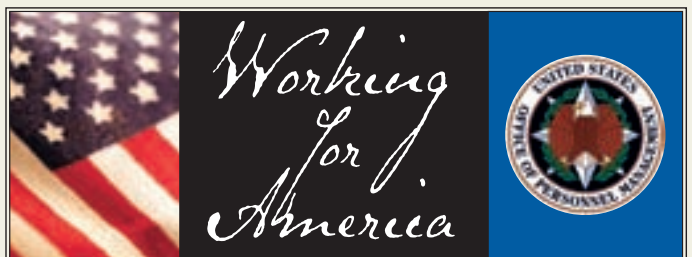
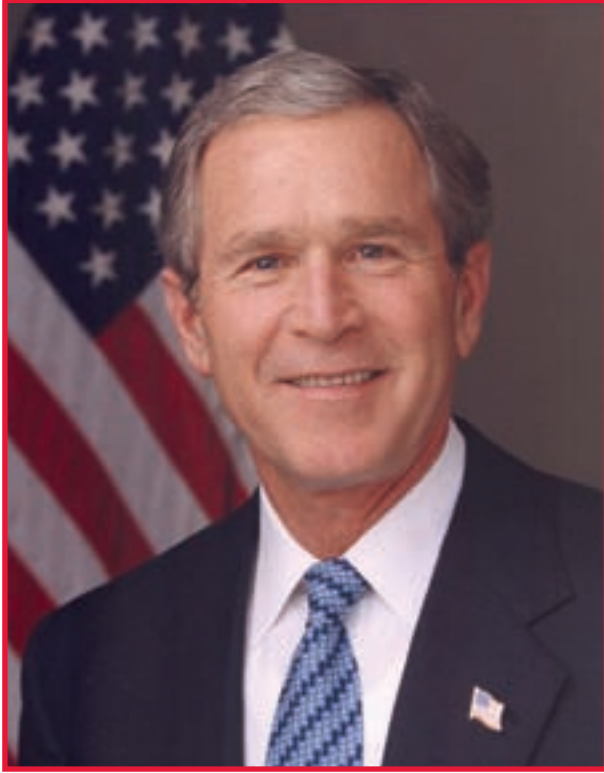




FEDERAL MANAGER'S/ DECISION MAKER'S EMERGENCY GUIDE

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT





In our time, America has been attacked. America has been challenged. Yet the uncertainty, and sorrow, and sacrifice of these years have not been in vain. Millions have gained their liberty; and millions more have gained the hope of liberty that will not be denied. The trumpet of freedom has been sounded, and that trumpet never calls retreat.

Before history is written in books, it is written in courage—the courage of honorable soldiers; the courage of oppressed peoples; the courage of free nations in difficult tasks. Our generation is fortunate to live in a time of courage. And we are proud to serve in freedom’s cause.

—President George W. Bush





THE ROLE OF THE FEDERAL GOVERNMENT TO PROTECT CIVILIAN EMPLOYEES

The Federal Emergency Dismissal Protocol calls for the General Services Administration (GSA), the Federal Emergency Management Agency (FEMA—now an agency within the Department of Homeland Security) and the Office of Personnel Management (OPM) to consult and decide on the operating status of the Federal Government and Federal buildings during an emergency. These agencies have on-going access to critical information provided by other offices within the Department of Homeland Security (DHS), law enforcement and other related agencies that inform respective decision making. Your agency is a part of the network that would immediately receive confirmed reports on any situations.

There are a variety of means in which this will be done, including the Washington Area Warning System (WAWAS), which has outlets in a large and growing number of Federal agencies.*

The Regional Incident Communication Coordination System links key agencies, Government officials and first responders in the D.C. region. Alert messages are sent out electronically to pagers, blackberries, personal digital assistants and computers, and cell phones that can accept text.

In a natural or man-made event (such as a terror incident), FEMA, GSA, and OPM will convene the principals for a review of the situation and make decisions for each of their respective areas of responsibility.

Your agency's access to confirmed reports in the event of an emergency will help provide your management with guidance appropriate to secure the safety of the building.

Immediate notification of changes to the operating status of the Federal Government will be relayed to key Federal and local authorities. Following this notification, the news media, the Federal Executive Board and other outlets across the National Capital Region and the Nation will be alerted to any change in operational status.

The operating status of the Federal Government is always available on the web site of the Office of Personnel Management — www.opm.gov.

*For more information on how to obtain a WAWAS instrument contact FEMA.

