

Lesson 2: Communicating within a Partnership

Lesson Overview

This lesson covers best practices and actionable techniques to help members of a public–private partnership communicate and share information during all stages of emergency management.

Learning Objectives

By the end of this lesson, you will be able to:

- Explain methods to share information between partners
- Identify best practices to communicate with partners during an emergency

Effective Communication

In order for public–private partnerships to effectively prepare for, respond to, and mitigate for disasters, they need to be able to communicate effectively. Partners share information to support planning, decision making and operations in the whole community approach. The whole community approach leads to greater understanding of community needs and capabilities through information and resource sharing across organizations and sectors.

Effective communication between partners includes both coordinated communication during an emergency and information sharing between partners before and after an emergency. Determining methods for emergency communications and information sharing in a public–private partnership prior to an incident allows a partnership to better respond during an incident.

Throughout this lesson, you will learn best practices to share information between partners. You will also learn how to communicate with partners during an emergency.

Read the story below to learn more about the importance of effective communication in public-private partnerships.

Ian Hay

President, SouthEast Emergency Response Network (SEERN)

The real mission for us is to be on the left-side of a disaster. We want to build relationships. We want to build a Common Operating Picture. We want to develop that real-time information sharing environment, so the locale, or the State or the region can look at an incident that's happening and bring their best resources in real time; at the same time, notifying Federal authorities of the scale of what's happening.

So really our mission is to try and focus on the preparedness side by being engaged in exercises, by going to lots of conferences, by networking and marketing. We really try to serve as a translator that speaks a little bit of emergency management, that speaks a little law enforcement, speaks private sector, and can also reduce the critical elements up to the Federal level.

Information Sharing

When partners share information, they can better prepare for potential incidents and improve response and recovery capacity. The practice of information sharing and methods should be established and

agreed upon by the partners involved. Information can be shared through traditional tools, such as list serves and meetings, and through new media, such as social networking tools, which allow for quick updates and coordination with partners and citizens.

How information is shared depends upon:

- How quickly the information is provided or updated
- What level of security is desired by the partners in safeguarding the information

In the following screens, you will learn about what information is typically shared and how partners may choose to share it.

Types of Information That Can Be Shared

Partners can share many types of information. Not all of these types of information necessarily need to be shared in every partnership. However, information sharing between partners can greatly benefit emergency management efforts in the whole community and make the partnership more successful.

Explore the four types of information partners might share:

Response plans

Public-sector agencies and private-sector companies with critical infrastructure, large numbers of employees, or multiple locations may have their own emergency response plans in place. By sharing these individual response plans, the partnership can ensure they do not needlessly duplicate efforts or neglect essential response activities. It can also allow agencies to learn from one another and guide partners without response plans develop their own.

Contact information

Sharing the contact information of key members is important in all public–private partnerships. Knowing who needs to be contacted and how to contact them in an emergency makes it easier and faster to disperse information. Outside of an emergency, it also allows all partners to coordinate training sessions, meetings, and other activities.

Sensitive or proprietary information

Sensitive or proprietary information is information to which access needs to be controlled or restricted for privacy or security reasons. Response plans, threat information and contact information may be sensitive or proprietary themselves. Examples of private-sector sensitive or proprietary information that may be relevant in an emergency include facility layouts, storage facilities, security plans, and locations of back-up sites. Public agencies may also have sensitive information, such as critical information on risks and public works.

On the next screen, you will learn about the importance of safeguarding sensitive or proprietary information.

Threat information

Threat information details existing or potential threats to public safety and security. Threat information is typically sensitive information. Sharing threat information between partners can help partners become better prepared.

Guarding Sensitive and Proprietary Information

Remember that public and private organizations may be hesitant or uncomfortable sharing sensitive and proprietary information in a partnership. Remember to consider threat information, response plans, and contact information of partners as sensitive.

Partners worry about sharing this type of information for two reasons. First, both public and private partners worry about the improper dissemination of sensitive information. Improper dissemination of information includes giving private-sector proprietary information to competitors or sharing sensitive response plans publicly so that public safety and security is compromised.

These worries are legitimate concerns for all partners. Therefore, it is essential that partnerships take actions to safeguard all shared information and control access to it. Partnerships should also provide detailed explanations to all partners on how sensitive or proprietary information will be used or disseminated.

Sharing Information Securely

There are many methods to share information in a secure way that are appropriate to the kind of information being shared.

