



System Assessment and Validation for Emergency Responders (SAVER)

Alert/Notification Systems Technology Guide

April 2012



**Homeland
Security**

Science and Technology

U.S. Department of Homeland Security



System Assessment and Validation for Emergency Responders

Prepared by Space and Naval Warfare Systems Center Atlantic

The *Alert/Notification Systems Technology Guide* was funded under Interagency Agreement No. HSHQDC-07-X-00467 from the U.S. Department of Homeland Security, Science and Technology Directorate.

The views and opinions of authors expressed herein do not necessarily reflect those of the U.S. Government.

Reference herein to any specific commercial products, processes, or services by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government.

The information and statements contained herein shall not be used for the purposes of advertising, nor to imply the endorsement or recommendation of the U.S. Government.

With respect to documentation contained herein, neither the U.S. Government nor any of its employees make any warranty, express or implied, including but not limited to the warranties of merchantability and fitness for a particular purpose. Further, neither the U.S. Government nor any of its employees assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed; nor do they represent that its use would not infringe privately owned rights.

FOREWORD

The U.S. Department of Homeland Security (DHS) established the System Assessment and Validation for Emergency Responders (SAVER) Program to assist emergency responders making procurement decisions. Located within the Science and Technology Directorate (S&T) of DHS, the SAVER Program conducts objective assessments and validations on commercial equipment and systems and provides those results along with other relevant equipment information to the emergency response community in an operationally useful form. SAVER provides information on equipment that falls within the categories listed in the DHS Authorized Equipment List (AEL). The SAVER Program mission includes:

- Conducting impartial, practitioner-relevant, operationally oriented assessments and validations of emergency responder equipment; and
- Providing information that enables decision-makers and responders to better select, procure, use, and maintain emergency responder equipment.

Information provided by the SAVER Program will be shared nationally with the responder community, providing a life- and cost-saving asset to DHS, as well as to Federal, state, and local responders.

The SAVER Program is supported by a network of Technical Agents who perform assessment and validation activities. Further, SAVER focuses primarily on two main questions for the emergency responder community: “What equipment is available?” and “How does it perform?”

As a SAVER Technical Agent, the Space and Naval Warfare Systems Center (SPAWARSYSCEN) Atlantic has been tasked to provide expertise and analysis on key subject areas, including communications, sensors, security, weapon detection, and surveillance, among others. In support of this tasking, SPAWARSYSCEN Atlantic developed a technical guide to provide emergency responders with reference information on currently available alert/notification system technologies. Alert/Notification systems fall under AEL reference number 13IT-00-ALRT titled System, Alert/Notification.

For more information on the SAVER Program or to view additional reports on alert/notification systems or other technologies, visit the SAVER section of the DHS S&T Website at www.dhs.gov/science-and-technology/SAVER.

POINTS OF CONTACT

SAVER Program

National Urban Security Technology Laboratory

U.S. Department of Homeland Security

Science and Technology Directorate

201 Varick Street

New York, NY 10014

E-mail: NUSTL@hq.dhs.gov

Website: www.dhs.gov/science-and-technology/SAVER

Space and Naval Warfare Systems Center Atlantic

Advanced Technology Branch

P.O. Box 190022

North Charleston, SC 29419-9022

E-mail: ssc_lant_saver_program.fcm@navy.mil

TABLE OF CONTENTS

Foreword.....	i
Points of Contact.....	ii
1. Introduction.....	1
2. Technology Overview.....	1
3. Selection Considerations.....	2
3.1 Type of System	3
3.2 Software Licensing	3
3.3 Costs.....	4
3.4 Database.....	4
3.5 Delivery Capacity	5
3.6 Integration and Interoperability	5
3.7 System Access and Security	6
3.8 Message Delivery Acknowledgement and Tracking	6
3.9 Vendor-Provided Training and Support.....	6
3.10 Establishing Policy.....	7
3.11 Acceptance and Operational Testing	7
4. Conclusion	7

LIST OF FIGURES

Figure 2-1 Commonly Used Alert/Notification Devices.....	2
--	---

1. INTRODUCTION

The System Assessment and Validation for Emergency Responders (SAVER) Program developed this technology guide on alert/notification systems to provide emergency responders with information that will assist with making operational and product selection decisions. Product selection considerations are based on recommendations from a focus group of emergency responders with experience using alert/notification systems, as well as information collected during market research.

