



Incident Communications Emergency Reference

A Guide for Communication Professionals



Homeland
Security

To: America's Homeland Security Communicators



America and its citizens rose to the challenge on September 11, 2001.

Our Nation fought back. We are now stronger, safer, and better prepared to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur.

But we must still remain vigilant. As President Bush reminded all Americans in July 2002, when he announced his National Strategy for Homeland Security, "We are today a Nation at risk to a new and changing threat."

The Secretary of Homeland Security has the responsibility to manage major domestic incidents. A critical component of that national effort is communications—our ability to inform our citizens accurately and promptly about homeland security issues and incidents. As communicators, this is our challenge—at the Federal, State, local, and private levels.

This incident communications reference is intended to provide you with basic information on homeland security public affairs organization, communications response activity for an incident, and supporting background and contact information. We encourage you to review its content as you develop or update your respective incident communications plans, and to use it as necessary during an actual incident.

Your support, your involvement, and our teamwork in the months and years ahead are critical to the success of the Nation's incident response efforts as well as to ensuring that we keep our citizens appropriately informed.

Sincerely,

A handwritten signature in black ink that reads "Susan K. Neely". The signature is written in a cursive, flowing style.

Susan Neely
Assistant Secretary for Public Affairs

Incident Communications Emergency Reference

Office of Public Affairs

Contents

- vi Quick Response: National Incident
- vii How To Use This Incident Communications Emergency Reference

Chapter 1: Planning Ahead

- 1 What To Do Before an Incident
- 3 Risk Communication
- 7 Homeland Security Advisory System
- 10 Specialized Threat Information
- 10 Preparedness and Ready.gov
- 11 The Department of Homeland Security

Chapter 2: When a National Incident Happens

- 13 What DHS Will Do
- 15 What You Can Do
- 16 First 48 Hours Checklist
- 17 Joint Information Center—The First 12–24 Hours
- 18 Once the Initial Response is Over—48 Hours Onward
- 19 Supporting the Media in a National Incident

Chapter 3: Sources

- 23 Federal Public Affairs Contacts
- 26 State Public Affairs Contact Information
- 30 Acronyms and Terms
- 38 Other References

Appendix A: Tools and Templates

Appendix B: My Plans and Resources

Quick Response: National Incident


A major national incident has just happened and you are managing incident communications. If you cannot implement or access your Public Affairs Action Plan for some reason, consider the following actions immediately:

1. Notify your higher public affairs authority if applicable.
2. Ensure that you are a full member of the incident management team.
3. Establish communications with participating agency counterparts.
4. Contact the Department of Homeland Security (DHS) Public Affairs Duty Officer in the Homeland Security Operations Center by calling (202) 282-8111 or (202) 282-8101, or by e-mail at PublicAffairs.HSCent@dhs.gov.



How To Use This Incident Communications Emergency Reference

The Incident Communications Emergency Reference (ICER) is intended for use by communication professionals at the State and local levels. It is a job aid that is designed to help you plan ahead for a national incident and will help when a crisis occurs.

The first minutes of an incident are critical. This reference guide is a basic overview of key information and lists of key resources to help you in those early minutes. Web sites containing additional information are listed wherever you see a computer icon . You may not have power or Web access during an actual event; therefore, you may want to include hard copies of those Web-based resources in this reference notebook.

You can customize this reference to best suit your needs. For instance, we recommend that you put a copy of your organization's Public Affairs Action Plan behind the Appendix B tab. In addition, you might include information about local vulnerabilities, such as a nuclear power plant, dam, or chemical plant, and any other planning documents that you might need.

Chapter 1: Information you can use before an incident happens.

Chapter 2: Information you can use during the first hours of an incident. If you're wondering what the Department of Homeland Security (DHS) is doing at a certain point, look here.

Chapter 3: Reference information, such as phone numbers, Web addresses, and other information to help you in a crisis.

Appendix A: Tools and Templates: This section provides tools and templates that may be helpful during the first few hours of an incident.

Appendix B: My Plans and Resources: You can put a copy of your Public Affairs Action Plan here as well as any other documents that you feel would be critical in an emergency.

Success in incident communications is a team effort, and DHS wants to hear your suggestions for future editions of this guide. Please e-mail your comments to PublicAffairs.HSCent@dhs.gov.



Chapter 1

Planning Ahead

What To Do Before an Incident

The early hours of any unexpected incident can be confusing and difficult. We cannot anticipate every situation, but being well prepared with emergency communication skills and tools will help. By putting in place in advance the tools you will need, you will facilitate your ability to get timely and accurate information to the public.

1. Develop a Public Affairs Action Plan.

Start simple. Write a plan for your office, building, or agency. It does not have to be complicated.

It must be explicit and written for the person who could be putting it into action in your absence. Don't write it for you; write it so that anyone in your organization can pick it up and use it.

Make sure to include up-to-date notification lists which include multiple ways to reach key individuals. Pre-arrange as many systems and procedures as you can (e.g., electronic notification systems, toll-free hot-lines for public information).

2. Develop relationships with the responders in your region.

Get together and establish a formal or informal plan with all participating and cooperating agencies in your area. Learn their skills and capabilities, and try to coordinate with their plans. Make yourself useful to them and establish a collaborative relationship that can help both parties.

If you can, establish a formal agreement with a joint plan. The plan should be explicit as well as easy to understand and implement.

3. Become familiar with the threats in your area.

Coordinate with your State Homeland Security Advisor to identify possible threats. Identify which threats are in your area.

You may need to include specific elements in your Public Affairs Action Plan for each threat. Identify who will be your messenger for different types of events. For example, if the emergency is health-related, a medical doctor may be more credible than a politician.

4. Train your leadership in your Public Affairs Action Plan.

It is important that your leadership understands your Public Affairs Action Plan. Conduct training with your leadership and the leadership of cooperating agencies to facilitate better understanding of your plans.

Your leadership may offer changes to your plan that will improve your communication with them and enhance the success of your efforts.

5. Identify subject matter experts.

Having people who can flesh out some of the elements of your key messages will be useful to you when communicating with the media and the general public. These subject matter experts must have as intimate an understanding as possible of the elements of your key messages and be able to explain these elements clearly. If possible, have the subject matter experts complete media training well in advance of an incident.

6. Develop relationships with the media.

During an incident is not a good time for a first meeting with the members of your local media. Request meetings, help develop stories, and find opportunities to introduce yourself and be a good resource.

Schedule meetings with your leadership and editorial boards to help everyone better understand each other. This will help promote more accurate reporting in the event of an incident.

Through their questions, some reporters can provide you with feedback from the “street” that may help you clarify the information you are providing to the public. Having a good relationship with these reporters will help ensure that accurate and clear information is communicated in the event of a crisis.

7. Develop relationships with the formal and informal community leaders.

Some of the most helpful people are formal and informal community leaders. Find out who these influential people are and meet with them.

Think about nontraditional community leaders, such as popular local store managers, daycare providers, clergy, and fire chiefs, and include them in your communication efforts.

8. Plan for communicating with non-English speakers.

If your area has a large non-English speaking population, identify translators.

9. Train, prepare, plan, and don't be afraid to change your Public Affairs Action Plan if necessary.

No plan is useful unless everyone understands it completely and it is up-to-date. Don't be afraid to make changes to the plan. Things change all the time.

10. Participate in risk communication training.

Communicating in a major emergency situation, particularly a terrorist event, is very different from communicating about routine matters or smaller crises. It is critical that all members of your team attend training in risk communication.

Risk Communication

In ordinary circumstances, your role is to provide the public with information. This role does not change during the extraordinary time of an emergency, such as a terrorist attack, but the stakes are much higher.

There are several differences between ordinary and extraordinary times. These differences demand a new look at the context in which the messages are created and delivered.

Lives are at stake. An emergency situation differs drastically from a “normal” one primarily because, during an emergency event, information has the power to save lives. Possibly many, many lives. People require information to find out what is actually happening and also what they must do to safeguard their own and their family’s personal safety. But strong emotional responses to the event make understanding and acting upon that information more difficult.

...great distress or fear can also make it hard for people to process information. Word messages simply and repeat them often.

There is great uncertainty. Almost every instance of terrorism presents a new and previously unknown set of circumstances to you, as officials trying to manage the situation, and to the public at large. Even though we know a lot about ways in which a terrorist attack might unfold, in reality we do not know everything we might like to know. (For example, before anthrax was distributed through the mail, medical experts were not sure whether people could contract anthrax through the mail.) People in communities will be trying to cope with the situation and take necessary actions to protect their health and safety, while what we know and believe is constantly evolving.

Individual and community levels of distress peak.

Fear and uncertainty lead to unusually high levels of distress. Because of the psychological impact of acts of terrorism, it is not enough to give the facts of the situation and tell the public what to do, and expect that people will actually take these protective actions. High distress levels can keep individuals and communities from engaging in protective behaviors. However, how we communicate can actually help channel this distress into productive and protective behaviors instead of destructive ones. Distress, if not excessive, leads to information-seeking and precautionary behavior. But great distress or fear can also make it hard for people to process information. Word messages simply and repeat them often. People can better bear their fear and make appropriate decisions about safeguarding their health and safety when their fears are acknowledged, as opposed to when they are told not to be fearful.

The psychology of response to a terrorist attack is different from that of response to other types of emergencies. Current knowledge and widely accepted theories of disaster psychology suggest that many aspects of a terrorist attack, whether biological or other, have an impact on how the public thinks, feels, and responds to information. This will have implications for media communications. Some of these psychological aspects include:

- The intentional nature of the assault (as opposed to hurricanes and floods, for example)
- Unfamiliar agents or pathogens
- The random nature of the attacks and the fact that they are largely outside our control as members of the general public, officials, the media, etc.
- The potential for permanent and catastrophic harm and loss
- The involuntary nature of exposure

Given these aspects of terrorism, we know that people react and respond to information differently in times of attack from the way they do in ordinary times.

In what ways do people react differently to terrorism?

On the basis of experience from past emergencies, experts believe that an individual's decisionmaking process changes during a catastrophic emergency related to terrorism.

- **People simplify.** Individuals' ability to comprehend numerous levels of detail decreases early in their response to an emergency. This means that people will generally miss nuances that help define a situation early. Advice, including the protective actions individuals need to take, must be stated clearly, simply, and repeatedly.

Research indicates that the first message to reach listeners may often be the most accepted message, even if more accurate information surfaces later.

