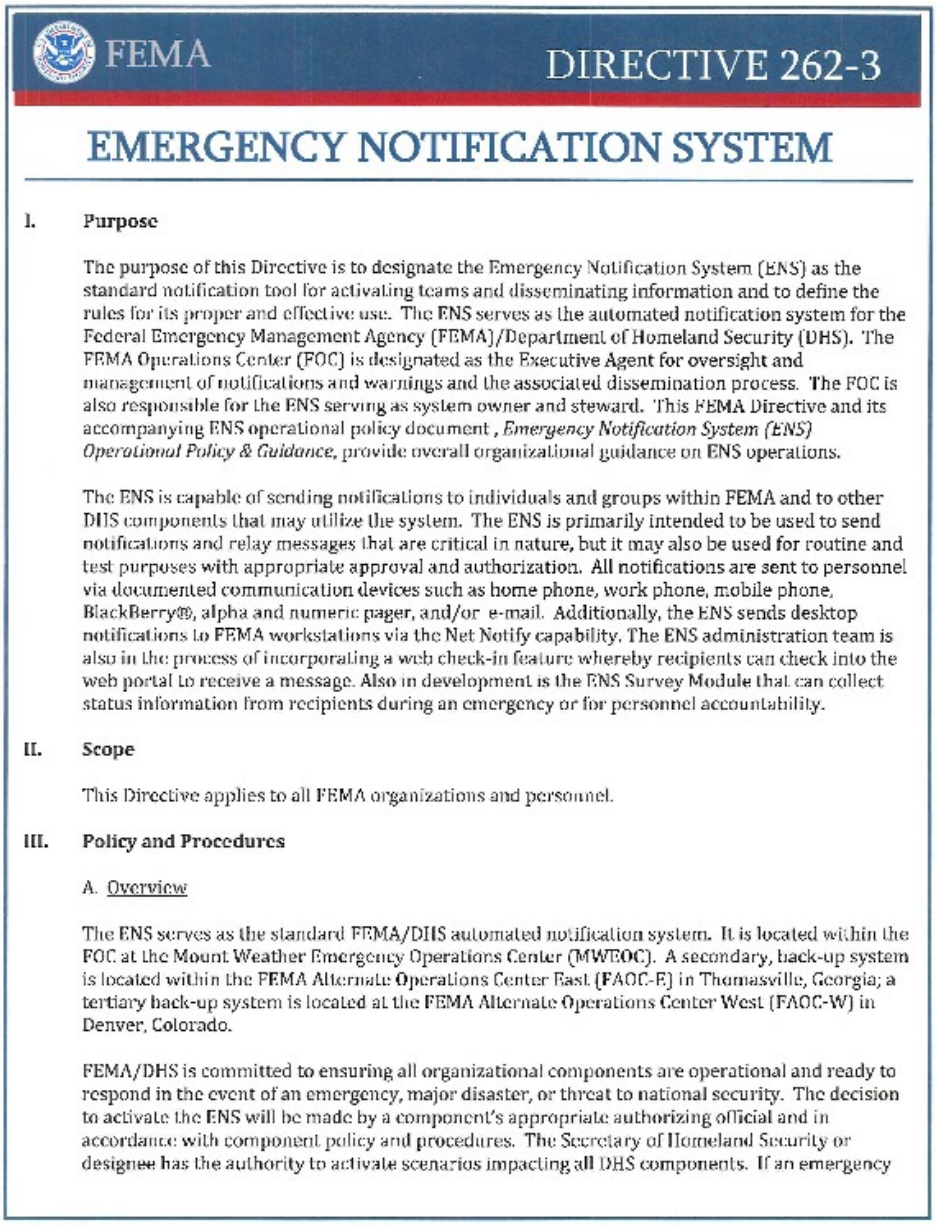
Regional Watch Centers (RWC): RWCs are staffed 24/7 and manage the data and activate scenarios in accordance with the *FEMA Watch Guide* and their regional policies and procedures. The RWCs can also provide the Tier 1 ENS support.