Alert/Notification systems allow for real-time dissemination of information and intelligence via equipment such as mobile phones, pagers, computers, etc. This technology guide focuses only on systems designed to allow emergency response agencies to send alerts and notifications to emergency responders, and not systems designed to interface with the general public.

2. TECHNOLOGY OVERVIEW

With the proliferation of personal electronic mobile information devices, including mobile phones, pagers, tablets, smart phones, etc., alert/notification systems have new ways of delivering both critical and routine information to emergency responders. Alert/Notification systems designed to work with mobile devices use computer systems and existing telecommunication and information networks to deliver both audio messages and text-based messages. Audio messages usually involve a recorded message sent directly to a mobile phone or to a home or business telephone line. Text-based messages can be delivered by short message service (SMS), fax, or e-mail. Text-based messages may also include graphic information, like images or maps, depending on the capabilities of the alert/notification system.

Some of the notifications agencies send using an alert/notification system are:

- Storm warnings and updates;
- Evacuation orders;
- Missing person and abduction reports;
- Hospital readiness;
- Prisoner escapes;
- School/Campus emergencies;
- Fires, chemical spills, and gas leaks;
- Terrorist threats;
- Dam or levee breaks;
- Event reminders; and
- Meeting notices.

Alert/Notification systems are comprised of computer software and hardware. The software is used by system administrators to generate message content and create a database that contains recipient information (e.g., contact numbers, e-mail, etc.). The hardware runs the software for the system and interfaces with telecommunication networks, such as the Internet, telephone

system, and cellular networks, to deliver the messages. Once configured by the system administrator(s), the alert/notification system permits users to send messages to recipients using multiple methods of communication.

To generate a message, the alert/notification system user:

- Logs onto the system and validates their authority to activate a message;
- Generates the message or selects a pre-generated message;
- Selects the individuals or group(s) to receive the message and the delivery method for the message (e-mail, text message, voice message, etc.); and
- Reviews the message, recipients, and other settings, and then releases the message.

Most systems monitor active messages and require acknowledgement of the message by recipients.

As illustrated in Figure 2-1, messages can be sent to pagers, mobile phones, smart phones, tablets, PCs, telephones, and fax machines, depending on the capabilities of the individual systems. Most systems will generate voice messages, SMS (text) messages, and e-mails.

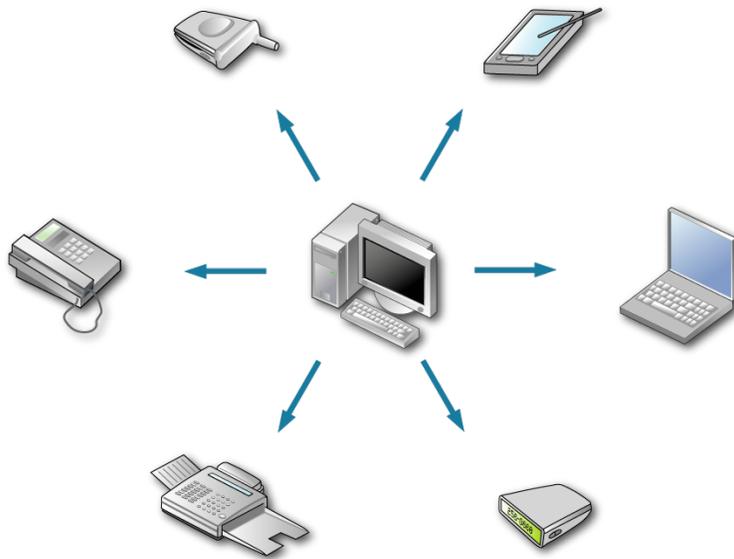


Figure 2-1 Commonly Used Alert/Notification Devices

3. SELECTION CONSIDERATIONS

There are a number of commercially available alert/notification systems on the market, each with different features and capabilities. For example, some alert/notification systems are designed for specific types of organizations (e.g., school, hospital, law enforcement) while others may offer capabilities in modules that can be purchased separately. When procuring alert/notification systems, consideration should be given to the type of system; software licensing; associated costs; size of the database; delivery capacity of the system; integration and interoperability capabilities of the system; system access and security; message acknowledgement and tracking;

vendor-provided training and support; policy development; and acceptance and operational testing.