- **People become much more vigilant in a crisis.** They check out their neighbors for signs of terrorism, surf the Internet for background information, become glued to the media for news and context. This hypervigilance can have negative emotional consequences (added trauma from additional exposure to a traumatic event, for example), but is also useful as it helps people collect and assess the infor-

mation they are getting. Is it consistent? What do people they respect think about it?

- **People maintain their current beliefs.** People are adept at maintaining faith in their current beliefs during a crisis. They tend to avoid contradictory or conflicting information. This means that if a new situation challenges conventionally held beliefs or views, it may be difficult to convince people that there is a new truth. Resistance to change (in beliefs) increases.
- **People rely on past experiences.** Whether or not past experiences are relevant, people use them to help define new ones. People remember what they see. They tend to believe what they have experienced in their own lives. When faced with a terrorism emergency, however, they will have to rely on experts. But even reputable experts may disagree about the level of threat, the risks, and the appropriate recommendations. In nonemergency times a natural give and take occurs among experts. In times of crisis, conflicting information may leave the public with increased uncertainty and fear. Research indicates that the first message to reach listeners may often be the most accepted message, even if more accurate information surfaces later.

What are the objectives of the public in an emergency?

Most citizens share five main objectives during emergencies, including those provoked by terrorists:

- Protect themselves and loved ones
- Get the facts they want and need to protect themselves
- Be able to make choices and take action
- Be involved in the response
- Stabilize and normalize their lives

How people feel can affect their ability to meet those objectives.

Fear. Fear is one of the single most powerful emotions present during a terrorism emergency. It has the capacity to propel community members to action. Whether that action is helpful or harmful to the community depends on whether the individual can hear, understand, and act

on sound guidance from authorities. In the aftermath of past emergencies, we have learned that the least common reaction to crisis is panic. Instead, people typically take action. Effective messages from officials can help people make appropriate decisions.

...we have learned that the least common reaction to crisis is panic. Instead, people typically take action. Effective messages from officials can help people make appropriate decisions.

Denial. Some members of the community may be in denial. They may choose not to hear or heed warnings or recommended actions. They may become confused by the recommendations—or simply not believe the threat is real or that it is an actual personal threat. In such cases, people may not act on even the best advice.

Denial, in fact, is one of the reasons why panic is rarer than we realize. People go into denial as a coping mechanism when the fear is too great. But there are several important antidotes to denial. The two key ones are: first, the legitimization of fear—people who feel entitled to be afraid don't have to go into denial, and second, action—people with something to do have more capacity to tolerate their fear and are therefore less vulnerable to denial.

Helplessness, hopelessness. Some people can accept that the threat is real, but it looms so large they believe the situation is hopeless, and therefore they feel helpless to protect themselves. The resulting withdrawal and paralysis can impair their ability to take appropriate protective action in an emergency.

People who feel powerless to affect the outcome are more likely to retreat to denial and the resulting helplessness and helplessness that lead to inaction. Therefore, self efficacy is important. Helplessness, hopelessness and denial are all reduced by messages of self efficacy and empowerment (not “everything will be fine,” but “it’s a bad situation, but there are things you can do to make it better, such as...”)

Stigmatization. Some members of your community may suffer even greater effects from the attack if the rest of the community stigmatizes them. Fear or isolation of a group may occur if the community perceives it as “risky.” For example, people may perceive groups, such as Arab-American communities following September 11, as being related to those who are “to blame,” and these groups can become targets of local violence, even though they are as much victims of the terrorist attack as their neighbors.

Vicarious rehearsal. Experience has shown that people farther away (by distance or relationship) from the threat may actually react as strongly as those who are more directly impacted. The media allow people to participate vicariously in a crisis when they are not in immediate danger. This psychologically normal response to new risky situations results in people mentally rehearsing the crisis as if they were experiencing it and asking themselves, “What would I do?” In their minds, they imagine that the risk is here (instead of there), now (instead of soon) and for sure (instead of maybe). They may believe that they, too, are at immediate risk and demand unnecessary services; as a result, they may go to the emergency room or take medications they do not need. Their stress reactions will be high, even though they are not in immediate danger, often resulting in some of the health consequences of stress. Further, because many of the agents are invisible and difficult to detect, we may not always be able to tell a community with certainty that it has not been exposed. This imaginative leap from there/soon/maybe to here/now/definitely can be beneficial if it is acknowledged and the opportunity is taken to prepare, emotionally and logistically, for a real crisis.

Suggested message components

To communicate effectively with people who are experiencing different reactions to an emergency situation, you should have distinct messages prepared that address their particular needs. These include messages that **express empathy, clarify facts, and call people to action.** The following table provides suggested message components, explains why they are important, and offers examples.

Suggested Message Components

What	Why	Example
Expression of empathy and acknowledgment of fear and uncertainty	Public officials are usually trained never to speak with or about emotions; rather, about facts. Therefore, expressing empathy, fear, or uncertainty can be particularly difficult for officials to do. Experts believe that citizens need to know that their feelings are understood and acknowledged by authorities. This helps establish a connection and makes it a little easier for audiences to hear the difficult information that usually follows.	“Whatever it [the loss of lives] is, it will be more than we can bear. . . .” R. Giuliani, September 11, 2001
Clarification of facts	It is important to provide as much factual information as you can about the situation.	“At 10:05 a.m., a bomb exploded at...”
What we do not know	Just as expressions of empathy may not always come naturally, discussing the unknown elements of the situation also goes against years of professional training and experience. You may be used to having confirmation of all of the facts before releasing information. However, waiting until you have an answer to every possible question could jeopardize public safety. There will be many things you do not know, such as when you suspect a particular agent was released but have not yet confirmed it. It is also likely that, in the initial stages of such an investigation, you will not know the route of exposure or who caused the situation. Even so, the public will benefit from learning what you know and don’t know.	“As our understanding of the situation evolves, we will provide you with updates on what we know and what we do not know.”
Steps we are taking to get more facts	Although there is much you may not know, you can communicate the immediate steps you are taking to get more facts and to begin to manage the emergency. The public can more easily accept high levels of uncertainty when they are aware of the actions you are taking to find answers. Be as specific about these actions as you can.	“We do not know right now if the train derailment is a terrorist act, but DHS and the FBI are gathering evidence and talking to witnesses to determine what caused the accident.”
Call to action—giving people things to do	Once you deliver the first four parts of the message, the public can better hear and act on your advice. In a crisis where immediate action needs to be taken (e.g., sheltering in place due to a radiological incident), this may be the second part of your message. In some cases of less urgency, even symbolic actions can help channel people’s energy and desire to do something.	<i>Protective actions:</i> ■ Boil your water before drinking or drink bottled water. <i>Helpful actions:</i> ■ Donate blood or money to a charity that is providing assistance. <i>Symbolic actions:</i> ■ Light a candle or fly the flag.
Referrals	Tell the public when the next update will occur and where they can go for more information, such as helpful Web sites to visit or hotlines to call.	“We expect to have the test results confirmed within the next 12 hours and will let you know what we are dealing with at that time. . . .”

Note: It is important to consider all of these components as you develop messages. In Appendix A, a message development worksheet is included to assist you in developing messages that include these components.

Homeland Security Advisory System

On March 11, 2002, the Homeland Security Advisory System (HSAS) was unveiled as a tool to improve coordination and communication among all levels of government, the private sector, and the American public in the fight against terrorism.

The HSAS combines threat information with vulnerability assessments. This information is then communicated with public safety officials and the public at large through a color-coded system with different Threat Condition levels. Changes in Threat Condition may indicate that protective measures should be implemented to reduce the likelihood or impact of an attack. Raising the Threat Condition has economic, physical, and psychological effects on the Nation, so changes in Threat Condition are not made lightly. The HSAS can be raised for the entire Nation, or can be raised for certain geographic regions or industry sectors, on the basis of intelligence reports at the time.

HSAS

- Low (Green)
- Guarded (Blue)
- Elevated (Yellow)
- High (Orange)
- Severe (Red)

The advisory system not only identifies the Threat Condition but also outlines protective measures that can be taken by others. The advisory system is binding on the executive branch and voluntary, although sug-

gested, for State, local, territorial and tribal governments, and the private sector. However, not only do all Federal agencies have action plans that correspond to the threat level, but so do all 50 states, most major cities and increasingly members of the private sector, thus reducing our vulnerability to attack. The actions required at each Threat Condition are primarily intended for security professionals. For this reason, State and local law enforcement and other security professionals at all levels of government and the private sector receive more specific information than is made available to the general public, including recommendations of protective measures that should be taken.

The following threat conditions represent increasing levels of risk of terrorist attacks. Beneath each threat condition are some suggested protective measures.

1. Low Condition (Green)

Declared when there is a low risk of terrorist attacks

- Refine and exercise, as appropriate, preplanned protective measures
- Ensure personnel receive proper training on the HSAS and specific preplanned department or agency protective measures

- Institutionalize a process to ensure that all facilities and regulated sectors are regularly assessed for vulnerabilities to terrorist attacks and that all reasonable measures are taken to mitigate these vulnerabilities

2. Guarded Condition (Blue)

Declared when there is a general risk of terrorist attacks

- Check communications with designated emergency response or command locations
- Review and update emergency response procedures
- Provide the public with any information that would strengthen its ability to act appropriately

3. Elevated Condition (Yellow)

Declared when there is a significant risk of terrorist attacks

- Increase surveillance of critical locations
- Coordinate emergency plans as appropriate with nearby jurisdictions
- Assess whether the precise characteristics of the threat require the further refinement of preplanned protective measures
- Implement, as appropriate, contingency and emergency response plans

4. High Condition (Orange)

Declared when there is a high risk of terrorist attacks

- Coordinate necessary security efforts with Federal, State, and local law enforcement agencies or any National Guard or other appropriate armed forces organizations

- Take additional precautions at public events and possibly consider alternative venues or even cancellation

- Prepare to execute contingency procedures, such as moving to an alternate site or dispersing the workforce

- Restrict threatened facility access to essential personnel only

5. Severe Condition (Red)

Reflects a severe risk of terrorist attacks

- Increase or redirect personnel to address critical emergency needs

- Assign emergency response personnel, and preposition and mobilize specially trained teams or resources

- Monitor, redirect, or constrain transportation systems

- Close public and government facilities






The Department of Homeland Security has developed some recommended actions for citizens to take during different threat conditions as described on the next page. These can be found at <http://www.dhs.gov/interweb/assetlibrary/CitizenGuidanceHSAS2.pdf>.



