# GETTING READY

## Company Primer on Preparedness and Response Planning for Terrorist and Bioterrorist Attacks


**Business Executives for National Security**

# Company Primer

# on

# Preparedness and Response Planning

# for

# Terrorist and Bioterrorist Attacks


**Prepared by**
**Business Executives for National Security**
**Metro Atlanta Region**
**Homeland Security Advisory Group**

## BENS Metro Atlanta Homeland Security Advisory Group

The Homeland Security Advisory Group (HSAG) is one of several working groups of the BENS Metro Atlanta region. The region has more than 100 members. The following HSAG members were key to the production of this booklet:

**William F. Brumund, Ph.D, P.E.**
*Principal, Golder Associates*
*Chairman of the HSAG; phone: (770) 496-1893*

**David A. Lee**
*Managing Director, Ridge Consulting, LLC; phone: (770) 399-0658*

**Jeffrey P. Colbath**
*First Vice President, Investments, Smith Barney*

**Shawn D. Smith**
*President and CEO, Emergency Visions, LLC*

Special thanks are due Dr. Scott F. Wetterhall, Director, Health Assessment and Promotion, DeKalb County Board of Health, Georgia, for his support and contribution in describing the bioterrorist threat and the governmental emergency response system.

### BENS Metro Atlanta Regional Executive Committee

As described on page three, BENS and its Metro Atlanta members are focused on helping strengthen our national and homeland security structures and processes. Guiding this important work in Atlanta and the Southeast is the Regional Executive Committee:

**Bernard Marcus**
*Chairman Emeritus, The Home Depot, Region Chair*

**James S. Balloun**
*Chairman and CEO, Acuity Brands, Inc., Region Co-chair*

**Guy F. Budinscak**
*Atlanta Office Managing Partner, Deloitte and Touché, LLP, Region Co-chair*

**Thomas M. Holder**
*Chairman and CEO, Holder Construction Co.*

**Zenon S. Nie**
*Chairman and CEO, C.E.O. Advisory Board*

**Thomas E Noonan**
*Chairman, President and CEO, Internet Security Systems, Inc.*

## Business Executives for National Security

For more than 20 years, Business Executives for National Security has served as the primary channel through which senior executives can help build a more secure America.

In 1982 business executive and entrepreneur Stanley A. Weiss founded the organization around the simple notion that America's security is everybody's business and that business leaders have a particularly important contribution to make. Today our members focus on developing new tools to combat new security threats that cannot be deterred or negotiated away and finding new resources to reshape and rebuild our military forces for the 21st Century.

Business and government must cooperate if we are to protect the American homeland against cyber attack, track terrorists' financial assets, improve intelligence capabilities, and prepare communities to meet a host of new security responsibilities. And the Defense Department must follow the lead of American business to take full advantage of information technology, outsourcing, and privatization to cut the cost of bureaucracy and overhead and invest the savings in our men and women in uniform.

Now more than ever, national security is everybody's business. Business Executives for National Security – proudly helping to secure America's future.

**Business Executives for National Security**
1717 Pennsylvania Avenue, NW, Suite 350
Washington, DC 20006-4603
p (202) 296-2125 - f (202) 296-2490
http://www.bens.org

**BENS Metro Atlanta Region**
191 Peachtree Street, NE, Suite 1500
Atlanta, GA 30303-1924
p (404) 220-1268 - f (404) 220-1263
bensatl@bens.org

# TABLE OF CONTENTS

## EXECUTIVE SUMMARY

Primarily driven by the terrorist events of September 11, 2001, many businesses are actively seeking guidance on how best to protect their workplace and allay employee concerns about their personal safety at work. Employees, and the public at large, assume that businesses are being proactive in working with government agencies and that they are developing adequate health and safety programs, crisis prevention plans, and post-incident response systems to address the myriad terrorist and bioterrorist risks that exist in today's world. Crisis preparedness requires that companies develop specific programs and procedures to ensure that the health and safety of all employees are an integral part of overall company policy.

Based on feedback from its private sector membership after the 9/11 attacks, the Homeland Security Advisory Group (HSAG), a working group of Business Executives for National Security (BENS) in the Atlanta area, found that companies of all sizes want guidance on what constitutes a reasonable response for firms developing Preparedness and Response Plans (P&RP) for potential future terrorist attacks. This Company Primer, prepared by the HSAG, is intended to raise awareness of company leaders about terrorist and bioterrorist threats, and to provide policy and procedural guidance, particularly to companies not large enough to have dedicated health and safety or security departments.

Specific information in this Primer includes:

- A discussion of the scope and scale of terrorist threats and types of attacks.
- An overview of bioterrorism, discussing potential agents, methods of attack, and overall treatment and control.
- Background on governmental emergency response, explaining local-state-federal relationships and special powers under a public health emergency.
- Procedures for recognizing and responding to bioterrorist attacks, including mailroom and ventilation (HVAC) security procedures, and the crucial importance of rapid interaction with local health officials and emergency management systems.

- Guidelines for maintaining business functions in the event of an attack. This section outlines and offers checklists for critical elements of P&RPs: initial risk assessments, insurance issues, facility security and preparation procedures, business interruption procedures (including issues with cash flow, record preservation, and clients and vendors), and communications procedures.

Though many of the P&RP guidelines are specific to bioterrorism, the plans can easily be adapted for preparing for and responding to more general terrorist threats. Those threats can come not only from radical international organizations but also from domestic extremist groups, ex-employees, or even potentially disgruntled employees, and could involve a wide range of conventional or unconventional weapons. Companies thus must plan for a variety of terrorist attacks and must understand the governmental framework in place to respond to terrorism. For most bioterrorist attacks, the first agency to be notified is the local (county) health department, not a state or federal agency. Businesses need to know their local public health officials and understand how health departments and local public safety officials will respond to potential terrorist or bioterrorist attacks.