Scenario: A scenario is a saved set of defined parameters used to send messages to specific devices (email, telephone, or short message service [SMS]/text) that are used by individuals. These individuals are first assigned to designated groups, and then these groups are associated with scenario(s).

Specific threat: Specific threat refers to a threat condition being implemented for a specific region or sector.

APPENDIX C: FEMA ENS DIRECTIVE

Figure 5 shows an example of an ENS directive. The full text of FEMA Directive 262-3 is on the following link:
https://intranet.fema.net/org/orr/collab/response/omd/RCB/FOC/ENS/Quick%20Documents/FEMA%20Directive%20262-3%20-%20Emergency%20Notification%20System.pdf



FEMA DIRECTIVE 262-3

EMERGENCY NOTIFICATION SYSTEM

I. **Purpose**

The purpose of this Directive is to designate the Emergency Notification System (ENS) as the standard notification tool for activating teams and disseminating information and to define the rules for its proper and effective use. The ENS serves as the automated notification system for the Federal Emergency Management Agency (FEMA)/Department of Homeland Security (DHS). The FEMA Operations Center (FOC) is designated as the Executive Agent for oversight and management of notifications and warnings and the associated dissemination process. The FOC is also responsible for the ENS serving as system owner and steward. This FEMA Directive and its accompanying ENS operational policy document , *Emergency Notification System (ENS) Operational Policy & Guidance*, provide overall organizational guidance on ENS operations.

The ENS is capable of sending notifications to individuals and groups within FEMA and to other DHS components that may utilize the system. The ENS is primarily intended to be used to send notifications and relay messages that are critical in nature, but it may also be used for routine and test purposes with appropriate approval and authorization. All notifications are sent to personnel via documented communication devices such as home phone, work phone, mobile phone, BlackBerry®, alpha and numeric pager, and/or e-mail. Additionally, the ENS sends desktop notifications to FEMA workstations via the Net Notify capability. The ENS administration team is also in the process of incorporating a web check-in feature whereby recipients can check into the web portal to receive a message. Also in development is the ENS Survey Module that can collect status information from recipients during an emergency or for personnel accountability.

II. **Scope**

This Directive applies to all FEMA organizations and personnel.

III. **Policy and Procedures**

A. Overview

The ENS serves as the standard FEMA/DHS automated notification system. It is located within the FOC at the Mount Weather Emergency Operations Center (MWEOC). A secondary, back-up system is located within the FEMA Alternate Operations Center East (FAOC-E) in Thomasville, Georgia; a tertiary back-up system is located at the FEMA Alternate Operations Center West (FAOC-W) in Denver, Colorado.

FEMA/DHS is committed to ensuring all organizational components are operational and ready to respond in the event of an emergency, major disaster, or threat to national security. The decision to activate the ENS will be made by a component's appropriate authorizing official and in accordance with component policy and procedures. The Secretary of Homeland Security or designee has the authority to activate scenarios impacting all DHS components. If an emergency

Figure 5: Sample of ENS Directive

APPENDIX D: ENS POC AND CONTACT INFORMATION

The following is a link to the POC list:
https://intranet.fema.net/org/orr/collab/response/omd/RCB/FOC/ENS/Lists/ENS%20POC%20update/Approval%20grouped.aspx

APPENDIX E: REQUEST FOR ACTIVATION

Figure 6 is a screenshot of the request for activation form. The complete form is on the following link:
https://intranet.fema.net/org/orr/collab/response/omd/RCB/FOC/ENS/Quick%20Documents/ENS%20Request%20for%20Activation.pdf

ENS Request for Activation

Please complete and submit to the FEMA Operations Center using the buttons below.
Call the FOC after submitting your request to confirm receipt.
FEMA-Operations-Center@fema.dhs.gov (800) 634-7084

Requestor and Agency/Group:			Phone number:		
Date of Activation:		Time of Activation:		Duration:	
Number of attempts:		Type of Delivery:		Device Order:	
Name of Scenario:					
Additional Groups:			Individuals to Tag In/Out:		
Exact Voice Verbiage:					
Exact Email Verbiage:					
Exact Text Verbiage:					
Additional Information:			FOC Notes:		