Personal protective measures: www.ready.gov

Workplace and personal protective measures: www.redcross.org

Citizen Guidance on the Homeland Security Advisory System

Risk of Attack	Recommended Actions for Citizens*
 <p>GREEN Low Risk</p>	<ul style="list-style-type: none"> ■ Develop a family emergency plan. Share it with family and friends, and practice the plan. Visit www.ready.gov for help creating a plan. ■ Create an “Emergency Supply Kit” for your household. ■ Be informed. Visit www.ready.gov or obtain a copy of “Preparing Makes Sense, Get Ready Now” by calling 1-800-BE-READY. ■ Know how to shelter-in-place and how to turn off utilities (power, gas, and water) to your home. ■ Examine volunteer opportunities in your community, such as Citizen Corps, Volunteers in Police Service, Neighborhood Watch, or others, and donate your time. ■ Consider completing an American Red Cross first aid or CPR course, or Community Emergency Response Team (CERT) course.
 <p>BLUE Guarded Risk</p>	<ul style="list-style-type: none"> ■ <i>Complete recommended steps at level green.</i> ■ Review stored disaster supplies, and replace items that are outdated. ■ Be alert to suspicious activity and report it to proper authorities.
 <p>YELLOW Elevated Risk</p>	<ul style="list-style-type: none"> ■ <i>Complete recommended steps at levels green and blue.</i> ■ Ensure disaster supply kit is stocked and ready. ■ Check telephone numbers in family emergency plan, and update as necessary. ■ Develop alternate routes to/from work or school, and practice them. ■ Continue to be alert for suspicious activity and report it to authorities.
 <p>ORANGE High Risk</p>	<ul style="list-style-type: none"> ■ <i>Complete recommended steps at lower risk levels.</i> ■ Exercise caution when traveling; pay attention to travel advisories. ■ Review your family emergency plan, and make sure all family members know what to do. ■ Be patient. Expect some delays, baggage searches, and restrictions at public buildings. ■ Check on neighbors or others who might need assistance in an emergency.
 <p>RED Severe Risk</p>	<ul style="list-style-type: none"> ■ <i>Complete all recommended actions at lower risk levels.</i> ■ Listen to local emergency management officials. ■ Stay tuned to TV or radio for current information/instructions. ■ Be prepared to shelter-in-place or evacuate, as instructed. ■ Expect traffic delays and restrictions. Provide volunteer services only as requested. ■ Contact your school/business to determine status of work day.

*Developed with input from the American Red Cross.

Specialized Threat Information

In addition to the ability to change the Threat Condition, the advisory system also uses communication tools, called threat products, to provide more targeted and specific information about terrorism to representatives of specific sectors of critical infrastructure or State and local homeland security professionals.

There are two types of threat products:

1. **Homeland Security Threat Advisories** (warnings)
2. **Homeland Security Information Bulletins** (non-warnings)

Homeland Security Threat Advisories contain actionable information about a threat targeting critical national networks, infrastructures, or key assets. They could relay newly developed procedures that, when implemented, would significantly improve security or protection. They could also suggest a change in readiness, protective actions, or response. This category includes products formerly called alerts, advisories, and sector notifications.

Homeland Security Information Bulletins communicate information of interest that does not meet the timeliness, specificity, or significance thresholds of warning messages. Such information may include statistical reports, periodic summaries, incident response or reporting guidelines, common vulnerabilities and patches, and configuration standards or tools. Bulletins may include preliminary requests for information from the recipients.

Either advisories or bulletins can be distributed without a change in the national threat level. Often a redacted version of a bulletin or advisory is made available on the department's Web site to provide context to the media or public and avoid confusion.

Preparedness and Ready.gov

The mission of the Department of Homeland Security (DHS) is to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and

minimize the damage from potential attacks and natural disasters. DHS pursues its mission through many avenues, including strengthening first responders, securing borders, and protecting infrastructure, but homeland security is a national, not a Federal, effort. In addition to strengthening local communities and first responders, DHS is also working to raise the basic level of citizen preparedness across the Nation.

The Ready Campaign is a public education campaign designed to educate and empower Americans to prepare for and respond to potential terrorist attacks. The goals of the campaign are to:

- Raise public awareness concerning the importance of being prepared;
- Motivate Americans to take specific actions to protect themselves, their families, and their communities; and
- Raise the basic level of citizen preparedness across the nation.

Ready.gov provides Americans with steps they can take that will minimize the impact a terrorist event or other emergency may have on their lives. It offers practical suggestions to increase preparedness, including learning about existing threats, assembling disaster supply kits, and developing family emergency plans.

- DHS will make available for State and local use campaign materials to improve citizen preparedness in your community. Businesses should also be encouraged to take action to protect their own businesses against disasters and to prepare employees for emergencies.
- Explaining weapons of mass destruction (WMD) to the public may require expertise not immediately available in your local area. Fact sheets are available at ready.gov as well as at the Federal Emergency Management Agency (FEMA), and the Centers for Diseases Control and Prevention (CDC) Web sites listed below.



Preparing for terrorism-related incidents: www.ready.gov

Preparing for general emergencies: www.FEMA.gov

Chemical, biological, and radiological threats: www.bt.cdc.gov

The Department of Homeland Security

The department's first priority is to protect the Nation against terrorist attacks. Agencies within DHS analyze threats and intelligence, guard our borders and airports, protect our critical infrastructure, and coordinate the response of the Nation in emergencies.

Besides providing a better-coordinated defense of the homeland, DHS is also dedicated to protecting the rights of American citizens and enhancing public services, such as natural disaster assistance and citizenship services, by dedicating offices to these important missions.

The DHS organizational structure has five components:

1. **Border and Transportation Security (BTS):** BTS is responsible for maintaining the security of the Nation's borders and transportation systems. It is home to agencies such as the Transportation Security Administration, U.S. Customs and Border Protection, and the border security functions of the Citizenship and Immigration Services and U.S. Immigration and Customs Enforcement. BTS works hand in hand with the U.S. Coast Guard.
2. **Emergency Preparedness and Response (EPR):** The Federal Emergency Management Agency (FEMA) is the major component of Emergency Preparedness and Response, and ensures that our Nation is prepared for, and able to recover from, both terrorist attacks and natural disasters.
3. **Science and Technology (S&T):** S&T coordinates the department's efforts in research and development, including preparing for and responding to the full range of terrorist threats involving weapons of mass destruction (WMD).
4. **Information Analysis and Infrastructure Protection (IAIP):** IAIP merges under one roof

the capability to identify and assess a broad range of intelligence information concerning threats to the homeland, to issue timely warnings, and to take appropriate preventive and protective action.

5. **Management and Administration (M):** The Under Secretary of Management is responsible for budget, management, and personnel issues in DHS.

Agencies within DHS analyze threats and intelligence, guard our borders and airports, protect our critical infrastructure, and coordinate the response of the Nation in emergencies.

Besides the five components, several other critical agencies are part of the department:

- **United States Coast Guard (USCG):** The Commandant of the Coast Guard reports directly to the Secretary of Homeland Security. However, the USCG also works closely with the Under Secretary of Border and Transportation Security as well as maintains its existing independent identity as a military

service. Upon declaration of war, or when the President so directs, the USCG would operate as an element of the Department of Defense, consistent with existing law.

- **United States Secret Service:** The primary mission of the Secret Service is the protection of the President and other government leaders, as well as security for designated national events. The Secret Service is also responsible for protecting U.S. currency from counterfeiters and safeguarding Americans from credit card fraud.
- **Bureau of Citizenship and Immigration Services (CIS):** While BTS is responsible for enforcement of

our Nation's immigration laws, the Bureau of Citizenship and Immigration Services dedicates its full energies to providing efficient immigration services and easing the transition to American citizenship. The Director of CIS reports directly to the Deputy Secretary of Homeland Security.

- **Office of State and Local Government Coordination and Preparedness:** A truly secure homeland requires close coordination between local, State, and Federal governments. This office ensures that close coordination takes place with State and local first responders, emergency services, and governments.





Chapter 2

When a National Incident Happens

What DHS Will Do

Before an Incident

Watching the homeland. The Department of Homeland Security maintains a continuously staffed operations center, the Homeland Security Operations Center (HSOC). This center is staffed with DHS personnel and representatives from key agencies of the Federal Government. They continually monitor incident developments from around the Nation, intelligence information, and news reports. They prepare incident summaries and advise the Secretary on courses of action and issues that warrant further evaluation. The senior watch officer (SWO) directs the actions of this comprehensive watch team.

The DHS Public Affairs Watch Team. DHS Public Affairs supports the HSOC watch with a public affairs duty officer. This duty officer works closely with the DHS Public Affairs Press Office on emerging media developments and interview coordination requirements. In many respects, this staff of experts functions as a continuous joint information center (JIC), constantly reviewing media activity and coordinating responses. In addition, this watch team has prearranged resources and information available to allow them to contact interagency public affairs personnel in

the Federal Government and counterparts with State, local, and private agencies or organizations. This watch team provides an in-place public affairs resource in the event that a national incident occurs. Under Threat Condition Yellow, the HSOC public affairs desk operates 16 hours a day on weekdays. Hours are extended during times of increased threat or vigilance.

During an Incident

The first hour of a national incident. DHS Public Affairs is fully integrated with the HSOC as an incident becomes known. When this happens, DHS Public Affairs has several tasks that it must manage on a simultaneous basis:

- It must support the Secretary, senior DHS leadership, and the HSOC. Upon activation of the Interagency Incident Management Team (IIMG), support will be provided through the Assistant Secretary for Public Affairs and senior leadership. The IIMG is a special on-call staff of representatives from all DHS components and key Federal departments and agencies. Its principal task is to advise the secretary on incident management. A public affairs representative serves on the IIMG.

- The Assistant Secretary for Public Affairs will activate the Incident Communications Emergency Policy and Procedures (ICEPP). The ICEPP is part of the National Response Plan. The ICEPP is a communication plan detailing initial coordination measures and contact requirements. It is structured to ensure that the primary incident communication processes of control, coordination, and communication are managed during the incident.
- In support of these steps, the HSOC public affairs duty officer will immediately initiate actions in the ICEPP.

Our communication goal. Our collective goal as communicators is to ensure that the American people are informed about an incident, including any associated health or preventive measures they will need to take or should take. The specific incident communications objective for DHS is to coordinate communication of the federal response and to deliver timely, accurate information to the public. To meet this objective, all levels of Government—Federal, State, and local—must work quickly to pool their knowledge and coordinate their efforts, thus ensuring a clear and consistent message to our citizens.

. . . all levels of government—Federal, State, and local—must work quickly to pool their knowledge and coordinate their efforts, to ensure a clear and consistent message to our citizens.