This Primer is not intended to be exhaustive in its content. Rather, by helping to develop an awareness and understanding of the potential risks, companies will begin to address these issues and develop a closer dialogue with government agencies responsible for combating terrorism in all its forms.

As one of several projects designed to aid businesses in becoming better prepared to deal with new security threats, this Primer is seen as an "evergreen" document; we recommend visiting the BENS web site (http://www.bens.org) for its latest version. While generic in parts, the document is specifically developed for companies in the greater Atlanta area. In addition, Appendix A provides website addresses to a variety of national health agencies and other organizations where additional information on this topic may be obtained. Most of the information in Appendix B is relevant to the greater metropolitan Atlanta area.

## 1.0 INTRODUCTION

September 11, 2001, focused the attention of the nation on the impact of a terrorist attack in a major metropolitan area. The anthrax attacks that followed demonstrated that terrorists could reach any size and type of organization in the United States. The possibility that any company may become the target for a terrorist or bioterrorist attack requires that companies consider and develop programs to reduce their vulnerability and develop explicit response plans in the event they or their surrounding area are attacked. These response plans should address personal health and safety, emotional distress, and a plethora of business continuation issues.

Following the September 11 attacks, the Homeland Security Advisory Group (HSAG) in Georgia, a working group of Business Executives for National Security (BENS), solicited input from its member organizations about what particularly useful activities might be pursued by the HSAG. Regardless of company size, member input indicated that all companies desired guidance about what would constitute a reasonable response for firms in developing Preparedness and Response Plans (P&RP) for potential future terrorist attacks. The HSAG committed to work with government health and safety officials and member firms to begin to address these planning concerns.

The goal of this Primer, the culmination of HSAG's work, is to raise the awareness of company management – particularly in companies not large enough to have dedicated security departments – about the scope of the potential problem. The Primer presents a brief overview of the scope and scale of the threat, a look at the government structure in place for companies to coordinate with in responding to threats, and an outline of issues that companies need to consider in developing their preparedness and response plans.

## 2.0 SCOPE AND SCALE OF THREAT

September 11 provided a stark example of the ability of terrorist groups with global reach, like Al-Qaida, to cause mass casualties on U.S. soil and significantly disrupt the flow of goods and services. However, both the 1995 Oklahoma City bombing and (most likely) the 2001 anthrax attacks demonstrate that these threats can come from domestic sources as easily as foreign ones, and can impact business and government anywhere in America. Thus, companies must prepare for potential terrorist attacks not only from well-financed groups on an international crusade, but also from a wide range of radical or fringe elements seeking to gain attention or further their agendas through acts of destruction.

In addition to these threats, companies cannot rule out irrational acts of vandalism or terrorist-type attacks by individuals such as disgruntled employees or ex-employees, other individuals, or groups with whom the company comes in contact in its normal course of business. Since the mid-1990s, companies have been aware of the need to ensure that their computers and electronic files are secure against hackers. Today, protecting these valuable electronic records and files against major attacks by cyber terrorists is a necessity. The reality is that companies, regardless of size, are not immune to disruptive and dangerous attacks from many sources.

Given the above, businesses must focus on the potential for terrorist activities (e.g., overt, covert, explosive, biological, chemical, or cyber) and develop systematic plans and procedures for workplace response; companies cannot rely solely on law enforcement agencies to protect them from such attacks. Company managers must incorporate in their business practices steps to increase awareness of, monitoring for, and security against terrorism and must develop response plans in case an attack occurs at their workplace.

## 3.0 TYPES OF ATTACKS

Not only could terrorist attacks target almost any location, they potentially could come in a wide range of forms, depending on the means and objectives of the responsible group. The attacks on the World Trade Center in 1993 and in Oklahoma City in 1995 both involved truck bombs utilizing conventional explosives. The 9/11 hijackers turned commercial airplanes into deadly unconventional weapons for a destructive, mass-casualty attack. Officials fear terrorists are attempting to acquire and use weapons of mass destruction (WMD), including chemical, biological, nuclear, and radiological weapons ("dirty bombs"), for similar ends. Cyber-terrorism could be used to disrupt economic activity, sow confusion, or mask another type of attack.

Although any of the threats described above can create an emergency situation and cause significant disruption to our society and its normal functions, including business and commerce, this Primer concentrates on enhancing the business community's understanding of a biological event. The biological attack is the least understood of these threats, and its manifestations are unfamiliar to the majority of people. Moreover, biological events may have certain characteristics that impose additional challenges. The event may be silently unfolding, escaping early detection. The scale of a biological event may be difficult to predict; there may be one or two victims or the number of casualties may exceed thousands. Unlike other disasters limited to a single location, the biological disaster may spread as disease is

communicated from one person to another. A biological event, even when small in scale, is a national emergency that demands close collaboration and coordination among federal, state, and local officials, and especially the private sector. To effectively respond to these threats, the public (law enforcement and public health) and private sectors (the business community) will need to work closely together, sharing information and resources. For these reasons, the bioterrorist attack deserves considerable attention, and throughout the remainder of this Primer we focus on "bioterrorism" (please refer to Section 4.2).

## 4.0 BASICS OF BIOTERRORISM

### 4.1 Background

A bioterrorist attack could happen in any workplace in America. Most company personnel know little about potential biotoxins or biopathogens or how to recognize these agents and respond in the event of an attack.

To mount an effective public response to bioterrorism, the business community needs to work closely with elected officials, public health departments, local hospital authorities, and emergency and other response agencies. This section provides an understanding of the basics of bioterrorism, the fundamentals of the government's emergency response system, and procedures for recognizing and responding to bioterrorist threats.