In IS-660: Introduction to Public–Private Partnerships, you learned about informal and formal tools for information sharing. As you should recall, informal tools for information sharing include:

- Webinars
- Email distribution lists
- Conference calls

Formal tools include

- Information networks
- Fusion centers

Each of these tools is more suited to sharing certain kinds of information. You should decide which of these methods is right for you based on how secure you need it to be.

Explore the differences between insecure and secure networks below:

Insecure networks

Insecure networks generally include more informal information sharing methods, such as listservs or conference calls that do not have firm ways to control access to information. These methods can be good ways to share information and collaborate in a partnership. However, they may not be secure enough to use to disseminate highly sensitive information, such as response plans or facility layouts.

Secure networks

Secure networks are designed to protect and control access to sensitive or proprietary information. A partnership can either set up its own network, or utilize existing secure networks such as the DHS

Homeland Security Information Network (HSIN) or InfraGard. The following actions help to ensure that the network is secure:

- Limit access to the network using membership criteria. For example, a partnership may limit access to users with email addresses from one of the participating organizations.
- Require users to register before accessing sensitive materials. Registration requests could be approved by a network administrator on a case-by-case basis.
- Establish policies to ensure all data uploaded on to the network is encrypted.
- Disable the copy, edit, and print functions within files that contain sensitive information to prevent improper dissemination.

Information Sharing in Practice

Information sharing in a public–private partnership varies widely in practice. In addition to the more formal types of information sharing mentioned earlier, partners share information more informally. Partners may share lessons learned about preparation, response, and mitigation from recent incidents. Individual agencies or businesses may share their concerns or opinions on topics related to emergency management. All of these types of information sharing help to foster the collaboration that makes public–private partnerships successful.

Read the stories below to learn more about information sharing in a public–private partnership.

Ira Tannenbaum

Director of Public-Private Initiatives for New York Office of Emergency Management

We've put a program in place in NYC called CORPNet, where our 24-hour-a-day, 7-day-a-week command is busy monitoring the city for the public sector, we'll share roughly 95% of our information via email to registered private sector partners. It could be weather, which is our number one hazard in the city; it could be water main breaks; things that will disturb or disrupt your business; or even general police activity. So we'll share our information as much as possible, but we'll also bring them in to educate them about emergency management. I often say that, when I go out and I speak to businesses, that OEM is the "Office of Expectation Management." A lot of what I do is try to help people understand what to expect during an emergency.

Emergency Communications

Emergency communications are another vital aspect of communication within a public-private partnership. Emergency communications are different from the types of information sharing mentioned earlier in this lesson because emergency communications occur during an incident as opposed to before. Emergency communications can include situation updates, assistance requests, and instructions to control or manage response efforts.

Partnerships can relay emergency communications using one of the following methods:

- Direct communication
- Incident alerts
- Situational reporting
- Private-sector representation at an EOC

You will learn about each of these methods in the next section of this lesson.

Direct Communication

Direct communication is the most straightforward means to contact your partners: look up the appropriate point of contact (POC) and get in touch with them via their preferred method. However, it may not be the most efficient method to communicate with all members of a partnership during an emergency. Direct communication can be slow when there are many partners, particularly when time-sensitive or complex information needs to be transmitted.

When using direct communication to contact partners, a partnership should have contact information for all key individuals in all partner organizations. This information should include primary and secondary methods to ensure that the right people are reached in time.

This information also needs to be maintained over time. Partnerships can establish processes through which this contact information is updated on a regular basis.

Incident Alerts

During an incident, requests for information from partners can overwhelm a public-private partnership. Multiple partners may need access to the same information as quickly as possible, making direct communication difficult. To handle these needs, some partnerships send out incident alerts, public notifications, or informative bulletins to their members during emergencies. These alerts can trigger response plans or evacuation procedures and generally inform all relevant parties as quickly as possible.

Explore the steps to set up incident alerts in a partnership below.

Determine the source

First, a partnership needs to determine which organization will be the source of the incident alerts. A partnership usually selects one partner, typically a public safety agency, to write and disseminate incident alerts. Ensuring that incident alerts originally emanate from one source helps guarantee the validity and importance of the information in the alert.

Identify recipients

Public-private partnerships should determine which groups should receive the incident alert directly from the source. Some partnerships instruct the source to send incident alerts to business associations or similar groups which can then relay relevant messages to their members in turn. This system gets important information into the right hands quickly. Other partners may designate which parties should receive incident alerts based on the type of incident or the geographic areas affected.