Communication links. With this objective in mind, DHS will organize an interagency/intergovernmental effort addressing incident communications control and coordination. The purpose is to gather the facts about the incident and to establish initial coordination

points, particularly at the State and local levels. DHS will also activate a special conference-call line, the National Incident Communications Conference Line (NICCL), to bring all key participants together via phone. DHS will initiate the NICCL and will facilitate State and local access to the line. DHS will establish communication links to the following:

- Federal public affairs contacts (cabinet departments, key agencies)
- Incident site public affairs leaders (State, local, private, as appropriate)

Incident site actions. DHS recognizes that the public affairs team at the site of a national incident faces significant challenges. Information may be limited and hard to verify, and the true cause of the incident—terrorist or otherwise—may be unconfirmed. Public affairs communicators at the incident site must respond to and support their incident managers or political leadership, especially since a JIC would not be established so early in a crisis. DHS has a similar challenge, but the audience is the Nation, and a range of other communication issues must be addressed. The challenge, therefore, is for both DHS and the site manager to work together in those early minutes and address the control, coordination, and communication process issues. Who contacts whom first is not important, but early communication between DHS and the incident site is critical to maintaining public confidence. Generally, DHS will focus its communication efforts toward the national level and the impact of the incident nationwide, while the State, local, or private authorities manage the specific incident.

After the first releases. After the first releases of information, including those at the site and by DHS, it is expected that a JIC would be established to manage the incident communications process.

What You Can Do

The Emergency Phase—First Hours

The emergency phase of an incident starts the moment an incident occurs. The incident will be evolving rapidly and information may be inconsistent or difficult to verify. It is likely that media interest will be very intense. A good plan can help you stay on top of the situation and can help you handle any uncertainties. Alerting higher authorities and keeping them up to date with regular reports as much as possible will also help you in your requests for assistance, if needed.

In general, the following steps will need to be completed in the early hours of an incident:

- Verify and assess the situation
- Conduct notifications
- Assess the magnitude of the crisis
- Organize and delegate assignments
- Prepare information and obtain approvals
- Release information to public

Your Public Affairs Action Plan, created in advance of an actual incident, should address exactly what communication activity will take place during a crisis. The more detailed and complete your plan is, the better off you will be when a crisis happens. For example, in your crisis plan, you should have a detailed notification list that is updated regularly and includes several ways to contact key people. In advance, you should also determine exactly who will be on your response team and who will be responsible for what. Plan for backups in case specific people are not available.

As you develop information for release to the public during the initial hours, keep in mind your primary communication objectives:

- Acknowledge the event with empathy.
- Explain and inform the public, in simplest terms, about the risk.
- Establish organization/spokesperson credibility.
- Provide emergency courses of action (including how and where to get more information).
- Make a commitment to stakeholders and the public concerning your continued communication with them.

A number of tools in Appendix A can help you in your initial response. Tools include the Incident Situation Summary/Incident Verification checklist and several message development and press statement development templates. The First 48 Hours Checklist on the next page may also be helpful.

First 48 Hours Checklist

Critical First Steps After Verification

Notification	Done
1. Ensure your leadership is aware of the emergency and that they know you are involved.	<input type="checkbox"/>
2. Use your crisis plan’s notification list to ensure all of the communication chain of command is aware and know you are involved.	<input type="checkbox"/>
3. Give leadership your first assessment of the emergency from a communications perspective and inform them of the next steps you are taking.	<input type="checkbox"/>
Coordination	Done
1. Contact local, State, and Federal partners now.	<input type="checkbox"/>
2. If potential criminal investigation, contact FBI counterpart now.	<input type="checkbox"/>
3. Secure spokesperson as designated in the plan.	<input type="checkbox"/>
4. Initiate alert notification and call in extra communication staff, per the plan.	<input type="checkbox"/>
5. Connect with the Joint Information Center-make your presence known.	<input type="checkbox"/>
Media	Done
1. Be first: Provide a statement that your agency is aware of the emergency and is involved in the response. (Use the Template for Prescribed, Immediate Response to Media Inquiries.)	<input type="checkbox"/>
2. Be credible: Give directions to media about when and where to get updates from your agency.	<input type="checkbox"/>
3. Be right: Start monitoring media for misinformation that must be corrected now.	<input type="checkbox"/>
Public	Done
1. Trigger your public information toll-free number operation now if you anticipate the public will be seeking reassurance or information directly from your organization. (You can adjust hours of operation and number of call managers as needed.)	<input type="checkbox"/>
2. Use your initial media statement as your first message to the public.	<input type="checkbox"/>
3. Ensure your statement expresses empathy and acknowledges the public’s concern about the uncertainty.	<input type="checkbox"/>
4. Give the precleared facts you have, and refer the public to other information sites, as appropriate.	<input type="checkbox"/>
5. Remind the public that your agency has a process in place to mitigate the crisis.	<input type="checkbox"/>
6. Start monitoring public calls to catch trends or rumors now.	<input type="checkbox"/>
Partners/Stakeholders	Done
1. Send a basic statement to partners (the same as to the media) to let them know you are thinking about them.	<input type="checkbox"/>
2. Use prearranged notification systems (preferably e-mail Listserv®).	<input type="checkbox"/>
3. Engage leadership to make important first phone calls, based on your plan, to partners and key stakeholders to let them know your agency is responding.	<input type="checkbox"/>
4. Use the internal communication system (e-mail) to notify employees that their agency is involved in the response and that updates will follow. Ask for their support.	<input type="checkbox"/>

Joint Information Center—The First 12–24 Hours

After the initial releases of information, a Joint Information Center (JIC) will likely be established to help coordinate future releases and to manage the tremendous media presence that inevitably accompanies a national incident. The National Incident Management System (NIMS) describes the principles, components, and procedures needed to support effective emergency public information operations. (See the Web address for NIMS at the bottom of the page.)

A JIC is a group of representatives, from agencies and organizations involved in an event, who handle public information needs. The JIC structure is designed to work equally well for large or small situations and can expand or contract to meet the needs of the incident. Ideally, there will be only one JIC.

The JIC is led by a public information officer (PIO) who advises the local, regional, State, or Federal Incident Commander (IC) and who supervises the operations of the JIC. The PIO has four primary responsibilities:

- Gather incident data
- Analyze public perceptions of the incident
- Prepare spokespersons
- Inform the public

The basic JIC organization creates positions to support the PIO’s primary responsibilities. These positions

should be staffed by individuals with particular skills in the areas of these responsibilities. To provide accurate and timely information to the public, the JIC must have the most current and accurate information on the incident. The JIC should be established close to the IC to facilitate the flow of information.


When multiple public or private agencies and organizations come together to respond to an incident, efficient information flow is critical to the success of the public affairs response. A JIC is a centralized “communication hub” that serves to achieve that information flow.

Establishing a JIC, developing processes and procedures, and training staff on how to operate a JIC effectively allow organizations to be more proactive in responding to the information needs of responders; the public; Federal, State, and local governments; foreign governments; and industry.

Because of the critical nature of providing emergency information to disaster victims, time spent getting organized rather than responding at the time of an event can lead to confusion and a loss of public confidence. Through a JIC, the different agencies (including State, local, and other entities) involved in a response can work in a cohesive manner, enabling them to “speak with one voice.”

You may find the JIC Equipment and Supplies Checklist, in Appendix A helpful.

Public Affairs-Related JIC Positions	Skills
Data Collector	Investigative Reporting
News Release Writer	Writing/Editing
Phone Dissemination	Interpersonal/Verbal

 **NIMS: <http://www.dhs.gov/dhspublic/display?theme=51&content=3423>.**

Once the Initial Response is Over—48 Hours Onward

After the initial phase of the crisis is over, the public and the media will start to look for more in-depth information—particularly why the crisis happened, what are the long-term effects, and what can be done to be sure it doesn't happen again. The exact timing of the next phase depends on the nature of the crisis and how it unfolds. In some cases, the crisis may still be evolving a great deal at the 48-hour point.

At this stage, it is important to stick to your plan, adjust your procedures as needed, and get out information as you have it. Pay attention to local media. Once the dust starts to settle, you will be left with

local media. If you ignore the local media, your long-term relationship with them will be damaged.

Consider whether the level of resources used in the initial phase is still needed, if additional resources are needed, and if assignments need to be adjusted.

Eventually, the crisis will be less intense and take you into the postevent phase. Then you can evaluate your response, help key stakeholders recover from the crisis, address any late-breaking issues, and plan for the future.

Supporting the Media in a National Incident

Although disasters and major incidents attract national and often international interest, they are essentially local in nature. Individuals have two immediate questions: (1) Am I in danger? (2) Is someone I care about in danger?

Letting the public know what to do for their own individual safety becomes an instant priority, and circulating information quickly can be a matter of life and death.

When time and resources are stretched, focus on TV and radio as the primary means for getting out your message. Recent research indicates that 57 percent of Americans will turn to television to get information in the event of a terrorist attack, 15 percent will turn to radio, and nine percent will turn to Government and news Web sites.¹ Although the survey did not address other types of emergencies, it is reasonable to expect similar results.

Letting members of the public know what to do for their own safety becomes an instant priority, and circulating information quickly can be a matter of life and death.

No matter what the medium, reporters and the public have basic needs. Your Public Affairs Action Plan should address these needs.

The kinds of questions that may be asked by the media and the public are listed below.

What the Media Will Ask First

- What happened?
- Who is in charge?
- Has this been contained?
- Are the victims being helped?
- What can we expect?
- What should we [the public] do?
- Why did this happen?
- Did you have forewarning?
- How long have you known about this?
- What do these data or this information mean?

¹Poll of 1,001 adults, conducted from August 5–11, 2003 by the Pew Internet & American Life Project and by Federal Computer Week magazine.

- What bad things aren't you telling us?
- Is this terrorism?
- Could this be terrorism?
- Are you investigating this situation as possible terrorism?
- Is the FBI involved in this investigation?
- When will you be able to tell us whether or not this situation is terrorism?

What the Public Will Ask First

- Are my family and I safe?
- What have you found that may affect me?
- What can I do to protect myself and my family?
- Who caused this?
- Can you fix it?

Working with the Media

The quickest way to improve your relationship with the media is to understand the finite aspects of their job—they have space and time to fill and deadlines to meet. Know those deadlines, and work to accommodate them. During a crisis, be available—if necessary, around the clock—to help reporters get the facts and get them right, before deadline. Attempt to give media a reasonable expectation of when new information will be provided. Establish a schedule for information releases as quickly as possible.