### 4.2 What is "bioterrorism"?

The Centers for Disease Control and Prevention (CDC) in Atlanta, Georgia, defines "bioterrorism" as the illicit use of biological agents (e.g., bacteria, viruses, and parasites or their byproducts) to cause illness and spread fear. Bioterrorism could be intended to harm humans and other living organisms, to influence the conduct of government, or to intimidate or coerce a civilian population. An act of bioterrorism may produce a state of emergency and create a disaster. Bioterrorism, however, is fundamentally different from both natural disasters (e.g., floods, tornadoes, and hurricanes) and other forms of man-made emergencies (e.g., fires, industrial accidents, and transportation failures) — because these other events lack the intentional generation of fear or panic caused by terrorism.

Bioterrorism is a form of "asymmetric" warfare, whereby a relatively small event (such as incidents of anthrax after the 9/11 attacks in 2001) can produce widespread changes in a population's beliefs, behaviors, and practices. Law enforcement and intelligence authorities recognize that

**Bioterrorism is a form of "asymmetric" warfare.**

bioterrorist events may be perpetrated by a disillusioned individual, small splinter groups, organized protest groups, or apocalyptic ideological groups. Often the primary purpose is to instill fear and panic and create economic disruption to accomplish some ideological goal.

### 4.3 Biological agents

Certain biological organisms are better suited than others for use as weapons. This is due to the ease with which a terrorist can grow, acquire, and/or maintain adequate quantities of the organism, the ability to spread the organism to large numbers of victims, the ability of the organism to spread from person to person once released, and the severity of the disease caused by the organism.

The CDC has organized potential pathogens into a variety of categories. The U.S. public health system and primary healthcare providers as well as emergency response participants (such as firefighters and Emergency Medical Technicians) must be prepared to address various biological agents, including pathogens that are rarely seen in the United States. High-priority agents (Category A), including the organisms shown in the table below, pose a risk to national security because they:

- Can be easily disseminated or transmitted from person-to-person;
- Result in high death rates and have the potential for major public health impact;
- Might cause public panic and social disruption; and
- Require special action for public health preparedness.

**Category A — Potential Organisms for Bioterrorism**
(source: Centers for Disease Control and Prevention)

| |
|---|
| Anthrax *(Bacillus anthracis)* |
| Botulism *(Clostridium botulinum* toxin) |
| Plague *(Yersinia pestis)* |
| Smallpox *(Variola major)* |
| Tularemia *(Francisella tularensis)* |
| Viral hemorrhagic fevers (filoviruses {e.g., Ebola, Marburg} and arenaviruses {e.g., Lassa, Machupo}) |

### 4.4 What may an attack look like?

There are several ways a bioterrorist event may manifest itself. The biological event may result from a "covert" attack (i.e., unannounced release of a pathogen into the environment). A covert attack may be unleashed by the receipt of an object, such as a package or piece of mail, accompanied by a warning or threat. Alternatively, the attack may be an "overt" act, where the release of the pathogen into the environment is either announced or witnessed by persons present. It is important to note that a bioterrorist event could be committed in

conjunction with another type of attack (e.g., cyber-terrorism), magnifying the terror effect or potentially masking the more deadly medical emergency that is about to unfold.

### 4.5 Example of a "covert" release of biotoxin or biopathogen

In this scenario, a known or suspected pathogen is released into the environment in a covert manner, causing exposure to a number of persons. For example, release of a biological agent could occur through delivery of a package contaminated with anthrax spores or another pathogen. Biological agent release also could occur via the ventilation system (HVAC) in a building, where dispersal could take place within a matter of minutes.

Because this release is – by definition – not witnessed, the effects of such an event can be widespread and difficult to isolate or recognize. Exposed individuals might begin to visit ambulatory clinics and emergency departments following the onset of symptoms. Because the early phase of these illnesses may have non-specific symptoms (e.g., fever, malaise), they are difficult to distinguish from other ordinary ailments, such as acute respiratory or influenza-like illnesses.

As a result, the attack may be recognized only after a physician notices a sudden increase in the number of patients with similar symptoms and notifies public health authorities. Other clues that may signal a covert bioterrorist attack include an increase in unexplained deaths, an unusual age distribution of patients (e.g., severe illness among normally healthy persons 20-50 years old), atypical timing of a disease (e.g., flu-like illness during the summer months), or an unusual form of a disease (e.g., inhalational anthrax).

### 4.6 Example of an "overt" release of biotoxin or biopathogen

In this scenario, a known or suspected pathogen is overtly released into the environment, causing exposure to a number of persons. Such an exposure could follow aerosolized dispersion of a pathogen. In addition to securing the site to prevent additional human exposure, efforts would focus on identifying or confirming the pathogen involved and isolating persons suspected of having been exposed.

### 4.7 Treatment and control of biological attacks

The goal of the medical care community (i.e. hospitals, physicians, and other health care providers) is to diagnose the disease (which frequently may be unfamiliar to most clinicians) and provide treatment. Some of the diseases can be spread from person to person, through coughing or sneezing or via direct contact (touching) of bodily fluids or contaminated clothing. When treating a patient with a disease that can be spread from person to person, hospital personnel will implement additional isolation measures (e.g., masks, specially ventilated rooms) to prevent the spread of the agent.

The goal of public health authorities is to detect and control the outbreak of the illness. Public health officials will focus on identifying and treating "exposed" persons (i.e., persons who may have had contact with the pathogen but who do not yet have signs or symptoms of disease), and preventing the spread of disease. For some diseases (e.g., anthrax), control measures will include providing antibiotics to such exposed persons. The antibiotics, if given soon enough after exposure, may prevent the occurrence of illness altogether or may make the illness less severe. Similarly, for some diseases (e.g., smallpox), vaccinations are given to exposed persons to reduce the spread of illness. For pathogens that spread from person to person such as smallpox, public health authorities may also consider quarantine.