Figure 6: Request for Action Form

APPENDIX F: ENS RULES OF BEHAVIOR

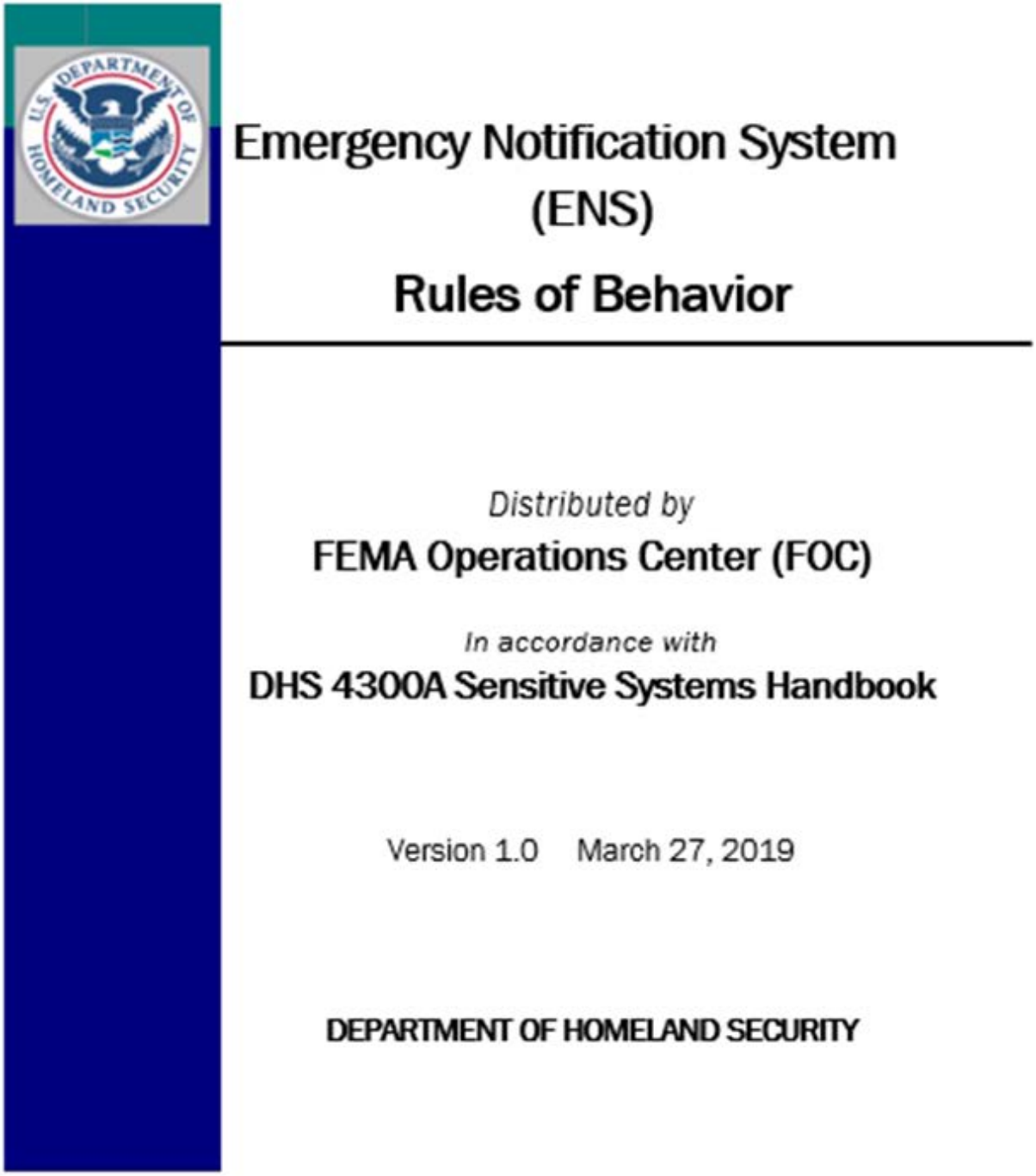


Figure 7: Cover Page of the FEMA Emergency Notification System Rules of Behavior

Document Change History

Version	Date	Description
1.0	January 10, 2011	Initial draft
1.0	January 12, 2011	Deleted general DHS ROB section/updated specific rules
1.0	January 21, 2011	Slight formatting mods.
1.0	February 8, 2011	Added section regarding former employee acct. deletions
1.0	June 14, 2011	Final
1.0	March 27, 2019	Updated