3.1 Type of System

The purchasing organization should first determine whether a subscription-based or agency-owned system is the most effective solution to meet their needs.

3.1.1 Subscription-Based Alert/Notification Systems

In a subscription-based alert/notification system, the vendor hosts and maintains the system hardware and software at an off-site location, and the agency pays a recurring fee for its use. The service provider performs system upgrades and maintains the hardware, software, communications network, and telephone lines. The system may be located in a region separate from the subscriber, ensuring the system continues to operate in the event of a regional disaster in the area in which the agency is located.

Some subscription-based vendors charge clients a monthly or annual fee based on the number of recipients in the member database and/or the selected level of usage, enabling a specified number of calls/messages to be sent during a given time period before additional charges apply. This may be a cost-effective solution depending on the types of hosting plans available and the agency's usage levels. Other service providers charge a fee each time the system is used to send a message; this may be a more economical solution if the system is going to be used strictly in the event of an emergency.

3.1.2 Agency-Owned Alert/Notification Systems

Agency-owned alert/notification systems are operated and maintained by the purchasing agency, giving the owning agency control over physical access to the system. Depending on the demands of the system, agencies may be able to utilize their existing computer infrastructure (e.g., workstations, laptops, servers, backup hardware) or may need to purchase additional hardware to meet system needs. In addition to the required hardware, trained employees are needed to use and maintain the hardware, software, and communications network. Depending on an agency's existing information technology infrastructure and staffing, it may need little additional equipment and/or staffing to support an alert/notification system.

Upgrades to the agency's communications network and telephone services may be needed to handle the increased volume of traffic generated by an alert/notification system. Further, if the alert/notification system is located within the organization, a local or regional disaster could disrupt the operation and effectiveness of the system—therefore, a backup system at a remote location should be considered.

3.2 Software Licensing

Whether a subscription-based or agency-owned system is selected, almost all alert/notification system vendors license their software. Licenses may be unlimited, meaning the agency can have as many copies of the software running as it needs, or limited. Limited licenses are generally available in two types: limited installations and limited users. With limited installation licenses, the agency must purchase licenses for each computer on which the software will be installed. Limited user licenses must be purchased for each individual permitted to send messages and/or

access the software for configuration purposes. Agencies should consider their usage needs along with licensing restrictions and ensure they purchase enough licenses to accommodate planned use.

3.3 Costs

Costs associated with an alert/notification system include both initial costs and operating costs. The initial procurement and implementation costs may be affected by the number of recipients stored in the database, the number of software licenses required, the costs associated with system redundancy, and any hardware and software updates required for operation of the system. Initial costs may also include purchasing and upgrading the receiving hardware used by recipients and acquisition of dedicated communication lines required for system operation. Purchasing extended warranties can affect the initial cost of the system but may lower operating costs over time.

Operating costs may include the costs to pay personnel responsible for daily operation of the system, vendor “per-call” and/or database storage fees, Web-based access of the system, and the cost of bandwidth and maintaining any dedicated communication lines required for system operation. Licensing fees (limited or unlimited) may also contribute to operating costs if the number of personnel authorized to operate the system increases. When considering an alert/notification system purchase, agencies may want to contact nearby organizations to determine the feasibility of sharing systems/costs. Other costs may include those associated with receiving hardware, technical support, and maintenance.

3.3.1 Receiving Hardware

Many agencies issue personnel pagers or mobile phones for agency use. When acquiring an alert/notification system, an agency should review existing equipment and determine if it needs to be upgraded to take full advantage of the alert/notification system. Additional mobile phones and pagers may need to be purchased so all intended recipients will be able to receive messages.

3.3.2 Technical Support and Maintenance

The service level and availability of technical support vary by system type and vendor. The cost of support includes both initial fees paid for technical support as well as ongoing monthly or annual costs to continue support. Vendors offer different levels of service; some may conduct routine onsite maintenance while others may expect the agency to perform such duties. Vendors may offer a maintenance contract for agency-operated systems and regular system updates may be offered for both types of systems.

3.4 Database

Prior to deployment of an alert/notification system, the contact database must be populated with the message recipients’ contact information. Contact information may include the recipient’s name; home, work, and mobile phone numbers; rank and discipline; and e-mail addresses. Contact information can be imported from another database, such as a human resources system, or manually entered into the database by a system administrator or by the recipient via a registration Web page.