## 5.0 BACKGROUND ON GOVERNMENTAL EMERGENCY RESPONSE SYSTEM

### 5.1 Local, state, and federal relationships

In most states, the local political jurisdiction (typically the county) has responsibility for emergency management and response. Typically, this authority is delegated to an emergency management agency. Most jurisdictions have adopted the Incident Command System (ICS) to control and manage a coordinated response to a terrorist event. The ICS provides a robust management system for responding to all types of emergencies and terrorist attacks, including biological events. Mutual aid agreements between local, state, and federal agencies enable effective coordination and sharing of resources across boundaries, particularly in the event of a crisis.

**During a bioterrorist attack, the local public health agency usually retains overall responsibility for command and control or emergency operations.**

When the disaster response outstrips local resources or involves multiple jurisdictions, the local emergency manager seeks assistance and coordination at the state level. When state capacity is exceeded, the Governor, often through a state emergency management agency, seeks federal assistance from the Federal Emergency Management Agency (FEMA). The ICS is used by FEMA along with four basic principles of emergency management (mitigation, preparedness, response, and recovery); these systems are advocated by FEMA for use in emergency preparedness and response initiatives related to all types of emergency situations, including bioterrorism.

Public health departments operate in a similar manner. Local health departments may seek assistance from their state health department, and

the state health department may seek assistance from the Centers for Disease Control and Prevention. When a disaster overwhelms a jurisdiction's medical services, the federal government may mobilize the National Disaster Medical System. The NDMS comprises 7,500 volunteer health professionals organized into general and specialty teams.

In the event of a bioterrorist attack, these basic local-state-federal relationships hold, with an additional stipulation. Presidential Decision Directive (PDD) 62 and PDD 63 stipulate that in the event of a terrorist attack, the Federal Bureau of Investigation (FBI) will take the lead role for "crisis management" or issues related to preventing or responding to acts of terrorism. At the federal level, FEMA has lead responsibility for consequence management.

During a bioterrorist attack, however, the local public health agency usually retains overall responsibility for command and control of emergency operations, except where state or federal statutes transfer authority to a specific state or federal agency. Thus, mutual-aid agreements among local jurisdictions remain in effect, as well as any existing arrangements for providing assistance between a state government and its localities. Similarly, if the state requires federal assistance for consequence management, FEMA maintains lead responsibility for coordinating assistance. FEMA is also responsible for providing aid to states and local agencies through the Federal Response Plan; this plan defines how the federal government will provide assistance in the event of a presidential declaration of emergency.

Although these multiple layers and roles make the emergency response seem complex and hierarchical, in practice, particularly in matters related to public health, the local, state, and federal agencies closely coordinate and mutually support each other's activities.

### 5.2 Special powers under a public health emergency

In the event of a bioterrorist event, the local jurisdiction (e.g., county executive officer, mayor, or other chief elected official), in concert with the local health authority, may declare a public health emergency. Under these circumstances, the local health authority may exercise those powers vested under such a declaration. Similarly, a Governor may declare a state of public health emergency, thereby invoking, within the limitations of the state statute, broad exercise of power to address the emergency situation.

These special powers may be invoked during a state of public health emergency to manage the emergency and control property. Examples of where these powers might be needed in the event of a terrorist or bioterrorist attack include requirements to manage and control:

- Distribution of health care supplies (e.g., antibiotics and vaccines)
- Use and distribution of material and supplies
- Stressed medical resources and facilities (e.g., clinics and hospitals)
- Access to health care facilities (e.g., unruly mobs descending upon emergency departments seeking medications)
- Safe disposal of infectious waste and human remains
- Fair compensation of property seized for state purposes under emergency circumstances (e.g., the government uses a private facility as an infirmary to treat or isolate patients)
- Necessary destruction of property (e.g., nuisance abatement).

## 6.0 PROCEDURES FOR RECOGNIZING AND RESPONDING TO BIOTERRORIST ATTACKS

### 6.1 Recognizing the attack

#### 6.1.1 Absenteeism or other unusual patterns

As employers, businesses provide a vital window on the health status of a community. A covert or unannounced release of a biological pathogen may cause an illness that first manifests as increased absenteeism in the workplace. Employers should be familiar with the sick-leave patterns of their employees, and should ensure timely reporting to senior management when an unanticipated increase or unusual pattern develops.

It is important that businesses, in turn, report unusual patterns of absenteeism to the local public health department, or to a local healthcare professional or government official in communities that do not have a public health department presence. All states are actively developing Preparedness and Response Plans (P&RP) for terrorist and other catastrophic events, with the help of federal funding distributed by the CDC. One of the elements in many state plans is a "Sentinel" program, through which local health departments and the states can effectively assimilate and analyze early signs indicating the possibility of a bioterrorist attack. An unusual or high incidence of absenteeism in the workplace is one useful piece of information in making these assessments. Employers should communicate with local health departments and discuss how they (the private sector in general) can support these efforts.

#### 6.1.2 Mailroom procedures for managing suspicious packages

Because all businesses receive mail, and because it is relatively easy to send biological agents through the mail (e.g. the 2001 anthrax incidents), companies should develop specific procedures for managing suspicious packages. Employees need to be educated about recognizing suspicious packages and the procedures to follow if they receive such a package. Emphasis should be on minimizing exposure (unprotected contact between employees and the suspicious package) and timely notification of appropriate authorities. Follow-

ing are some of the common warning signs of mail and packages that might indicate a terrorist or bioterrorist parcel:

- Unexpected mail or mail from someone unfamiliar to you
- Addressed to someone no longer with your organization or otherwise outdated
- Excessive postage
- Handwritten or poorly typed addresses
- Incorrect titles
- Title, but no name
- Misspellings of common words
- Oily stains, discolorations, or strange odors
- No return address, or a return address that cannot be identified as legitimate
- A city or state in the postmark that doesn't match the return address
- Restrictive endorsements, such as "Personal" or "Confidential"
- Oddly shaped, or an unusual weight for its size
- Protruding wires, or dripping powders or liquids