Even print media face short deadlines because of their online Web editions. Improving technologies require a revamping of the way emergency information is provided to the media, so the best way for a public agency to approach this responsibility is to provide all media

with simultaneous and identical access. As technology progresses, this becomes easier to do. Through the use of preestablished e-mail addresses, fax numbers, and onsite media opportunities (including teleconferencing, so offsite media can stay informed), you can be an exemplar of fairness. In the first critical hours or days of an emergency, do not play favorites. Equal access to information is imperative. If you have a message to communicate that is essential to the well-being or safety of the public, it is not up to you to decide from what source people obtain information. Give the same information to all media all the time.

Today, everyone seems to have the same deadlines, and this requires a revamping of the way emergency information is provided to the media.

How to keep reporters informed

The more you can anticipate the needs of the media, the more completely you will accomplish your goals: inform the public, help the public understand safety actions or recommendations, and gain public acceptance for official activities during the response and recovery of a major terrorism-related emergency. Background information—the information that will not change during a crisis—should be in place as soon as possible and should be easily retrievable.

Media operations in a crisis

During an unfolding emergency, media may operate differently than in non-emergency situations. During the early moments of a crisis, you must expect from media the possibility of the following:

- **Diminished information verification.** Since it is difficult to reach all reporters with confirmed information at the beginning of a crisis, some early reports might be tentative, sometimes incorrect.

■ **United efforts between media and government.**

Media and government share the same goals—to communicate accurate, timely emergency information to the public during a crisis.

- **In major crises, expect the national media to dominate.** Most people will obtain their news from the national media. Local media will feed information to national broadcast and electronic media. The national media will coordinate the coverage. Messages meant for local audiences will have to compete for airtime with the national coverage. Respect local media deadlines, and keep the information flowing to help disseminate local messages.

Messages meant for local audiences will have to compete for airtime with the national coverage.

- **Media will expect a JIC.** The JIC can provide the media with consolidated information for their viewers and listeners. Initially, the media will accept that much of their information must come from the command post. Within hours or days, depending on the crisis, media will look for other perspectives and other places from which to broadcast. If you want the media to use official releases of information, you will have to ensure that the information is timely, fresh, and easy to access. An effective, well-functioning media command center is one that gives the most, the most accurate, and the freshest information.
- **Provide scientific expertise.** Be prepared to provide a scientific expert who can address technical or medical questions in a crisis. Remember not to assume that everyone knows the technical jargon.

Getting emergency information to the media

Some options for getting the information out to the media are the following:

Media releases: In an emergency, print information must move electronically to the media or be given as handouts to media at the site of the incident. If information is important enough to put down on paper (and the information will remain current for at least a 12-hour cycle), releases may be a good option.

Press conferences: A press conference can be arranged at the site of the crisis, allowing the release of information to all media, even if it's conducted without press kits or an opportunity for questions and answers.

Satellite media tours: At the national or regional level, or at the local level if media in other cities are pushing for access, a satellite media tour may be appropriate. While a satellite media tour can be arranged in a matter of hours during a crisis, it may not be an efficient tool early in the emergency. A tour may be an effective tool for communities to talk to each other through the media—offering support, ideas, and lessons learned. Satellite media tours are usually conducted by a single spokesperson or subject matter expert (SME) and are intended to allow local media to interview the SME (who is in another location) directly. To avoid confusion, be sure that the SME has a Teleprompter® identifying the speaker as well as the name and city of the reporter. These interviews typically are live-to-tape. This concept will work well if satellite trucks are parked outside your door.

Telephone news conferences or Web casts: Computer and phone technology now allow a public information officer to set up a toll-free telephone number that media can call at a specified time to listen to updates from response officials. Participating spokespersons need not be collocated. A local, State, or Federal press

opportunity could be conducted by phone, even if spokespersons were in many locations. In addition, such technology is interactive so that media persons can ask questions.

Commercial press release services: Services such as PR Newswire and US Newswire give organizations access to national, regional, or specialized media by using media lists and fax numbers. Many of these services are available 24 hours a day.

E-mail Listservs® and broadcast faxes: Many media are prepared to receive information from organizations through e-mail or by fax.

Web sites and video streaming: The Internet-connected public and media often go to the Web for information. Official Web sites can be a great media-response tool.

Response to media calls: The basic relationship between public information officials and the media subsists on the simple calls from media representatives requesting information or an interview. In an emergency, the way an organization responds to these calls may make a difference in the way the organization's responsiveness or professionalism is portrayed to the public. Every organization must establish a workable plan to respond to a potential surge of media calls. This aspect of working with the media is a must. Training, planning, and coordination will make the difference. Media should know ahead of time how the flow of information will work, how to get their requests answered, and what you can or cannot do. You may also want a backup plan in case your phone lines overload.



Chapter 3

Sources

Federal Public Affairs Contacts

Many different Federal organizations are involved in Homeland Security. The following list provides public affairs contact data and a brief explanation of each organization's mission in securing our Nation.

Department of Homeland Security

(202) 282-8010
www.dhs.gov
Office of Public Affairs
Washington, DC 20528

Department of Agriculture

(202) 720-4623
www.usda.gov
Deputy Director of Communications and Press Secretary
Room 402-A, Whitten Building
Washington, DC 20250-1301

Department of Commerce

(202) 482-4883
www.doc.gov
Office of Public Affairs
Room 5413
Washington, DC 20230

Department of Defense

(703) 697-5131
www.dod.mil
Office of Secretary of Defense
Office of Public Affairs
Washington, DC 20310-6605

Department of Education

(202) 401-3026
www.ed.gov
Office of Public Affairs
400 Maryland Avenue, SW
Washington, DC 20202

Department of Energy

(202) 586-4940
www.doe.gov
Office of Public Affairs
1000 Independence Avenue, SW
Washington, DC 20585

Department of Health and Human Services

(202) 690-6343
www.hhs.gov
Office of Public Affairs
200 Independence Avenue, SW
Washington, DC 20201

Department of Housing and Urban Development

(202) 708-0685
www.hud.gov
Office of Public Affairs
451 7th Street, SW
Washington, DC 20410

Department of the Interior

(202) 208-6416
www.doi.gov
Office of Public Affairs
1849 C Street, NW
Washington, DC 20240

Department of Justice

(202) 616-2777
www.us.doj.gov
Office of Public Affairs
950 Pennsylvania Avenue, NW
Washington, DC 20530-0001

Department of Labor

(202) 693-4676
www.dol.gov
Office of Public Affairs
Frances Perkins Building
200 Constitution Avenue, NW
Washington, DC 20210

Department of State

(202) 647-2492
www.state.gov
Public Communication Division
PA/PL/PC, Room 2206
Washington, DC 20520

Department of Transportation

(202) 366-4570
www.dot.gov
Office of Public Affairs
400 7th Street, SW
Washington, DC 20590

Department of the Treasury

(202) 622-2910
www.treas.gov
Office of Public Affairs
1500 Pennsylvania Avenue, NW
Washington, DC 20220

Department of Veterans Affairs

(202) 273-6000
www.va.gov
Office of Public Affairs
Washington, DC 20011

Centers for Disease Control and Prevention

(404) 639-7290
www.cdc.gov
Office of Public Affairs
1600 Clifton Road
Atlanta, GA 30333

Central Intelligence Agency

(703) 482-7778
www.cia.gov
Office of Public Affairs
Washington, DC 20505

Environmental Protection Agency

(202) 564-4355
www.epa.gov
Office of Public Affairs
Ariel Rios Building
1200 Pennsylvania Avenue, NW
Washington, DC 20460

Federal Bureau of Investigation

(202) 324-3691
www.fbi.gov
J. Edgar Hoover Building
935 Pennsylvania Avenue, NW
Washington, DC 20535-0001

Federal Communications Commission

(202) 418-0500
www.fcc.gov
Office of Public Affairs
445 12th Street, SW
Washington, DC 20554

General Services Administration

(202) 501-1231
www.gsa.gov
Office of Public Affairs
1800 F Street, NW
Washington, DC 20405

National Aeronautics and Space Administration

(202) 358-1600
www.nasa.gov
Office of Public Affairs
300 E Street, SW
Washington, DC 20546

National Nuclear Security Administration

(202) 586-7371
www.nnsa.doe.gov
Office of Public Affairs
1000 Independence Avenue, SW
Washington, DC 20585

National Transportation Safety Board

(202) 314-6100
www.nts.gov
Office of Public Affairs
490 L'Enfant Plaza, SW
Washington, DC 20594

Nuclear Regulatory Commission

(301) 415-8200
www.nrc.gov
Office of Public Affairs
Washington, DC 20555

Office of Personnel Management

(202) 606-2402
www.opm.gov
Office of Public Affairs
1900 E Street, NW
Washington, DC 20415-0001

U.S. Postal Service

(202) 268-2143
www.usps.gov
Office of Public Affairs
Room 10501
475 L'Enfant Plaza
Washington, DC 20260-3100

American Red Cross

(202) 303-5551
www.redcross.org
Office of Public Affairs
National Headquarters
2025 E Street, NW
Washington, DC 20006

State Public Affairs Contact Information

Each State and Territory has a Homeland Security Advisor appointed to be a liaison between the State and DHS. The following list provides public affairs contact information for each State or Territory.