CONTENTS

Background

The DHS general rules of behavior apply to all DHS employees and to all DHS support contractors. These rules of behavior are consistent with IT security policy and procedures within DHS Management Directive 4300.1 (Information Technology Systems Security), DHS Sensitive Systems Policy Directive 4300A, and the DHS 4300A Sensitive Systems Handbook.

Any person who is in noncompliance with these rules of behavior is subject to penalties and sanctions, including verbal or written warning, removal of system access for a specific period of time, reassignment to other duties, criminal or civil prosecution, or termination, depending on the severity of the violation.

System-Specific (ENS) Rules Of Behavior

In addition to the general rules of behavior regarding DHS systems and IT resources, all individual components are responsible for developing such rules of behavior for their systems, and for having all users read and sign them. Emergency Notification System (ENS) users are also required to read and sign the following rules of behavior agreement, which has been specifically developed for the ENS by the FEMA Operations Center (FOC).

The FOC is responsible for distributing the ENS Rules of Behavior to all official component POCs and ensuring their signature. However, it is the responsibility of those POCs to distribute the document to all other component users of the system, and ensure strict adherence to the rules on their portion of the system. A hard copy of the signature page should be retained by the component POC or in the individual's personnel file for the duration of their system use.

The authority and requirements for system-specific rules of behavior for major applications, such as the ENS, are outlined in Appendix III of OMB Circular A-130 and NIST Special Publication 800-18, Rev. 1, *Guide for Developing Security Plans for Federal Information Systems.* The following ENS Rules of Behavior are based on these guidelines. Note that these rules also pertain to the Net Notify (desktop notification) capability, as well as the entire ENS system (web application, hardware, network, etc.).

System Access

- I understand that the DHS general Rules of Behavior regarding System Access also apply to ENS access.
- I understand that I have been given specific privileges within ENS as my duties require; I will not attempt to perform functions within the ENS that are not necessary to fulfill the functions of my position.

- If assigned component POC responsibilities, I understand that it is my responsibility to remove a user in my component/group from the ENS and revoke their system access once the user is no longer a DHS employee and/or does not require ENS access (i.e., resignation, dismissal, transfer, etc.).
- I understand that system interconnections are strictly forbidden on the ENS unless written approval is given by the FOC Director and the appropriate authorizing official.

Scenario Activation

- If assigned administrator rights, I will not attempt to change, manipulate, or activate scenarios unless I am appropriately authorized to do so and such actions are necessary to the functions of my position.
- If assigned administrator rights to edit and/or activate ENS scenarios, I will not create inappropriate, unnecessary, harmful (financially, safety, security, or otherwise), bothersome, vulgar, or offensive scenarios/messages, nor will I manipulate existing scenarios/messages in the aforementioned manner.

Passwords and Other Access Control Measures

- I understand that the DHS general Rules of Behavior regarding Passwords and Other Access Control Measures also apply to ENS access.
- If assigned administrator rights, I will not attempt to change the pre-defined password requirements for neither my component nor any other within the ENS.

Administrator/Privileged Accounts

- In order to protect the integrity of the data on my component's system, I understand that administrator, privileged, and shared/group accounts should be limited and should only be created with approval from the component POC.

Data Protection

- I understand that the DHS general Rules of Behavior regarding Data Protection also apply to the ENS.
- I will actively protect the integrity of not only my component's data, but also other component's data; I will not attempt to access the data of other components.
- I will not share personnel contact information, group membership information, personal pin numbers, or other personally identifiable information (PII) stored in the ENS with others.
- PII – Personally Identifiable Information
    - All use of PII data within ENS is strictly confined to emergency alerting, warning, notification, and official informational purposes only.
    - ENS PII data must NOT be shared either internally or externally to the agency.