*The U.S. Postal Service has a useful poster highlighting procedures for handling suspicious mail at www.usps.com (search "suspicious mail").*

If a parcel appears suspicious (i.e. may contain biological, chemical or explosive agents), the following are some important steps to take:

- Handle the parcel with care
- Isolate the parcel
- Don't open, smell, or shake the parcel
- Call the police

### 6.1.3 Security procedures for building ventilation (HVAC)

The release of a biological agent into the ventilation system of a building is a considerable threat. Given that a bioterrorist action of this nature is likely to be covert, rather than witnessed, and large numbers of people could be exposed to a biological agent in a very short period of time (minutes), businesses should closely evaluate their security procedures and physical vulnerabilities. The following could be indicative of a terrorist or bioterrorist release via a building's HVAC:

- Damage to HVAC intakes or other evidence of tampering
- Residue or discoloration in or near HVAC intakes
- Other indications of tampering with HVAC equipment

The following actions should be performed to minimize the possibility of this type of event:

- Inspect HVAC equipment and all intakes frequently
- Insure that HVAC equipment is in a secure location
- Include the ventilation system as part of a hazard vulnerability assessment and in subsequent emergency response plans
- Define procedures for notifying local law enforcement and local public health agencies regarding any perceived threat or indication of a bioterrorist event

### 6.2 Familiarity with your local emergency management system

Timely notification of authorities requires employers to be familiar with how their state and local public health agencies and emergency management systems operate. Inviting local officials to speak at chamber of commerce meetings and other gatherings of business leaders can foster relationships between the business community and public health and safety officials.

Because an effective response to a biological event requires action by multiple agencies and response sectors, an essential element of preparedness is the development of relationships and familiarity with operating procedures across all sectors. Procedures for coordination, command and communication must be established in advance if all of the goals of the disaster response are to be met in a timely and effective fashion. Business leaders need to know their emergency response agencies and personnel.

**Due to the nature of biological agents, hours, even minutes, can make a significant difference in the ability to isolate and contain the event.**

If these relationships between the private and public sector have been established, a business will know who to call when something unusual occurs. The business manager, sensing something unusual in the absenteeism pattern of employees, will know to call the local or state health department. Employees and their supervisors will know to call appropriate public safety officials and public health officials for consultation and advice when a suspicious package arrives.

Time is a key element of an effective response. Due to the nature of biological agents, hours, even minutes, can make a significant difference in the ability to isolate and contain the event. Therefore, a business not only needs to know "who to call," but to do so promptly. Appendix B provides contacts and phone

numbers for county health units in Georgia and website links to other important agencies that would be involved in an emergency.

### 6.3 Community response to bioterrorist attacks

#### 6.3.1 Providing general support for community morale

Unlike natural disasters, for example floods and earthquakes, that produce immediate and physically horrific results, biological events may unfold slowly and invisibly, as a result producing deep public fears. Psychological responses following a biological terrorist attack could include anger, panic, fear of contagion, search for a scapegoat, social isolation, demoralization, loss of faith in social institutions, and loss of faith in governmental agencies.

A critical element for any community is an effective risk communications plan, with identification of credible and trusted spokespeople who can provide accurate and frequent assessments of what is known and what is not known as events unfold. Rumors need to be anticipated and mechanisms established for debunking them. Business leaders can provide needed support to government by offering credible spokespersons to calm the public, instill confidence and trust in the agencies responding to the crisis, and reassure citizens that the disaster is being adequately addressed.

In addition to government agencies that need to have a comprehensive and credible communications protocol, individual companies need to develop a communication plan they can implement in the event of a crisis. The key elements of such a plan are addressed in Section 7.5.4 of this document.

#### 6.3.2 Providing support for employees

As members of the community, a company's employees will face the same challenges to mental health as others within that community. Medical personnel anticipate that a biological attack may produce contagious somatization (i.e. breathing difficulties, tremors, sweating, feelings of anxiety, and labile mood). Symptoms such as these may compel the "worried well" to seek care at health care facilities, thereby overwhelming the capacity of the health care system to provide care for legitimate victims.

**The "worried well" seeking care at existing health care facilities could overwhelm the capacity to provide care for legitimate victims.**

Restoration of mental health following a biological event may be a prolonged process. The impact upon mental health may extend well beyond those who directly experienced the disaster, including those who witnessed events via television or other media.

Employers need to recognize the importance that employees will place upon ensuring the safety of their family members and other loved ones before returning to work. Societal norms have created expectations that health care workers, public safety officials, and other emergency personnel will report for duty, regardless of the level of threat to personal health or safety. But recent surveys of hospital staff and administrators have consistently identified care (e.g. child care) for family members of staff as the highest priority and the most likely barrier to an effective hospital response. Unless addressed in advance, similar concerns among non-health-care workers could delay their return to the workforce.

#### 6.3.3 Providing specific support for emergency response

If local, state, or federal goverments declare a state of public health emergency and/or invoke special powers, businesses may be called upon to provide emergency support for various functions (e.g. local distribution of medical supplies). The type and level of support would depend upon the nature of the emergency and the type of business. Businesses may be called upon to provide both facilities and supplies to support public safety efforts.

## 7.0 GUIDELINES FOR MAINTAINING BUSINESS FUNCTIONS

### 7.1 How an attack can affect business

**Any Preparedness & Response planning agenda should include risk assessment, facility preparation and response, insurance issues and communication procedures.**

Because the sizes, nature, geographic locations, procedures, and physical layouts of companies vary widely, it is impossible to develop a generic Preparedness and Response Plan (P&RP) that could be effectively used by any one company. In addition, most businesses are vulnerable to numerous types of natural and man-made hazards, which should be addressed with hazard-specific P&RPs. Nevertheless, there are a number of common issues and elements that should be considered when developing a biological event P&RP for a business entity. This section outlines some of the critical issues and elements of a Preparedness and Response planning agenda, including risk assessment, facility preparation and response, insurance issues and communications procedures.