ALABAMA

State Capitol
600 Dexter Avenue
Montgomery, AL 36130
(334) 956-7254

ALASKA

State Capitol
P.O. Box 110001
Juneau, AK 99811
(907) 465-3500

AMERICAN SAMOA

Office of the Governor
Pago Pago, AS 96799
011-684-633-4116

ARIZONA

Governor's Office
1700 W. Washington
Phoenix, AZ 85007
(602) 542-7030

ARKANSAS

State Capitol
Room 238
Little Rock, AR 72201
(501) 682-3606

CALIFORNIA

State Capitol
First Floor
Sacramento, CA 95814
(916) 445-4571

COLORADO

State Capitol
Room 127
Denver, CO 80203-1792
(303) 866-6324

CONNECTICUT

State Capitol
210 Capitol Avenue
Hartford, CT 06106
(203) 805-6600

DELAWARE

Tatnall Building
William Penn Street
Dover, DE 19901
(302) 659-3362

FLORIDA

Executive Office of the Governor
Room 206
State Capitol
Tallahassee, FL 32399-0001
(850) 488-5394

GEORGIA

State Capitol
 Room 100
 Atlanta, GA 30334
 (404) 656-1776

GUAM

Executive Chamber
 P.O. Box 2950
 Agana, GU 96932
 (671) 475-9600

HAWAII

State Capitol
 415 South Beretania Street
 Honolulu, HI 96813
 (808) 586-0034

IDAHO

State Capitol
 700 West Jefferson, 2nd Floor
 Boise, ID 83720
 (208) 334-3460

ILLINOIS

James R. Thompson Center
 100 West Randolph, Suite 16-100
 Chicago, IL 60601
 (217) 782-0244

INDIANA

206 State House
 Indianapolis, IN 46204
 (317) 232-4578

IOWA

State Capitol
 Des Moines, IA 50319
 (515) 281-3231

KANSAS

State Capitol
 Second Floor
 Topeka, KS 66612-1590
 (785) 296-3232

KENTUCKY

State Capitol
 700 Capitol Avenue
 Frankfort, KY 40601
 (502) 564-2611, ext. 322

LOUISIANA

P.O. Box 94004
 Baton Rouge, LA 70804-9004
 (225) 925-7500

MAINE

State House, Station 1
 Augusta, ME 04333
 (207) 287-3531

MARYLAND

State House
 Annapolis, MD 21401
 (410) 974-3901

MASSACHUSETTS

State House
 Room 265
 Boston, MA 02133
 (617) 776-3200, ext. 25533

MICHIGAN

P.O. Box 30013
 Lansing, MI 48909
 (517) 373-3400

MINNESOTA

State Capitol
 Room 130
 St. Paul, MN 55155
 (651) 296-0001

MISSISSIPPI

P.O. Box 139
 Jackson, MS 39205
 (601) 359-3150

MISSOURI

State Capitol
 P.O. Box 720
 Jefferson City, MO 65102
 (573) 751-1752

MONTANA

State Capitol
 Helena, MN 59620-0801
 (406) 841-3953

NEBRASKA

P.O. Box 94848
Lincoln, NE 68509-4848
(402) 471-1970

NEVADA

State Capitol
Governor's Office
101 North Carson Street
Carson City, NV 89701
(775) 684-5670

NEW HAMPSHIRE

State House
Concord, NH 03301
(603) 223-3641

NEW JERSEY

State House
Governor's Office
P.O. Box 001
Trenton, NJ 08625
(609) 292-4791

NEW MEXICO

State Capitol, Fourth Floor
Santa Fe, NM 87503
(505) 690-0210

NEW YORK

Executive Chamber
State Capitol
Albany, NY 12224
(518) 402-2227

NORTH CAROLINA

State Capitol
Raleigh, NC 27603-8001
(919) 733-2126

NORTH DAKOTA

State Capitol
600 East Boulevard Avenue
Bismarck, ND 58505-0001
(701) 328-2200

NORTHERN MARIANA ISLANDS

Capitol Hill
Saipan, MP 96950
(670) 664-2276

OHIO

77 South High Street
30th Floor
Columbus, OH 43215
(614) 466-6178

OKLAHOMA

State Capitol
Oklahoma City, OK 73105
(405) 521-2342

OREGON

State Capitol
900 Court Street, NE
Room 257
Salem, OR 97310
(503) 378-6496

PENNSYLVANIA

Main Capitol Building
Room 308
Harrisburg, PA 17120
(717) 787-2500

PUERTO RICO

La Fortaleza
San Juan, PR 00901
(787) 721-7000

RHODE ISLAND

State House
Providence, RI 02903
(401) 222-2080

SOUTH CAROLINA

P.O. Box 11829
Columbia, SC 29211
(803) 734-2100

SOUTH DAKOTA

500 East Capitol
Pierre, SD 57501
(605) 773-5706 or -3212

TENNESSEE

State Capitol
Room G-9
Nashville, TN 37243-0001
(615) 313-0662

TEXAS

P.O. Box 12428
Austin, TX 78711
(512) 463-6516

UTAH

210 State Capitol
Salt Lake City, UT 84114
(801) 554-5452

VERMONT

109 State Street
Montpelier, VT 05609
(802) 872-4095

VIRGINIA

State Capitol
Richmond, VA 23219
(804) 225-3048

VIRGIN ISLANDS

Government House
21-22 Kongens Gade
Charlotte Amalie
St. Thomas, VI 00802
(340) 774-0294

WASHINGTON

Legislative Building
Olympia, WA 98504
(253) 512-8481

WEST VIRGINIA

State Capitol
Charleston, WV 25305
(304) 558-3830

WISCONSIN

115 East
State Capitol
Madison, WI 53702
(800) 943-0003

WYOMING

State Capitol
Cheyenne, WY 82002
(307) 777-4909

Acronyms and Terms

AAR	After-Action Report	Bio	Biological
ABS	Arson and Bomb Squad	BLS	Basic Life Support
AASHTO	American Association of State Highway and Transportation Officials	BNICE	Biological, Nuclear, Incendiary, Chemical, Explosive
ACADA	Automatic Chemical Agent Detection and Alarm	BOL	Bureau of Labs
ACBIRC	Advanced Chemical/Biological Integrated Response Course	BSI	Basic Support Installation
ACF	Alternate Care Facility	BTCP	Biological Terrorism Contingency Plan
ACP	Access Control Points	BTS	Border and Transportation Safety (Directorate – DHS)
ACT	Area Command Team	BTS	Bureau of Transportation Statistics
AFB	Air Force Base	BW	Biological Warfare and/or Weapons (context-dependent)
AG	Attorney General	C/B	Chemical and Biological
ALI	Annual Limit on Intake	C/E	Communications and Electronics
ALS	Advanced Life Support	C2	Command and Control
AMF	Alternative Morgue Facility	C3	Command, Control, and Communication
AMS	Aerial Measuring System	CA	Chemical Agent
AMS	Atmospheric Monitoring System	CAM	Chemical Agent Monitor
ANG	Air National Guard	CAO	Chief Administrative Office(r)
AP	Arrival Point	CAR	Congressional Affairs Representative
AP	Associated Press	CBIRF	Chemical/Biological Incident Response Force (USMC)
APHIS	Animal and Plant Health Inspection Service	CBN	Chemical, Biological, or Nuclear
ARAC	Atmospheric Release Advisory Capability	CBP	Customs and Border Protection
ARC	American Red Cross	CBR	Chemical, Biological, Radiological
ARNG	Army National Guard	CBRDT	Chemical/Biological Rapid Deployment Team
ATF	Alcohol, Tobacco, and Firearms (Bureau)	CBRN	Chemical, Biological, Radiological, Nuclear
ATSDR	Agency for Toxic Substance and Disease Registry (USPHS)	CB-RRT	Chemical and Biological-Rapid Response Team
AUSA	Assistant U.S. Attorney	CBRT	Chemical and Biological Response Team (from TEU)
BDC	Bomb Data Center	CCMIS	Crisis Consequence Management Information System
BHS	Bureau of Health Services		

CCP	Casualty Collection Point	CMU	Crisis Management Unit
CDC	Centers for Disease Control and Prevention	CNS	Central Nervous System
CDE	Committed Dose Equivalent	CNU	Crisis Negotiations Unit (FBI)
CDR	Commander	COA	Courses of Action
CDRG	Catastrophic Disaster Response Group	COG	Continuity of Government
CDU	Contagious Disease Unit	COI	Critical Operational Issue
CEDE	Committed Effective Dose Equivalent	COMMDIR	Communications Directory
CEO	Chief Executive Officer	CONOPS	Concept of Operations
CEOC	County Emergency Operations Center	CONPLAN	Concept of Operations Plan
CGD	Coast Guard District	CONUS	Continental United States
CHS	Correctional Health Services	COOP	Continuity of Operations
CIA	Central Intelligence Agency	COP	Chief of Police
CIG	Central Information Group	COSIN	Control Staff Instructions
CIMRT	Critical Incident Management Response Team	CP	Command Post
CIMS	Critical Incident Management Support	CPX	Command Post Exercise
CIMST	Critical Incident Management Support Team	CRM	Communications Resource Manager
CINC	Commander-in-Chief	CRO	Congressional Relations Officer
CIRG	Critical Incident Response Group	CRTF	Commander, Response Task Force (DoD)
CIS	Citizenship and Immigration Service (formerly INS)	CSE	Communications Security Establishment
CISD	Critical Incident Stress Debriefing	CSG	Coordinating Subgroup
CISM	Critical Incident Stress Management	CSG	Counterterrorism Security Group
CLO	Congressional Liaison Officer	CST	Weapons of Mass Destruction Civil Support Team (National Guard)
CMC	Crisis Management Center	CT	Counterterrorism
CME	Chief Medical Examiner	CWA	Chemical Warfare Agent
CMG	Consequence Management Group	CY	Calendar Year
CMRT	Consequence Management Response Team	DAC	Disaster Assistance Center
		DALO	Disaster Area Liaison Officer
		DART	Damage Assessment Reconnaissance Team
		DART	Disaster Assessment and Recovery Team

DCA	Disaster Communication Agreement	DOJ	Department of Justice
DCE	Disaster Communications Equipment	DOL	Department of Labor
DCE	Disaster Coordinating Element	DOMS	Director of Military Support
DCE/MED TF	Disaster Coordinating Element/Medical Task Force	DOS	Department of State
DCO	Defense Coordinating Office	DOT	Department of Transportation
DCT	Donations Coordination Team	DOTreas	Department of the Treasury
DEA	Drug Enforcement Agency	DPH	Department of Public Health
DECON	Decontamination	DPMU	Disaster Portable Morgue Unit
DEI	Dose Equivalent Iodine	DPP	Domestic Preparedness Program
DEP	Department of Environment Protection	DPW	Department of Public Works
DEQ	Department of Environmental Quality	DRTF	Disaster Relief Task Force
DEST	Domestic Emergency Support Team	DSN	Defense Switch Network
DFAIT	Department of Foreign Affairs and International Trade	DSWA	Defense Special Weapons Agency
DFO	Disaster Field Office	DTG	Date Time Group
DHS	Department of Homeland Security	DTRA	Defense Threat Reduction Agency
DHS	Disaster Health Service	DTRG	DoD Technical Response Group
DIR	Director	DVA	Department of Veterans Affairs
DMAT	Disaster Medical Assistance Team	EAG	Exercise Analysis Group
DMORT	Disaster Mortuary Operational Response Team	EAR	Exercise Analysis Report
DNA	Deoxyribonucleic acid	EAS	Emergency Alert System
DOC	Department of Commerce	EBR	Endogenous Biological Regulators
DoD	Department of Defense	EBS	Emergency Broadcasting System
DoDD	Department of Defense Directive	ECC	Emergency Communications Center
DoDRDB	Department of Defense Resource Database	ECD	Effective Cumulative Dose
DOE	Department of Energy	ED	Effective Dose
DOED	Department of Education	ED	Emergency Department
DOI	Department of the Interior	EDC	Economic Development Corporation
		EDT	Eastern Daylight Time
		EDT	Explosive Device Team
		EEI	Essential Elements of Information
		EIS	Emergency Information System