- All ENS PII data must be protected to the greatest extent possible by the operating office.
- Misuse of PII data must be immediately reported to ens-admin@fema.dhs.gov.

Use of Government Office Equipment

- I understand that the DHS general Rules of Behavior regarding Use of Government Office Equipment also apply to the ENS.
- I understand that the printing of ENS sensitive but unclassified (SBU) material (group lists, activation reports, and other documents) should be handled with care, to ensure that any sensitive data is not revealed to unauthorized individuals. All printers, faxes, etc. used for these activities should government owned and used with discretion.

Software

- I understand that the DHS general Rules of Behavior regarding Software also apply to the ENS.
- I agree to comply with all Vesta Communicator (ENS application) software copyrights and licenses.

Internet and E-mail Use

- I understand that the DHS general Rules of Behavior regarding Internet and E-mail Use also apply to the ENS.
- I understand that I must possess and maintain an active DHS email account in order to gain and retain access to the ENS.

Telecommuting (Working at Home or at a Satellite Center)

- I understand that the DHS general Rules of Behavior regarding Telecommuting (Working at Home or at a Satellite Center) also apply to the ENS.
- I will physically protect any laptops I use to access the ENS.
- I understand that remote ENS access can only be performed on a DHS-issued laptop/computer and through DHS/FEMA network access.

Laptop Computers

- I understand that the DHS general Rules of Behavior regarding Laptop Computers also apply to the ENS.

Incident Reporting

- I understand that the DHS general Rules of Behavior regarding Incident Reporting also apply to the ENS.

- I will promptly report any suspicious activity within the ENS (account sharing, unauthorized access, inappropriate messages, etc.), and/or any IT security incidents, whether suspected or confirmed, to the ENS ISSO (ENS-Admin@fema.dhs.gov) and the 24/7 FOC staff (FEMA-Operations-Center@fema.dhs.gov).

Accountability

- I understand that I have no expectation of privacy while using any DHS equipment and while using DHS Internet or e-mail services.
- I understand that my access and activities will be regularly monitored by the FOC and the ENS ISSO.
- I understand that controls are in place to ensure separation of duties, and to limit the processing privileges of individuals.
- I understand that I will be held accountable for my actions while accessing the ENS.

ENS USER ACKNOWLEDGEMENT/SIGNATURE

Acknowledgment Statement

I acknowledge that I have read, understand, and I will comply with the Emergency Notification System (ENS) rules of behavior. I understand that failure to comply with these rules could result in verbal or written warning, demotion of ENS privilege level, removal of system access, reassignment to other duties (component discretion), criminal or civil prosecution, or termination.

Name of User (printed): _____

User's Phone Number: _____

User's E-mail Address: _____

DHS Component: _____

Location or Address: _____

ENS Supervisor/POC: _____

Supervisor's Phone Number: _____

User's Signature Date

** A hard copy of this page should be retained by the component POC or within each individual user's personnel file. **

APPENDIX G: POINT OF CONTACT DUTIES FOR ENS POC PROGRAM

General Responsibilities

- Designate a 2- to 3-day period quarterly to activate tests of the Point of Contacts' (POC) groups and teams.
    - There should be no activations for tests at another time.
    - POCs should inform their group/team members of the tests well in advance.
    - POCs review reports of the tests and correct data, training, or other issues.
- POCs should perform these tasks monthly:
    - POCs should perform frequent outreach to their teams/groups:
        - POCs should provide their contact information to the teams/groups and users.
        - POCs should remind users to log in and update their information.
        - POCs should remind users of their roles and responsibilities.
        - POCs should remind users of established security requirements.
        - POCs should remind users that they (POCs) are the primary source for all Emergency Notification System (ENS) issues and only the POC may request assistance from the Enterprise Service Desk (ESD) or the ENS-Administrative (ENS-Admin) team.
        - POCs should provide training or other relevant information.
    - POCs must comply with best practices and standards established by the FEMA Operations Center (FOC).
    - POCs must be mindful of and comply with security requirements.
    - POCs should be the first tier technical support for ENS issues.
    - Only POCs should contact ESD or the ENS-Admin team for assistance.
    - POCs should review the ENS SharePoint site frequently for training and other updated information.
    - POCs should notify the ENS-Admin team of issues, security concerns, or other activities that may impact ENS/FOC operations.
    - POCs should contact the ENS-Admin team for questions before performing actions they are uncomfortable with.
    - POCs should attend training before assuming duties as a POC and at a time thereafter, as required.
    - POCs should provide their contact information to the ENS-Admin team, as well as their supervisor's contact information.
    - POCs should notify the ENS-Admin team if they no longer perform duties as a