These items, however, are only examples of some of the more important issues that must be considered when assessing risks and developing a company-specific P&RP. In developing specific P&RPs, executives are encouraged to study many of the internet references cited in Appendix A and may wish to retain consultants with special experience and expertise in this area.

Due to the nature of biological weapons and the varied methods of delivery, most companies might never be affected by a direct attack, but many could be severely affected by degradation in basic services such as mail, transportation, and communications.

Anthrax has proven to be particularly disruptive to the mail system, contaminating mail handling facilities and any office or business to which it is delivered. A coordinated attack could have nationwide consequences for mail delivery for an extended period of time. Increased costs, long delays, lost mail, and potential restrictions on mail service would have devastating effects on business throughout the country.

Numerous other infectious agents could also be used, with the most likely targets being transportation hubs (airports, train/subway systems and port facilities), central city areas and areas with large population concentrations, including stadiums, convention centers or shopping malls. These attacks might be aimed at creating fear and terror in the population and contaminating the facilities to render them temporarily unusable. Businesses with strong public profiles, important locations (e.g., businesses near critical infrastructure, in tall buildings, near federal offices, etc.), or well-known political ties could be more attractive targets for an attack.

Although communication systems are not likely to be targeted directly by bioterrorist attacks, they could be targeted by cyber-terrorists in conjunction with bioterrorist attacks. Maintaining and/or reestablishing communications with local emergency response personnel, employees, customers, suppliers, and the community will be a major component of any response plan.

### 7.2 Risk assessment

In developing a site-specific P&RP, an assessment needs to be made on the vulnerability of a particular site or business. While the likelihood of a specific company or building being targeted for a terrorist attack is difficult to predict, a survey of some general risk factors can be a guide to a company's vulnerability and how detailed a specific P&RP plan should be. Some of the risk assessment factors that should be considered include:

- Industry – Is your company or facility a "critical industry" or part of a critical infrastructure?
  - Transportation, communication, power, water supply, health services, defense, or banking?
- Geography – Is your facility located near other entities that provide critical services?
  - Transportation hubs or central structures – bridges, tunnels, subways, airports, or ports?
  - Refineries, chemical plants, storage facilities or pipelines?
  - Nuclear/conventional power plants or major electrical switching centers?

  - Defense facilities: naval ports, air bases, logistic deports, command centers?
  - Specialized facilities: governmental centers, communication hubs, Federal Reserve banks, FAA control centers, CDC Headquarters, national sites of significance.

Although not meant to be exhaustive, the above list illustrates some factors that may increase the risk profile of a specific company.

### 7.3 Facility preparation and response

Following is a partial list of considerations to help deter and respond effectively to bioterrorist attacks.

- Does the facility have a security system?
- Does it have a method of identifying employees and visitors?
- Are parking areas monitored?
- How is access restricted to sensitive or critical areas?
- Have employees been trained to report and respond to unusual activity?
- Have mail handling personnel been trained to identify and respond to suspicious packages?

In the event of a chemical, biological or radiological (CBR) attack, it may be necessary for employees and visitors to remain in your office building for an extended period of time. This "Shelter-in-Place" concept has some planning implications that are unique to CBR attacks:

- Identify suitable "shelter-in-place" areas where personnel are to congregate. These should be interior rooms in a building and be above ground level because some chemical or biological agents are heavier than air.
- Do the "shelter-in-place" locations have facilities and supplies stored "in house" for employees and visitors for a one to three day period (water, food, first aid, communications, etc.)?
- Can the "shelter in-place" areas be easily isolated from the exterior environment by shutting down the HVAC system and sealing doors, windows, and vents?
- Does the area or building have shower facilities for decontamination?
- Have you made a survey of and do you understand the operation of the HVAC system(s)?
  - Are the air intake(s) secure or out of reach from ground level?
  - How does the HVAC respond to fire alarms or actual fire detection?
  - How quickly can the HVAC be shut down? Who knows how to shut down the system?
- Do you have a way of communicating with employees and emergency response personnel (e.g. in case there is a need to evacuate or remain in building)?
- Do you have battery operated radios, lights, and cell phones?

### 7.4 Insurance issues

**Has your company purchased the optional terrorist coverage for all insurance policies available under the Terrorism Risk Insurance Act of 2002?**

Because of the terrorist attacks of September 11, 2001, the U.S. Congress passed the Terrorism Risk Insurance Act of 2002 (TRIA). This act applies to **all** insurance policies written or renewed after November 26, 2002, and creates a risk-sharing mechanism that spreads any losses from foreign acts of terrorism. Under TRIA, all policy holders are offered an opportunity to purchase a terrorism endorsement for their specific insurance policy. In essence, by purchasing this endorsement, the insurance company will not attach a terrorism exclusion to the specific policy. Although it is difficult to generalize, the cost of the terrorism endorsement typically ranges from 2% to 10% of the basic policy premium (2002-2003 data). In 2002, most companies were purchasing the TRIA endorsement for property insurance and workers compensation insurance policies. These higher risk lines of insurance had TRIA endorsement costs in the range of 6% to 10% of the policy premium. On other lines of insurance the acceptance rate for the TRIA endorsement was less than 50% and for some lines of insurance was in the range of 25% even though the cost of the TRIA endorsement was at the low end of the range cited above.

Business executives should be aware of the TRIA provisions and should carefully consider whether it is prudent, for their situation, to purchase the optional terrorism insurance coverage.

### 7.5 Checklist of Issues for Preparedness and Response Plans

The following checklist, although it does not address all the issues, provides a useful guide of items to consider when preparing a P&RP.