REQUIREMENTS FOR INDIVIDUAL AGENCIES

Agency Occupant Emergency Plans (OEP)

Federal agencies that operate in buildings managed by the U.S. General Services Administration are required to establish an Occupant Emergency Plan (OEP). The OEP is a short-term emergency response program that establishes procedures for safeguarding lives and property. An Occupant Emergency Program Guide to assist in the development an OEP is available at www.gsa.gov

Each Federal building has unique factors that may affect the security measures that should be taken to protect employees. Some of those factors are the location of the building, proximity to other prominent landmarks or buildings, building design features, and the mission of the agencies housed within. For this reason, it is inadvisable to make one Government-wide protocol which all agencies must follow. Instead, security measures and evacuation procedures must be tailored to meet the unique features of each facility.

The primary basis by which security measures are determined is through a facility threat assessment. As a part of its routine efforts, the Federal Protective Service (FPS) conducts recurring threat assessments for GSA-controlled property.* Federal agencies in buildings not managed by GSA should contact the FBI or local police for emergency preparedness and or threat assessments.

Employees should be encouraged to familiarize themselves with the procedures that have been put into place at their agency, as well as the means of notification that an agency will use to inform and instruct employees.

As part of every agency's OEP, employee volunteers

are used to assist in the effective evacuation and other duties during an emergency. During evacuation drills, employees should make a mental note of identifying garments (arm bands, caps, etc.) worn by floor team leaders, monitors and other volunteers. In the event of an actual emergency, it will be reassuring to know the individuals who are in place to assist with the evacuation.

Meeting Special Needs

It is the responsibility of each agency to provide a safe working environment for all employees, including those employees with special needs. Managers who oversee individuals with special needs should be proactive to ensure they have the same level of protection as all other employees. Within every agency's Occupant Emergency Plan (OEP), should be a component which addresses the concerns of employees who may need assistance during an emergency. Managers should be aware of these procedures and conscientious in communicating this information to employees with special needs. Further, managers should be proactive in asking employees with special needs about the questions and concerns these people may have about emergency procedures.

One practical step every manager should take to protect individuals with disabilities is to establish a "buddy" system for disabled employees. The buddy system should be fully integrated into the agency OEP. Information on setting up a buddy system can be found at <http://www.usfa.fema.gov/downloads/pdf/publications/fa-154.pdf>. For additional information on meeting the needs of disabled employees, contact the National Organization of the Disabled (www.nod.org).

* Federal Protective Service contact phone numbers for all states can be found at www.gsa.gov

REQUIREMENTS FOR INDIVIDUAL AGENCIES

Guidance on Telework or Other Flexibilities

Agencies must have plans in place that allow the business of government to continue during emergency situations. Designated Continuity of Operations (COOP) facilities may not have all the staff needed to support important missions and cannot accommodate enough key staff to facilitate maximum government operations. Not all key staff may be designated to report to COOP sites. Telework is a virtual resource solution and provides access to resources that may not be available otherwise.

Telework supports agency leadership in accomplishing the mission. Recent OPM guidance on emergency planning has emphasized the role of telework. Agencies have the flexibility to use teleworkers in emergency situations but it won't happen spontaneously. A viable on-going telework program is the foundation that must be in place. With 21st century technology, agencies can conduct agency financial and other transactions with appropriate security and authentication mechanisms away from Federal buildings. With the appropriate remote administration of essential support systems e.g., the provision of help-desk support, teleworkers can help ensure the continuity of business operations.

To facilitate the use of telework during emergencies, certain steps are necessary. Agencies must:

- Develop a cadre of regularly scheduled “core” teleworkers.
- Permit teleworkers to experience working off-site and learn to communicate electronically with colleagues and clients by doing it regularly.
- Permit supervisors and managers to experience managing employees without face to face contact.

With telework in place during emergencies, experienced teleworkers won't need to master new computer programs, and managers will learn to supervise a “virtual workforce” by doing it under normal conditions.

To make telework a viable option during emergencies, agency work must be organized to facilitate electronic communication and eliminate paper-based processes

whenever possible, e.g., automating reports and procedures as much as possible. Employees need to experience functioning in a “virtual office,” and they need to be linked via computer and telephone from home or alternative work sites. Managers need to be comfortable supervising people they don't see regularly.

Agency policy should be reviewed for clear distinctions between core and situational telework. Telework agreements can be tailored to the two categories:

- Core telework—regular and recurring at least 1 day a week.
- Situational telework—occasional and non-routine.