POC.
    - POCs should maintain accurate data for all information within their area of responsibility.
    - POCs should understand the "rules of the road" and agree to stay within their boundaries.
    - Personally Identifiable Information (PII)
        - All use of PII data within ENS is strictly confined to emergency alerting, warning, notification, and official informational purposes only.
        - ENS PII data must NOT be shared either internally or externally to the agency
        - All ENS PII data must be protected to the greatest extent possible by the operating office
        - Misuse of PII data must be immediately reported to ens-admin@fema.dhs.gov.

Submit ideas and suggestions or other feedback to ENS-Admin@fema.dhs.gov

ENS-Admin Team/FOC Responsibilities

The ENS-Admin team and/or the FOC will do the following:

- Maintain an accurate POC contact list.
    - Ensure an updated list is frequently posted to a SharePoint site.
    - Collect data via data calls, as needed.
- Provide an overview of the ENS program, role, and function within DHS.
- Remind POCs of ENS program resources and other sources of information (SharePoint, etc.).
- Develop a policy for addressing POCs who do not comply with these requirements. These may include the following:
    - Contact supervisor with a report of noncompliance.
    - Provide remedial training.
    - Recommend removal as POC.
- Provide training sessions via Webinar:
    - Train new POCs as they assume the role.
    - Provide training and corrective training as needed or requested and when staffing is available.
- Inform POCs of updates, changes, new features and functions, etc.
- Define procedures for requesting technical support (see below).
- Establish procedure (checklist) for incoming and outgoing POCs (see below).

ENS Incoming POC Checklist

[ ] Immediately contact the ENS-Admin team.

[ ] Provide contact information.

[ ] Provide supervisor contact information.

[ ] Describe the requirements and background for the groups/teams.

[ ] Identify backup POC (if applicable).

[ ] Receive training from the ENS-Admin team (note: not the previous POC), along with rights, etc.

[ ] Receive the POC packet, which includes the following:

- Training/reference materials;
- Best practices and standards;
- Schedules for testing, training, etc.;
- Technical support procedures;
- Rules of the road;
- ENS overview;
- Expectations, roles, and responsibilities;
- Job aids;
- Templates;
- Procedure for submitting ideas or suggestions;
- Sources of information (SharePoint, etc.);
- Recommendations for maintaining and updating users, groups/teams (frequent outreach to users);
- POC list; and
- Rules of behavior (signed).

ENS Outgoing POC Checklist

[ ] Notify the ENS-Admin team immediately you will no longer serve as POC. [ ] Identify your replacement.

[ ] Return unneeded materials or provide to your replacement. [ ] Provide relevant information to your replacement.

[ ] Inform the ENS-Admin team if you are leaving FEMA.

ENS POC Technical Support Procedures

- Receive notification of a problem from the user within your area of responsibility.
    - If you are not the POC, find the correct POC from your resources (POC list, SharePoint, etc.) and instruct him/her to contact the correct POC.
- If you can correct the problem, then no further action is required.
    - Likely problems may be a password reset, incorrect or incomplete data, incorrect group membership, lack of training, etc.
- If the problem appears to be system related, send an email to ENS-Admin@fema.dhs.gov. If you receive no response within a reasonable amount of time or after-hours, contact the ESD.
    - Note the circumstances of the issue and the user who is experiencing the problem.
    - Do not instruct the user to contact ENS-Admin or ESD. Only designated ENS POCs are authorized to elevate the issue.
- The ENS-Admin team will elevate or correct the problem.
- You will be notified by the ENS-Admin team when the issue has been corrected.