#### 7.5.1 Awareness and facility hardening

- ☐ Is outside of the building or workplace and parking lot adequately lighted?
  - ☐ Is a procedure in place to ensure light bulbs are checked and operating?
- ☐ Are there unusual cars in parking lot?
  - ☐ Is someone tasked with monitoring the cars in the parking lot?
- ☐ Is landscaping around building neat and well kept (minimize hiding places)?
- ☐ Is the workplace locked when appropriate?
  - ☐ Are all doors and locks operating properly?
  - ☐ Are door closers properly adjusted to close doors after entry/egress?

- ☐ Does the work facility have a security system?
  - ☐ Is the security system routinely used?
  - ☐ Is there a procedure in place to deny access to the workplace for exemployees?
- ☐ Does the company have an adequate method of identifying all who work in or visit the facility?
- ☐ Is access restricted in critical or sensitive areas?
- ☐ Is access limited to only current employees and visitors?
- ☐ Have employees been trained and encouraged to be alert and look for unusual packages, cars, and other factors that might be a sign of a suspicous event?
  - ☐ Is there a procedure for reporting any unusual activity or facility problems within the company?

### 7.5.2 Facility procedures

- ☐ Have personnel responsible for handling mail been briefed on what to look for and what to do with suspicious packages?
- ☐ Are employees trained and encouraged to be on the lookout for suspicious packages or activities in the workplace?
  - ☐ Does the company have someone designated to periodically survey the building or workplace and look for suspicious packages or activities?
  - ☐ Has the company identified someone to be the contact if there are suspicious activities?
- ☐ In the event of an emergency evacuation of the workplace, is a procedure established where employees are to meet and take stock of the situation?

### 7.5.3 Business interruption procedures

- ☐ Does the company, and all its various units, have adequate Business Interruption insurance?
  - ☐ Is there an exclusion for acts of war, terrorism, or civil unrest?
  - ☐ Has the optional terrorist endorsement under TRIA been purchased?
- ☐ Are necessary and critical paper and electronic files frequently backed-up?
  - ☐ Are the files stored on-site or off-site?
  - ☐ Are critical files, papers, and backed-up data stored in fireproof vaults?
  - ☐ Are electronic files and other critical data stored off-site in case access to the facility or workplace is restricted?

- ☐ How would the business continue if the workplace or storage facilities were destroyed or access to these facilities restricted for days, weeks, months?
- ☐ Where would critical employees work and how would business processes continue if tomorrow you could not re-enter the workplace for any reason?
- ☐ Would or could the company continue to provide deliverables, products, or services to clients in the event of a terrorist attack?
  - ☐ For how long?
- ☐ What would be the financial impact on the business entity if there were a delay in delivering goods or services to clients?
  - ☐ Can a significant increase in accounts receivable be handled by the company?
  - ☐ Would all/some employees be put on temporary furlough (with or without pay)?
  - ☐ Does company have an adequate line of credit or financial capacity to allow it to continue for a sufficient period of time if the workplace need to be decontaminated or rebuilt?
  - ☐ What would happen to inventory, work product, hardware, software, and fixed assets? Could all or some be reused?

### 7.5.4 Communications procedures

In the event of a terrorist act or civil disaster, timely, accurate communications will be critical for the success and survival of a company. The following should be considered in developing a communications plan:

- ☐ Designate a communications team. Ensure all communications go through this team. One defined communications channel is superior to random people reporting.
- ☐ Who will be the primary contact with the local and state public health and public safety agencies?
  - ☐ Has the company met with local public health, public safety, and fire department officials to discuss specific preparedness and response plans?
  - ☐ Have specific first responder agency contacts been identified?
  - ☐ Do the individuals tasked with communication responsibilities have the contact numbers of the agency personnel (e.g. office phone, fax number, mobile phone number, home phone number)?
- ☐ What and how will you communicate with your employees?
- ☐ What and how will you communicate with the families of the employees?

- ☐ What and how will you communicate with your clients?
  - ☐ They want to know if and how their businesses will be affected by your situation.
- ☐ What and how will you communicate with your vendors?
  - ☐ They want to know if and how their business will be affected by your situation.
  - ☐ They want to know if they will be paid for goods and services provided.
- ☐ What and how will you communicate with the media?
  - ☐ Who is the best and most credible spokesperson for the company?
  - ☐ How often will the company provide media updates?
  - ☐ The company should set the schedule for media communications.

## 8.0 SUMMARY

No company executive likes to think about planning for or responding to a terrorist or bioterrorist attack at his or her workplace. But the events of 9/11 and the following anthrax attacks served as a wake-up call to American businesses that ignoring such threats and being complacent is not a good business decision. It is incumbent upon the private sector to take steps to develop Preparedness and Response Plans (P&RP) to help ensure that a terrorist attack in the workplace can be effectively handled. In many ways, P&RP development for such attacks is not dramatically different than developing response plans for natural disasters or other crises. However, issues of "hardening" the workplace, increased awareness of potential terrorist threats, training, and interaction with governmental agencies can be specific to this type of planning.

When considering plans for and responses to a terrorist event, it is clear that the private sector must work closely with public health and public safety agencies. In most cases, the business community is not knowledgeable about the roles, responsibilities, or interactions of public health and public safety agencies. An important step in any business entity's development of an effective P&RP is to build a better understanding of and liaison with the appropriate public health and public safety personnel and to integrate its efforts with those of government. We hope this Primer underscores the need for that integration and helps educate executives and others in the business community on how best to prepare for terrorism.