Decide what to include in an incident alert

Incident alerts should include detailed, actionable information that can inform the response of your partnership's members. As such, incident alerts should include:

- Type of incident (fire, terrorist attack)
- Location of the incident
- Expected impact on the surrounding area

- Resources already dispatched

Example of a Public Alert and Notification System

FEMA's Integrated Public Alert and Warning System (IPAWS) is a good example of a public alert and notification system. IPAWS also enables government organizations to enhance situational awareness and collaboration by exchanging messages via multiple communication pathways including: [Emergency Alert System \(EAS\)](#), [Commercial Mobile Alert System, \(CMAS\)](#), and [National Weather Service Dissemination Systems](#), including NOAA Weather Radio.

Public officials including Federal agencies; State, local, tribal, and territorial governments; and public safety organizations are generally granted the authority to alert the public of emergency situations through Federal, State, and local laws. Other public or private sector organizations may be eligible depending on their public safety mission. For more information on the Integrated Public Alert and Warning System (IPAWS) program, visit: <http://www.fema.gov/emergency/ipaws/index.shtm>.

Situational Reporting

Situational reporting is the term used to describe communications that keep your partners informed of changing circumstances during an emergency. It should take place through an established forum, such as your partnership's information sharing network or a secure Web site. Information provided in a situational report could include:

- Observed developments in the incident, such as changes in location or severity
- Resources requested or deployed
- Response actions taken, such as the evacuation of a facility
- Extent of damage incurred

FEMA has developed SAVER2, or the Situational Awareness View for Emergency Response and Recovery, as a way to achieve shared situational awareness. This Web-based information sharing system displays available data from multiple emergency management partners to enable an integrated approach during daily operations and disasters.

Private Sector Representation at an EOC

Private sector representation at an incident's Emergency Operations Center (EOC) facilitates emergency communications between the public and private sectors. These representatives frequently relay information between the EOC and private sector partners and advocate for private sector and constituent interests. There is an official Private Sector Representative in the National Response Coordination Center (NRCC), but State and local EOCs should include private sector representatives when appropriate.

Partnerships should determine the role and responsibilities of the representative by asking themselves the following questions:

- What information can the EOC representative disclose to private sector organizations or the media?
- What types of incidents activate the private sector representative to come to the EOC?

- Where will the EOC representative be physically located?
- How will the partnership ensure continuous representation?
- How will the representative be trained?

The Role of Private Sector Representatives

The inclusion of a private sector representative at an incident's EOC literally gives the private sector a seat at the table. The private-sector representative ensures all private sector operational partners are informed of the latest developments and their interests are taken into account when the EOC makes critical decisions.

Read the story below of a former private sector representative talk about his experience.

LaNile Dalcour

Life Safety/Security Director, Brookfield Industries

As the private sector rep in the NRCC for FEMA I've had a lot of roles and responsibilities. My primary role when I started was to cover the NRCC during the Alabama tornados. Right after that, I had the Mississippi flood. So I spent my first 3, almost 4 weeks with FEMA in this position actually working inside the NRCC. But then my role also expands outside of just being the person working in the NRCC. In addition to that, I have many opportunities to kind of be a liaison for the private sector to have discussions with folks from the public sector as to what the needs and expectations are for our world. And, in most cases folks in the private sector, we have an emergency plan, we have an emergency procedure, but where we seem to lack help is recovery planning and business continuity and things like that. So I love this opportunity to be able to talk directly to the government about what the industry needs are and not just the commercial real estate industry, which I'm involved in, but the private sector industry as a whole.

National Emergency Communications and Information Sharing

DHS and FEMA already have some networks and services in place to facilitate emergency communications and information sharing between the public and private sectors. Earlier, you learned about HISN. The following are also methods to share information:

- FEMA created the position of the Private Sector Representative in the National Response Coordination Center (NRCC), which allows the private sector to have a seat at the table and support emergency management coordination
- Email subscription services such as [GovDelivery](#) allow individuals to sign up through a list serve to automatically receive notifications when new information is available on their area of interest, which allows users to share information and stay updated without having to continually visit different Web sites
- The Private Sector Incident Communications Conference Line (PICCL) is a communications tool used by the Critical Infrastructures/Key Resources (CIKR) incident communications coordinators to disseminate information to CIKR sectors during incidents

You can find more information on communication channels at <http://www.fema.gov/privatesector/>

Lesson Summary

This lesson presented the following topics:

- Methods to share information in a public–private partnership
- Best practices to communicate with partners during an emergency

In the next lesson, you will learn about best practices to share resources in partnerships.