EM	Emergency Management	FBI	Federal Bureau of Investigation
EMA	Emergency Management Agency	FCC	Federal Coordinating Center
EMAC	Emergency Management Assistance Compact	FCO	Federal Coordinating Office
EMS	Emergency Medical Services	FD	Fire Department
EMSHG	Emergency Management Strategic Healthcare Group	FDA	Food and Drug Administration
EMT	Emergency Medical Technician	FECC	Federal Emergency Communications Coordinators
ENDEX	End of Exercise	FEMA	Federal Emergency Management Agency
EOC	Emergency Operations Center	FHWA	Federal Highway Administration
EOD	Explosive Ordnance Disposal	FMCSA	Federal Motor Carrier Safety Administration
EOO	Emergency Operations Organization	FOIA	Freedom of Information Act
EOP	Emergency Operations Plan	FOSC	Federal On-Scene Coordinator
EPA	Environmental Protection Agency	FOUO	For Official Use Only
EPI	Emergency Public Information	FRA	Federal Railroad Administration
EPR	Emergency Preparedness and Response	FRERP	Federal Radiological Emergency Response Plan
ERAMS	Environmental Radiation Ambient Monitoring System	FRMAP	Federal Radiological Monitoring & Assessment Plan
ERT	Emergency Response Team	FRP	Federal Response Plan
ERT	Evidence Response Team	FSL	Federal, State, Local
ERT-A	Emergency Response Team – Advance Element	FTA	Federal Transit Administration
ERT-N	Emergency Response Team – National Element	FUNCPLAN	Functional Plan
ERW	Enhanced Radiation Weapon	FY	Fiscal Year
ESD	Emergency Services Director	GEOCC	Government Emergency Operations Coordination Centre
ESF	Emergency Support Function	GIS	Geographic Information Systems
ESP	Extranet Secure Portal	GSA	General Services Administration
ETA	Estimated Time of Arrival	HAN	Health Alert Network
EU	European Union	HAZMAT	Hazardous Materials
EXPLAN	Exercise Plan	HHS	Department of Health and Human Services
FAA	Federal Aviation Administration	HMRU	Hazardous Materials Response Unit (FBI)
FasT	Field Assessment Team		

HQ	Headquarters	INS	Immigration and Naturalization Service (now CIS)
HQDA	Headquarters, Department of Army	IOF	Initial Operating Facility
HRS	Hours	IPC	Initial Planning Conference
HRT	Hostage Rescue Team	IRR	Initial Response Resource
HSAS	Homeland Security Advisory System	IRT	Initial Response Team
HSCG	Homeland Security Coordination Group	ISG	Incident Support Group
HSD	Human Services Department	IST	Incident Support Team
I&W	Indications and Warnings	IT	Information Technologies
IAIP	Information Analysis and Infrastructure Protection	JAS	Joint Alternate Site
IAW	In Accordance With	JIC	Joint Information Center
IC	Incident Commander	JICG	Joint International Control Group
ICC	Incident Command Center	JOC	Joint Operations Center
ICC	Intelligence Control Center	JS	Joint Staff
ICE	Immigration & Customs Enforcement	JTF-CS	Joint Task Force – Civil Support
ICEPP	Incident Communications Emergency Policy and Procedures	JTTF	Joint Terrorism Task Force
ICP	Incident Command Post	KI	Potassium Iodide
ICPAE	Interagency Committee on Public Affairs in Emergencies	LAN	Local Area Network
ICRP	International Commission on Radiological Protection	LE/LEA	Law Enforcement/Law Enforcement Agency
ICS	Incident Command System	LEGATS	Legal Attaches
ICU	Intensive Care Unit	LFA	Lead Federal Agency
ID	Infectious Disease	LHD	Local Health Department
IDS	Information Display System	LLEA	Local Law Enforcement Agency
IDS	International District Station	LNO	Liaison Officer
IED	Improvised Explosive Device	LOC	Levels of Concern
IFC	Intelligence Fusion Cell	LRN	Laboratory Response Network
IICT	Interagency Intelligence Committee on Terrorism	MARAD	Maritime Administration
IND	Improvised Nuclear Device	MATTS	Mobile Air Transportable Telecommunications System
INRP	Initial National Response Plan	MCI	Mass Casualty Incident
		MCSAP	Motor Carrier Safety and Assistance Program
		MD	Medical Doctor

MEDEVAC	Medical Evacuation	NLT	Not Later Than
MERS	Mobile Emergency Response System	NMRS	National Medical Response System
MMRS	Metropolitan Medical Response System	NMRT	National Medical Response Team
MOA	Memorandum of Agreement	NMRT-WMD	National Medical Response Team – Weapons of Mass Destruction
MOC	Mobile Operations Center	NOAA	National Oceanographic and Atmospheric Administration
MOPP	Mission-Oriented Protective Posture	NOC	National Operations Center
MOU	Memorandum of Understanding	NPS	National Pharmaceutical Stockpile
MPC	Mid-term Planning Conference	NRAT	Nuclear Radiological Advisory Team
MR	Medical Records	NRC	National Response Center
MSCA	Military Support to Civil Authorities	NRC	Nuclear Regulatory Commission
MSD	Military Support Detachment	NRP	National Response Plan
MSDS	Material Safety Data Sheets	NSA	National Security Agency
MSEL	Master Scenario Events List	NSSE	National Special Security Event (e.g. Olympics)
MSFO	Marine Safety Field Office	NWS	National Weather Service
NASA	National Aeronautics and Space Administration	OAS	Organization of American States
NATO	North Atlantic Treaty Organization	ODP	Office for Domestic Preparedness
NBC	Nuclear, Biological, and/or Chemical	OEM	Office of Emergency Management
NCA	National Command Authority	OEMC	Office of Emergency Management and Communications
NCEH	National Center for Environmental Health	OEP	Office of Emergency Preparedness
NCR	National Capital Region	OER	Office of Emergency Response
NCS	National Communications System	OES	Office of Emergency Services
NDMS	National Disaster Medical System	OJP	Office of Justice Programs
NEST	Nuclear Emergency Search Team	ONCRC	Office of National Capital Region Coordination
NIEOC	National Interagency Emergency Operating Center	OPA	Oil Pollution Act
NGB	National Guard Bureau	OPCON	Operational Control
NHTSA	National Highway Transportation Safety Administration	OPLAN	Operations Plan
NIFC	National Interagency Fire Center	OPORD	Operations Order
NIH	National Institutes of Health	OPS	Operations
		OPSEC	Operational Security

OSC	On-Scene Commander	RECS	Radiological Emergency Communications System
OSC	On-Scene Coordinator		
OSD(PA)	Office of the Secretary of Defense (Public Affairs)	REM	Roentgen Equivalent Man
		REOC	Regional Emergency Operations Center
OSHA	Occupational Safety and Health Administration	RETCO	Regional Emergency Transportation Coordinator
PA	Public Affairs		
PA	Public Announcement	RETREP	Regional Emergency Transportation Representative
PAHO	Pan American Health Organization		
PAO	Public Affairs Officer	RFI	Request For Information
PCC	Policy Coordinating Committee	RL	Recording Level
PCO	Privy Council Office	ROC	Regional Operations Center
PCR	Polymerase Chain Reaction	RRT	Regional Response Team
PD	Police Department	S-60	DOT Office of Intelligence Security
PDD	Presidential Decision Directive	SABA	Supplied Air Breathing Apparatus
PDF	Portable Document Format	SABT	Special Agent Bomb Technician
PIO	Public Information Officer	SAC	Special Agent-in-Charge (FBI)
POC	Point of Contact	SBA	Small Business Administration
POD	Point of Distribution	SCADA	Supervisory Control and Data Acquisition System
POMSO	Plans, Operations, and Military Support Officer	SCC	Secretary's Command Center
		S/CT	Office of the Coordinator for Counterterrorism
PPE	Personal Protective Equipment		
PSN	Public Switched Network	SEMA	State Emergency Management Agency
PT&E	Preparedness, Training, and Exercises	SEMO	State Emergency Management Office
PW	Public Works		
Rad	Radiological	SEOC	State Emergency Operations Center
RAD	Radiation Absorbed Dose	SERT	Secretary's Emergency Response Team
RAP	Radiological Assistance Plan		
RC	Reserve Component	SG	Solicitor General
RDD	Radiological Dispersal Device	SIMCELL	Simulation Cell
RDECOM	U.S. Army Research, Development and Engineering Command	SIOC	Strategic Information Operations Center
		SITREP	Situation Report
REAC/TS	Radiation Emergency Assistance Center/Training Site	SME	Subject Matter Expert

SMU	Special Mission Unit	USCG	U.S. Coast Guard
SNS	Strategic National Stockpile	USCS	U.S. Customs Service
SOPs	Standard Operating Procedures	USDA	U.S. Department of Agriculture
TBD	To Be Determined	USFS	U.S. Forest Service
TBP	To Be Published	USG	U.S. Government
TEU	Technical Escort Unit	USJFCOM	U.S. Joint Forces Command
TEW	Terrorist Early Warning (Group)	USMC	U.S. Marine Corps
TLD	Thermoluminescent Dosimeter	USNORTHCOM	U.S. Northern Command
TOC	Tactical Operations Centers	USPHS	U.S. Public Health Service
TOPOFF	Top Officials	USPS	U.S. Postal Service
TSA	Transportation Security Administration	VA	Veterans Administration
TSWG	Technical Support Working Group	VCC	Venue Control Cell
TTF	Terrorism Task Force	VHA	Veterans Hospital Administration
TTX	Tabletop Exercise	VIP	Very Important Person
TWG	Terrorism Working Group	VTC	Video Teleconferencing
UN	United Nations	WAN	Wide Area Network
URI	Upper Respiratory Infection	WBC	White Blood Count
US&R	Urban Search and Rescue	WHO	World Health Organization
USAR	United States Army Reserve	WHSR	White House Situation Room
USAMRICD	U.S. Army Medical Research Institute of Chemical Defense	WMA	Washington Metropolitan Area
USAMRIID	U.S. Army Medical Research Institute of Infectious Diseases	WMD	Weapon(s) of Mass Destruction
		WTO	World Trade Organization
		ZULU	Indicates use of Universal Coordinated Time (UCT)

Other References



Communicating in a Crisis: Risk Communications Guidelines for Public Officials, published by the Department of Health and Human Services in 2002, is an excellent risk communication resource with an extensive list of suggested reading. It is available online at www.mentalhealth.org, and printed copies can be obtained free of charge from the Substance Abuse and Mental Health Services Administration at (800) 789-2647. Reference document number SMA 02-3641.