Once the database has been populated, the recipients can be grouped into distribution groups for ease of sorting recipients. Recipients can be grouped by credential and location so that, for example, only firefighters residing within a certain area are notified to respond to a fire emergency. Firefighters residing outside the area would not receive the alert.

In addition to contact information for recipients, the database stores pre-generated text-based and/or voice messages. Pre-generated messages enable alerts to be issued more quickly. It is important to note that some systems may have restrictions on the number of text characters in text and e-mail alerts or the duration for voice message alerts. For text and e-mail alerts, some systems insert a vendor tagline at the end of the message that may count toward the maximum characters permitted in a message, further limiting the number of characters available for the notification. Also, computer-generated audio messages may be difficult for some recipients to understand.

Consideration should be given to the system's storage capacity for the member database and pre-generated messages. Some databases are expandable to accommodate an increase in members, stored messages, and receipt data. It is important to note that keeping the database up-to-date can be time consuming, and agencies should plan for database maintenance.

3.5 Delivery Capacity

In an emergency situation, many personnel may need to be notified very quickly, and insufficient capacity to deliver alerts can result in delays in responding to the situation. For this reason, a sufficient number of dedicated communication lines/circuits are essential for successful message delivery. For agency-owned systems, consideration should be given to the maximum message capacity and whether it will meet the agency's needs based on the number and type of messages (e.g., e-mail, text, etc.) that may need to be sent out simultaneously, as well as the amount of time required to send messages. Messages may be delayed as a result of limited bandwidth. For instance, text messages generated by the system may be delayed if the cellular network is overloaded. Subscription-based systems often share capacity with multiple agencies, operating under the assumption that the agencies will not require maximum capacity at the same time. Since this is a potential risk, some subscription-based systems offer a dedicated capacity (e.g., phones lines, server) specific to each client. While this is usually more costly, dedicated capacity ensures that each client's messages are delivered in a timely manner.

3.6 Integration and Interoperability

Alert/Notification systems that use a standardized message format are more likely to be able to communicate with a variety of other systems at the same agency (integration), as well as alert/notification systems used by other agencies (interoperability). Integration can aid in ensuring information continuity across systems and eliminating redundant data. Consideration should be given to the types of systems with which the alert/notification system will integrate, including systems employed by fusion centers, social media applications, computer aided dispatch (CAD) systems, Integrated Public Alert and Warning System (IPAWS), Geographic Information System (GIS) for mapping (plume dispersion models), and other incident management systems. One benefit of an alert/notification system integrating with other systems is that they improve situational awareness since these systems can then combine important information regarding events (e.g., location, weather, personnel responding, etc.).

3.7 System Access and Security

Administrators can access and operate alert/notification systems by multiple methods, most often via a secure Web-based interface, but also by phone, dedicated computer interface, or mobile device application. A Web-based interface offers the advantage of being available wherever an Internet connection exists.

Controlling who has access to the alert/notification system is very important. False or malicious alerts can cause large disruptions to agency operations and reduce trust in the alerting system. For this reason, access to the system and the database is usually secured via user group permissions and password restrictions. User group permissions determine which users have authority to send messages and define the number and type of messages that can be sent. Password protection prevents unauthorized access to the system.

It may also be important to determine if there are any security-related requirements associated with using U.S. Department of Homeland Security grants for purchasing a system (e.g., the National Information Exchange Model (NIEM) standards).

3.8 Message Delivery Acknowledgement and Tracking

Some alert/notification systems allow the system administrator to require confirmation of message receipt in order to track successful message delivery. Recipients may acknowledge messages by pressing a button (one-touch response on the phone keypad) or by responding to a text or e-mail message. Most systems automatically recognize and store message receipt confirmations; however, if the message recipient acknowledges receipt of the message by an alternate means, a feature that allows an agency to enter a message acknowledgement manually can be important.

Alert/Notification systems typically provide real-time monitoring that will keep system administrators informed of the current alert status throughout an incident by providing information regarding the number of people contacted and the number that have confirmed receipt of a message. In addition, some systems may restrict, or permit the administrator to restrict, the amount of time that recipients have to respond to a message. The system may also provide the number of attempts required to reach each recipient, as well as a report of successful and failed deliveries. Some systems can be configured by the administrator or dispatcher to cease alerting and notifying once it receives a specified number of acknowledgements. If a message cannot be delivered, some alert/notification systems report the reason a message was undeliverable (e.g., contact unreachable, number disconnected, out of office, etc.). Some systems will attempt to resend the message in case of delivery failure due to network issues.