Situational status can sell telework to hesitant managers and employees. Several options can help encourage reluctant managers to use telework in their planning and preparation for emergencies:

- Formalizing situational telework arrangements,
- Setting a specific length of time for the trial period,
- Moving to core telework if both parties like the arrangement; it's a no-risk, everybody-wins approach.
- Building emergency response contingencies into employees' telework agreements,
- Including agency telework coordinators in disaster planning and exercises,
- Helping agency decision makers understand that telework is an important agency tool, not just a “nice to have” flexibility for employees

Designation of Emergency Personnel

Agencies should designate **emergency employees** who are critical to agency operations in dismissal or closure situations. Each agency head has the discretion to identify and designate those employees who he or she judges to be necessary to continue agency operations in any given emergency situation. There are no standard definitions or categories in this regard, and agency heads (or their designees, as applicable) are free to make such determinations based on the agency's unique mission requirements and/or circumstances. The designation of emergency employees may vary according to the particular nature

of an exigency. Such designations should be part of an agency's emergency response/continuity of operations plans and should be communicated (preferably well in advance) to emergency employees, so that they can be prepared to support and sustain agency operations in an emergency.

In addition, agencies may wish to identify a cadre of “**mission-critical**” emergency employees who are expected to remain in contact with their agencies at all times during any closure situation and may be called to work during emergencies dealing with national security, extended emergencies, or other unique situations. Agencies must identify the emergency situations in which “mission-critical” emergency employees will be expected to report for work and whether such employees must report for work at their regular worksites or alternative worksites.

Shelter in Place Protocols

It is possible that some types of emergency events may make evacuation of a Federal building dangerous. In this situation, an agency may decide to Shelter-In-Place (SIP). SIP is a protective action taken where a facility's occupants take refuge inside an area of the building with no or few windows. In general, a facility will SIP when one of the following emergencies occurs outside the building: severe weather (tornado, hail, etc.), civil unrest, gunman/sniper, or a biological, chemical or radiological threat.

Management will decide whether to SIP Up (proceed to a higher level), SIP Down (proceed to a lower level), or SIP In (proceed to an interior area) within the facility after conducting a threat analysis of the situation based on the type of threat and its location. During a SIP event, occupants should pay close attention to announcements made on the facility's public address system.

The U.S. General Services Administration (<http://www.gsa.gov>) provides guidance for agencies to setup an Occupant Emergency Plan (OEP), which would include SIP procedures. Once developed, the OEP should periodically be exercised to maintain training proficiency and to identify adjustments to the plan. The most important thing is to know beforehand what to do if advised to SIP.

For additional information on SIP, contact:

American Red Cross

<http://www.redcross.org/services/disaster/beprepared/shelterinplace.html>

Department of Health and Human Services, Centers for Disease Control and Prevention

<http://www.bt.cdc.gov/planning/shelteringfacts.asp>

U.S. Department of Homeland Security

http://www.ready.gov/stay_or_go.html#stay



YOUR ROLE AS MANAGER

There have been several reports in the media about potential chemical or biological attacks against civilians. It is natural for us to fear the unknown.

As a manager, employees will look to you for support in a time of emergency. It is important that you understand the plan your agency has in place to respond to terrorist events. In addition, you should ensure that your employees have a clear understanding of what they are to do in an emergency. You should rehearse your plan repeatedly with your employees.

The following pages provide guidance on actions that you can take prior to, during, and following an attack that involves chemical or biological weapons. This is a general guide to help you begin to prepare. Each agency should have an emergency plan that provides contingencies for what you should do during an attack.

Senior managers may want to contact the Federal Protective Service at the Department of Homeland Security to have them survey your building and recommend safety and security procedures to ensure that you are doing everything possible to protect your employees.

As a manager, you must maintain open lines of communications with employees on measures your agency has implemented to protect them. Your employees will have questions—be sure you are available to fully discuss their concerns about their safety or suggestions they may have to improve security.

Questions to Ask about Your Preparedness

- Have you read your agency's Occupant Emergency Plan (OEP)?
- In the event of an emergency evacuation, are you (or is someone in your office) able to account for all employees?
- If employee volunteers (hall monitors, etc.) are not at work, are others available to take their places in the event of an emergency?
- Do you have a protocol to shelter-in-place? Do you have supplies available if the decision is made to shelter-in-place?
- How recently have you conducted drills on evacuation and shelter-in-place contingencies?
- Decision Maker: What is the protocol for shutting down the ventilation system in the event that the external air is contaminated or threatened? Do your security professionals have to wait until you make the decision, or do they have authority to immediately protect your employees?