Crisis Communications Handbook, published by Jane's Information Group in 2003, addresses a range of incidents and the differing internal and external communications responses. Copies start at \$24.00 and can be ordered online at http://catalog.janes.com/catalog/public/index.cfm?fuseaction=home.ProductInfoBrief&product_id=187 or by calling (703) 683-3700.



Crisis and Emergency Risk Communication, published by the Centers for Disease Control and Prevention in 2002, is a book that accompanied courses taught to State and local health officials by the CDC in 2002 and 2003. In addition, an interactive CD-ROM, Emergency Risk Communication (ERC) CDCynergy, provides many tools and worksheets that can be used for planning for and responding to terrorism and other health emergencies both within and outside of public health. Many tools in Appendix A of this guide are based on ERC CDCynergy materials. The set can be ordered from the Public Health Foundation for \$39.50 at www.phf.org. ERC CDCynergy may also be accessed online at <http://www.orau.gov/cdcynergy/erc/default.htm>.

Appendix A

Tools and Templates

Incident Situation Summary

Date and time: _____

Location: _____

Nature of incident: _____

Estimated number of victims: _____

Potential or critical infrastructure involved: _____

Evacuation status: _____

Response status: _____

Protective measures initiated: _____

Lead agency: _____

Incident Verification

It is important to verify the initial reports of an incident and to make sure that you have correct information. Verified information is a critical factor in making appropriate decisions regarding the incident.

Have all the facts been received? (to the best of your knowledge?) Yes/No

Did the information collected come from formal, credible sources such as a local, State, or Federal agency? Yes/No

Do you have similar reports about the incident from more than one source? Yes/No

Is the information from different sources consistent? Yes/No

Is the characterization of the event plausible? Yes/No

If necessary, was information clarified through subject matter experts? Yes/No

If you can answer “yes” to these key checkpoints, you have completed the key steps to verifying the situation.

Note: Verification is not a function for just one person. It requires input from a variety of sources.

Message Development for Emergency Communication

Step 1: Consider the following general factors

1. Target audience(s) (e.g., general public, health providers): _____

2. Purpose of messages (e.g., give facts/update, respond to media): _____

3. Method of delivery (e.g., TV interview, press release): _____

Step 2: Consider the six basic emergency message components

1. Expression of empathy: _____

2. Clarifying facts
Who: _____
What: _____
Where: _____
When: _____
Why: _____
How: _____
3. What we don't know: _____
4. Process to get answers: _____
5. Statement of commitment: _____
6. Referrals (for more information): _____
7. Next scheduled update: _____

Step 3: Decide what are the three most important message topics for you to cover

1. _____
2. _____
3. _____

Step 4: Develop a complete key message for each of your three message topics

TOPIC 1: _____

Complete message _____

Additional supporting facts (if any) _____

Soundbite _____

TOPIC 2: _____

Complete message _____

Additional supporting facts (if any) _____

Soundbite _____

TOPIC 3: _____

Complete message _____

Additional supporting facts (if any) _____

Soundbite _____

Step 5: Check your messages for the following and revise, if needed

- | | | |
|--|--|--|
| <input type="checkbox"/> Positive action steps | <input type="checkbox"/> Test for clarity | <input type="checkbox"/> Avoid humor |
| <input type="checkbox"/> Honest/open tone | <input type="checkbox"/> Use simple words, short sentences | <input type="checkbox"/> Avoid extreme speculation |
| <input type="checkbox"/> Applied risk communication principles | <input type="checkbox"/> Avoid jargon | <input type="checkbox"/> Avoid judgmental phrases |

JIC Equipment and Supplies Checklist

Equipment	Location	How to Obtain It
<input type="checkbox"/> Fax machine (preprogrammed for broadcast fax releases to media and partners)		
<input type="checkbox"/> Computers (on LAN with e-mail Listservs® designated for partners and media)		
<input type="checkbox"/> Laptop computers		
<input type="checkbox"/> Printers for every computer		
<input type="checkbox"/> Copier (and backup)		
<input type="checkbox"/> Several tables		
<input type="checkbox"/> Cell phones/pagers/personal data devices and e-mail readers		
<input type="checkbox"/> Visible calendars, flow charts, bulletin boards, easels		
<input type="checkbox"/> Designated personal message board		
<input type="checkbox"/> Small refrigerator		
<input type="checkbox"/> Paper		
<input type="checkbox"/> Color copier		
<input type="checkbox"/> A/V equipment		
<input type="checkbox"/> Portable microphones		
<input type="checkbox"/> Podium		
<input type="checkbox"/> TVs with cable hookup		
<input type="checkbox"/> VHS VCR		
<input type="checkbox"/> CD-ROM		
<input type="checkbox"/> Paper shredder		
<input type="checkbox"/> Copier toner		
<input type="checkbox"/> Printer ink		
<input type="checkbox"/> Paper		
<input type="checkbox"/> Pens		
<input type="checkbox"/> Markers		
<input type="checkbox"/> Highlighters		
<input type="checkbox"/> Erasable markers		
<input type="checkbox"/> FedEx and mail supplies		
<input type="checkbox"/> Sticky notes		
<input type="checkbox"/> Tape		

Equipment	Location	How to Obtain It
<input type="checkbox"/> Notebooks		
<input type="checkbox"/> Poster board		
<input type="checkbox"/> Standard press kit folders		
<input type="checkbox"/> Organized B-roll beta format (keep VHS copies around for meetings)		
<input type="checkbox"/> Formatted computer disks		
<input type="checkbox"/> Color-coded everything (folders, inks, etc.)		
<input type="checkbox"/> Baskets (to contain items not ready to be thrown away)		
<input type="checkbox"/> Organizers to support your clearance and release system		
<input type="checkbox"/> Expandable folders (indexed by alphabet or days of the month)		
<input type="checkbox"/> Staplers (several)		
<input type="checkbox"/> Paper punch		
<input type="checkbox"/> Three-ring binders		
<input type="checkbox"/> Organization's press kit or its logo on a sticker		
<input type="checkbox"/> Colored copier paper (for door-to-door flyers)		
<input type="checkbox"/> Paper clips (all sizes)		



Personal emergency kit checklists: www.ready.gov

Template for Prescribed, Immediate Response to Media Inquiries

Use this template if the media is “at your door” and you need time to assemble the facts for the initial press release statement. Getting the facts is a priority. It is important that your organization not give in to pressure to confirm or release information before you have confirmation from your scientists, emergency operations center, etc. The following are responses which give you the necessary time to collect the facts. Use the Template for Press Statement for providing an initial press release statement after the facts are gathered.

NOTE: Be sure you are first authorized to give out the following information.

Date: _____ Time: _____

Approved by: _____

Prescribed Responses

If on phone to media:

- We’ve just learned about the situation and are trying to get more complete information now. How can I reach you when I have more information?
- All our efforts are directed at bringing the situation under control, so I’m not going to speculate about the cause of the incident. How can I reach you when I have more information?
- I’m not the authority on this subject. Let me have (name) call you right back.
- We’re preparing a statement on that now. Can I fax it to you when it’s ready?
- You may check our Web site for background information, and I will fax/e-mail you with the time of our next update.

If in person at incident site or in front of press meeting:

- This is an evolving emergency and I know that, just like we do, you want as much information as possible right now. While we work to get your questions answered as quickly as possible, I want to tell you what we can confirm right now:
 - At approximately (time), a (brief description of what happened).
 - At this point, we do not know the number of (persons ill, persons exposed, injuries, deaths, etc.).
 - We have a (system, plan, procedure, operation) in place for just such an emergency and we are being assisted by (police, FBI, DHS) as part of that plan.
 - The situation is (under) (not yet under) control and we are working with (local, State, Federal) authorities to (contain this situation, determine how this happened, determine what actions may be needed by individuals and the community to prevent this from happening again).
 - We will continue to gather information and release it to you as soon as possible. I will be back to you within (amount of time, 2 hours or less) to give you an update. As soon as we have more confirmed information, it will be provided.
 - We ask for your patience as we respond to this emergency.

Notes: Depending on the incident, immediate protective measures may need to be provided.
Consider using an expression of empathy, if appropriate.

Template for Press Statement

If the media is “at your door” and you need time to assemble the facts for this initial press release statement, use the Template for Prescribed, Immediate Response to Media Inquiries. Getting the facts is a priority. It is important that your organization not give in to pressure to confirm or release information before you have confirmation from your scientists, emergency operations center, etc.

The purpose of this initial press statement is to answer the basic questions: who, what, where, when. This statement should also provide whatever guidance is possible at this point, express the association and administration’s concern, and detail how further information will be disseminated. If possible, the statement should give phone numbers or contacts for more information or assistance. Please remember that this template is meant only to provide you with guidance. One template will not work for every situation.

FOR IMMEDIATE RELEASE

CONTACT: (name of contact)

PHONE: (number of contact)

Date of release: (date)

Headline—Insert your primary message to the public

Dateline (your location)—Describe the current situation in two or three sentences.

Insert a quote from an official spokesperson demonstrating leadership and concern for victims.

“

”

Insert actions being taken.

List actions that will be taken.

List information on possible reactions of the public and ways citizens can help.

Insert a quote from an official spokesperson providing reassurance.

“

”

List contact information, ways to get more information, and other resources.

Public Information Emergency Response Call Tracking

Time of call: _____ a.m./p.m.

Nature of call:

Specific information contained in stock materials:

- Clarify recommendations
- Current status of the incident
- Hot topic 1 _____
- Hot topic 2 _____

Request for referral:

- For more information
- For medical attention
- Other _____

Feedback to agency:

- Complaint about specific contact with agency
 - Complaint about recommended actions
 - Concern about ability to carry out recommended action
 - Report additional information on incident
 - Rumor or misinformation verification (briefly describe)
-

Outcome of call:

- Reassured caller based on scripted information

Referred caller to:

- Expert outside the department
 - Personal doctor or healthcare professional (if health related)
 - Red Cross or other nongovernment organization
 - FEMA or State emergency management agency
 - Other _____
-

Action needed:

- None
- Return call to: Caller's name: _____ Telephone number: _____
Gender: M / F

Return call urgency:

- Critical (respond immediately)
 - Urgent (respond within 24 hours)
 - Routine
-

Call taken by: _____ **Date:** _____



Appendix B

My Plans and Resources