3.9 Vendor-Provided Training and Support

Vendor-provided training on usage of the system, as well as procedures for testing and monitoring the system for failures, may be available. Training location, type (e.g., train the trainer, Webinars, etc.), and availability vary by vendor. Consideration should also be given to any ongoing training options provided by the vendor since the system will likely remain operable for years after implementation. Agencies may want to conduct research prior to procurement to see if updates can be scheduled during off-peak times when emergency situations may be less likely to occur. If the system is shut down for updates, alerts will not be able to be sent out in the

event of an emergency. It is important to note that subscription-based systems may experience downtimes for vendor-provided, scheduled system updates.

3.10 Establishing Policy

Prior to installation, organizations should consider creating and implementing policies governing how the alert/notification system will be administered, maintained, and operated. Internal policies will need to be developed that designate individuals responsible for daily operation of the system. Additional policies may need to be implemented that designate how recipients can keep their contact information up-to-date in the system. Furthermore, a policy may need to be developed that establishes a schedule for routine testing (operational testing) of the system.

3.11 Acceptance and Operational Testing

Acceptance testing is the last point at which the agency can ensure an alert/notification system meets its needs and requirements prior to activation. It is highly recommended that a purchasing agency develop a comprehensive testing plan for acceptance that, at a minimum, tests the system's ability to generate multiple alerts and deliver them successfully to agency personnel. Agencies should require a successful acceptance test prior to taking ownership of the system or final agreement to a system subscription. To verify that the system continues to function properly, administrators may want to consider performing routine operational testing by sending out a trial message to new and existing recipients to ensure they can acknowledge receipt.

4. CONCLUSION

Alert/Notification systems can be used to effectively transmit alerts and warnings to emergency responders. Through quick delivery of an emergency message, emergency responders are able to respond when necessary. This technology guide focuses only on systems designed to provide alerts and notifications to emergency responders and was developed to assist emergency responder agencies with making operational and procurement decisions. Some alert/notification systems can communicate with public/mass notification systems in the event the public must be notified of emergency situations, but operational needs specific to these types of systems are not covered in this technology guide.

Some of the considerations discussed in this technology guide include:

- **System type:** The system may be subscription-based or agency-owned. Cost, database size requirements, internal policies, and deployment factors may affect an organization's decision to choose between these hosting options;
- **Delivery capacity of the system:** The number and type of messages that can be sent out simultaneously, and the amount of time required to do so, may affect emergency response operations. It is also important to ensure the system will be able to contact message recipients through a variety of methods, such as e-mail, cell phone, fax, pager, etc.;
- **Initial and operating costs of the system:** Software licensing, receiving hardware, vendor-provided training, technical support, as well as maintenance and warranties may all affect these costs;

- System integration and interoperability: Many alert/notification systems integrate with other technologies, such as systems employed by fusion centers, social media applications, CAD systems, IPAWS, GIS for mapping (plume dispersion models), and other incident management systems. Alert/Notification systems that use a standardized message format are more likely to be able to communicate with a variety of other systems at the same agency, as well as alert/notification systems used by other agencies;
- System access and security: Access to the system and the database is usually secured via user groups and password restrictions. By assigning appropriate user group permissions and requiring passwords for system login, agencies can limit access to the system. This not only protects agency personnel but also prevents false or malicious alerts from degrading an agency's ability to meet its mission;
- Message acknowledgement and receipt: Real time monitoring permits administrators to be constantly informed of the current alert status, the number of people that have been contacted, and the number that have confirmed receipt of the message; and
- Acceptance and operational testing: It is important for an agency to conduct stress testing of the system by sending multiple messages to multiple groups and ensuring all system features function correctly during acceptance testing. Periodic operational testing thereafter is also important.

The primary function or purpose of an alert/notification system is to quickly alert responders of potential threats or emergency situations and to provide direction on how to respond to any alerts. Emergency responder agencies that may be considering the purchase of an alert/notification system should carefully consider the overall system capabilities and limitations in relation to their jurisdiction's operational needs. By integrating with existing communication protocols and following internal policies, agencies can maximize the usage of their alert/notification system.