DEALING WITH THE THREAT OF TERRORISM OR INCIDENTS PRIOR TO AN ATTACK

1. **Educate your employees.** Conduct periodic “all-hands” meetings to keep employees educated. You know what steps you have taken to protect employees but they may not. By communicating your proactive measures, you will help to reduce the stress that your employees may feel.

Be sure to educate your employees about the availability of Employee Assistance Programs (EAP) within your agency. These programs provide important resources, such as counseling, to help your employees and their families.

2. **Communicate internally.** Keep your employees informed with accurate information regarding potential threats and how they could be affected. There are numerous military personnel or first responders around each community that can provide informative briefings to your employees to educate them on chemical and biological agents and potential effects.

Ensure that employees are familiar with the procedures in the individual and family preparedness guides. Further, they should understand your agency policy for reporting bomb threats, fire evacuations, and other emergency procedures in accordance with your local emergency preparedness plan. Practice these procedures ahead of time.

Keep in mind that drills are a very good opportunity to educate your employees. When employees, for instance, have evacuated a building during a fire drill, they are more likely to be focused on security than if you simply stop by their office and talk about safety procedures. While employees are in the middle of a drill, spend some time to explain what went right and what went wrong. Explain what they would need to remember if it were a real emergency.

3. **Be aware.** Encourage your employees to be on the lookout for and to report any suspicious activity. Observations and awareness of the surroundings

could prevent incidents from occurring and/or give responders valuable information if an event does occur.

4. **Provide opportunities** for employees to get necessary medical preparation (prescriptions, doctor’s letters, medical alert tags, and up-to-date immunizations) that could be vital. While there is no set cure all for these types of infections, good health preparation will aid the body’s natural defenses.
5. **Prepare.** Prepare necessary supplies in the event that you will have to “shelter-in-place” for a short time (officials expect this time would not exceed a few hours due to the availability of trained local responders and emergency services).

While each threat is different, you should look at your individual situation and determine what your employees may need in the event they are unable to immediately evacuate the area. Things you should consider are bottled water, food in sealed containers, a personal bag containing medication or other items that may be needed by individual personnel, battery operated radios in the event of power loss, and a first aid kit. Maintain a list of emergency contact numbers for your section.

6. **Take care of personal matters.** Encourage your employees to take care of personal and legal requirements (wills, powers of attorney, insurance policies). People deserve the peace of mind of knowing that their family and loved ones will be taken care of in the unlikely event they are harmed during an attack.
7. **Educate yourself.** The use of Personal Protective Equipment (PPE), such as escape hoods, has been implemented by some agencies as part of a comprehensive plan. Factors such as building location and design, and the specific mission of the agency, significantly affect the decision to purchase PPE. You should check with your



local security office to determine if such a requirement exists for your employees.

The threat of a chemical or biological attack outside a building can also be determined in part by the effectiveness of such agents in your area. Weather, wind speed, and temperature gradients all affect the use of such weapons. Agencies located in climates not conducive to the use of these agents can make their use impractical or less likely.

NOTE TO DECISION MAKERS: The decision to purchase PPE, such as escape hoods, should be driven by the Occupant Emergency Plan. You will need to address the health limitations of some employees who may not be able to wear this equipment. Additionally, there are training and retraining requirements for some PPE, to ensure the equipment is being used correctly. You will need to assess whether the real risk posed by a chemical or biological attack justifies the expenditure. It may be that the resources expended could be better used to prevent or mitigate the damage of more likely scenarios.

8. **Communicate with employee representatives** and employee groups. Senior managers should meet with the presidents and representatives of local unions and other employee groups. It is important they know what you are doing to protect employees and to listen to their concerns. It is crucial that you maintain two-way communication.
9. **Express your appreciation.** Senior managers should meet with employees who have volunteered to be “floor managers,” “safety monitors” or to carry out other duties during an emergency. These employees are truly heroes-in-waiting. You haven’t heard about them on the news because they have not been in an emergency situation. But they have volunteered to sacrifice their safety for the service and protection of their fellow employees. They need to hear from you that you believe what they are doing is noble.

DEALING WITH THE THREAT OF TERRORISM DURING AN ATTACK

1. Follow your local emergency operations procedures. Keep your employees informed as to what is going on. Use battery-operated radios or televisions, if necessary, to let your personnel know what the threat is and what is being done to ensure their safety.
2. Take control of the situation. It is natural to be fearful but it is important to be decisive. By staying calm you will help defuse panic. Have your employees follow the emergency procedures you have developed and rehearsed. This will help them feel a sense of safety especially if the procedures are well known to them. Account for your personnel as quickly as possible, and keep them together.
3. Lead. If your agency and first responders in your area have determined that employees should shelter-in-place, lead your employees to a designated shelter.
4. Monitor employee reaction. Watch for personnel who are having trouble following instructions or dealing with the situation. It can be helpful to pair them up with another employee with whom they feel comfortable. This will provide them a sense of familiarity and allow you freedom to manage the situation. Assist those who may be injured.
5. Modify rules that hinder progress. Agency rules and regulations are for normal operations and may not fit into your emergency event. Use common sense in determining which rules will apply and which add to the turmoil. Rules dealing with employees leaving work or using certain entrances and exits may not be appropriate. Be sure to follow your agency's guidelines on the scene.





DEALING WITH THE REPERCUSSIONS OF A TERRORIST ATTACK

1. Follow the directions of your local emergency responders. Ensure that all of your employees are accounted for and have been evacuated from the threat.
2. Determine what follow-on activities are required by your agency. Determine the operational status of the Federal Government for succeeding days (closings, shut downs) for your employees.
3. Keep in touch with your employees. Provide information and assistance to complete necessary reports and forms for leave, medical assistance, or emergency relief. Employee assistance programs (EAP) provide important avenues for counseling services and other means of assistance for employees and their families. Remind your team of EAP availability.
4. Be available for follow up with families. If employees have been injured, killed, or are missing, ensure that their families have been referred to the proper organizations for assistance. Follow your agency guidelines for dealing with death and grief.

While dealing with these types of tragedies is difficult, your presence and demeanor can go a long way in assisting employees through the situation. Let them know you are concerned, and do your best to manage the situation using available resources and emergency services. No one expects you to be a hero...only to help.

ADDITIONAL RESOURCES

The following publications are excellent resources for employees and managers to study to gain a more in-depth understanding about the potential risks and steps that can be taken to mitigate the damage from an attack.

- Are You Ready? A Guide for Citizen Preparedness (www.fema.gov/areyouready)
Federal Emergency Management Agency
- Occupant Emergency Program Guide (www.gsa.gov/attachments/GSA_PUBLICATIONS/extpub/GSA_OEP_Guide_6.doc)
General Services Administration
- Preparing Makes Sense. Get Ready Now (www.ready.gov/readygov_brochurev2.pdf)
Department of Homeland Security
- Evacuation Planning Matrix (www.atlintl.com/evacmtx/)—Contact OSHA for username/password.
Occupational Safety and Health Administration
- Guidance for Protecting Building Environments from Airborne Chemical, Biological, or Radiological Attacks (www.cdc.gov/niosh/bldvent/2002-139.html)
National Institute for Occupational Safety and Health
- Concept for CBRN Air-Purifying Escape Respirator Standard (www.cdc.gov/niosh/npptl/aperconoct15.html)
National Institute for Occupational Safety and Health
- Manager's Handbook on Handling Traumatic Events (www.opm.gov/emergency/)
Office of Personnel Management
- A Federal Employee's Emergency Guide (www.opm.gov/emergency/)
Office of Personnel Management

ACKNOWLEDGMENTS

Les Boord
National Institute for Occupational Safety
and Health

Lester Bush, MD
Central Intelligence Agency

Mike Byrne
Department of Homeland Security

Libby Camp
Department of Homeland Security

Duncan Campbell
Department of Homeland Security

Lucy Clark
Department of Homeland Security

Scott Deitchman, MD, MPH
National Institute for Occupational Safety
and Health

Eldon Girdner
Office of Personnel Management

Captain Elliott Grollman
Federal Protective Service

Jerome Hauer, MD
Health and Human Services

John Henshaw
Department of Labor

Paul Holbert
Office of Personnel Management

David Ippolito
Occupational Safety and Health Administration

Peter Laporte
City of Washington, D.C.

Bruce Lawlor
Department of Homeland Security

Laura Lawlor
Health and Human Services

Mike Lowder
Federal Emergency Management Agency

Rich Metzler
National Institute for Occupational Safety
and Health

Ruth McCully
Occupational Safety and Health Administration

Brian Montgomery
White House

Jim Rice
Federal Bureau of Investigation

Greg Rize
U.S. Secret Service

Ali Tulbah
White House

Mayor Anthony Williams
Washington, DC

Michael R. Zanotti, CEM, CBCP, NREMT-P
U.S. General Services Administration

OTHER AGENCIES

Department of Homeland Security
Department of State
Department of Justice
Centers for Disease Control
Homeland Security Council
National Institutes of Health



UNITED STATES OFFICE OF
PERSONNEL MANAGEMENT
1900 E Street, NW
Washington, DC 20415
202-606-1000
www.opm.gov