## Appendix A — General Website Links to Health Agencies and Organizations Nationwide

**All states contact information:**
http://www.statepublichealth.org

**US Department of Homeland Security**
http://www.ready.gov; http://www.dhs.gov

**National Institute for Occupational Safety and Health (NIOSH)**
http://www.cdc.gov/niosh/homepage.html

**Building Safety**
http://www.cdc.gov/niosh/bldvent/2002-139E.html

**Emergency Preparedness for Business**
http://www.cdc.gov/niosh/topics/prepared/prepared_contact.html

**Centers for Disease Control and Prevention (CDC)**
http://www.cdc.gov; http://www.bt.cdc.gov/emcontact/index.asp;
http://www.bt.cdc.gov/links.asp

**US Army Corps of Engineers** — protecting buildings and their occupants
http://buildingprotection.sbccom.army.mil/basic/

**Federal Emergency Management Authority**
http://www.fema.gov

**Emergency Management Guide for Business and Industry**
http://www.fema.gov/library/bizindex.shtm

**US Environmental Protection Agency** – building air quality
http://www.epa.gov; http://www.epa.gov/iaq/largebldgs/baqtoc.html

**American Red Cross**
http://www.redcross.org; http://www.redcrossatlanta.org

**Business and Industry Guide**
http://www.redcross.org/services/disaster/beprepared/busi_industry.html

**Office of Homeland Security** – homeland security state contact list
http://www.whitehouse.gov/homeland/contactmap.html

**United States Postal Service**
http://www.usps.com/news/2001/press/pr01_1010tips.htm

**United States Department of State** – travel warnings
http://www.travel.state.gov/travel_warnings

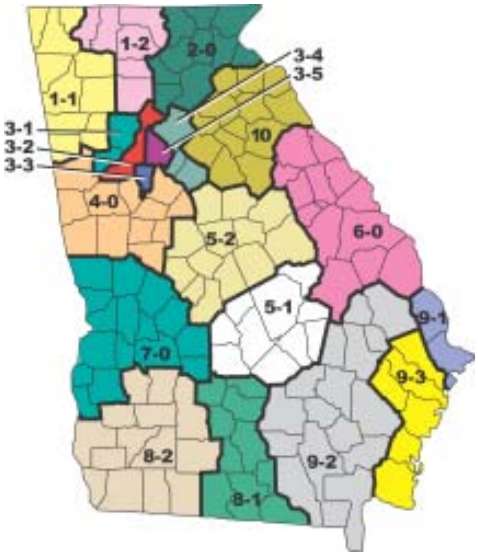
**Small Business Administration**
http://www.ibhs.org/docs/openforbusiness.pdf

## Appendix B — Listing of Georgia Public Health Officers, Local Emergency Contact Information, and Website Links Specifically for Georgia

The Georgia Division of Public Health (GDPH) is the lead agency entrusted by the people of the State of Georgia with the ultimate responsibility for the health of communities and the entire population. At the state level, GDPH is divided into numerous branches, sections, programs and offices, and at the local level, GDPH functions via 19 health districts and 159 county health departments. GDPH is part of a larger state agency, the Georgia Department of Human Resources (DHR).

The Division of Public Health, DHR, is responsible for setting public health policy and providing leadership for public health interests statewide: epidemiology and outbreak investigations, maternal and child health programs including the Women, Infant, and Children's (WIC) Nutrition program, environmental health and injury prevention, Emergency Medical Services (EMS) and medical aspects of state emergency response, vital records and health statistics, chronic disease prevention and health promotion, the Public Health Laboratory, and infectious disease prevention including sexually transmitted diseases (STDs), HIV/AIDS and tuberculosis. The director has direct supervisory responsibility for eighteen of the nineteen physician-level district health directors, and approximately ten program and administrative managers. The Division of Public Health has a budget of over $400 million and more than 6,000 state and related county public health employees.

### Georgia Public Health Districts




| | |
|---|---|
| 1-1 | Northwest (Rome) |
| 1-2 | North Georgia (Dalton) |
| 2 | North (Gainesville) |
| 3-1 | Cobb-Douglas |
| 3-2 | Fulton |
| 3-3 | Clayton (Morrow) |
| 3-4 | East Metro (Lawrenceville) |
| 3-5 | DeKalb |
| 4 | LaGrange |
| 5-1 | South Central (Dublin) |
| 5-2 | North Central (Macon) |
| 6 | East Central (Augusta) |
| 7 | West Central (Columbus) |
| 8-1 | South (Valdosta) |
| 8-2 | Southwest (Albany) |
| 9-1 | East (Savannah) |
| 9-2 | Southeast (Waycross) |
| 9-3 | Coastal (Brunswick) |
| 10 | Northeast (Athens) |

## State Health Officer:
**Kathleen E. Toomey, MD, MPH**
**2 Peachtree Street, NW**
**Atlanta, Georgia 30303-3186**
**Tel: (404) 657-2700 Fax: (404) 657-2715**

## District Health Officers:

**District 1 Unit 1: Northwest**
C. Wade Sellers, MD
1305 Redmond Rd., Building 614
Rome, Georgia 30165-1391
Tel: (706) 295-6704 Fax: (706) 802-5435

**District 1 Unit 2: North Georgia**
Thomas Chester, MD, MPH
100 W. Walnut Avenue, Suite 92
Dalton, Georgia 30720-8427
Tel: (706) 272-2342 Fax: (706) 272-2221

**District 2: North**
Melody A. Stancil, MD
1280 Athens Street
Gainesville, Georgia 30507
Tel: (770) 535-5743 Fax: (770) 535-5958

**District 3 Unit 1: Cobb/Douglas**
Alpha Bryan, MD
1650 County Services Parkway SW
Marietta, GA 30060-4010
Tel: (770) 514-2330 Fax: (770) 514-2320

**District 3 Unit 2: Fulton**
Dennis Daniels, MPH, DrPH
99 Butler Street
Atlanta, Georgia 30303-3045
Tel: (404) 730-1205 Fax: (404) 730-1294

**District 3 Unit 3: Clayton**
Stephen Morgan, MD
1380 Southlake Plaza Dr.
Morrow, GA 30260
Tel: (770) 961-1330 Fax: (770) 961-8370

**District 3 Unit 4: East Metro**
Alan Sievert, MD
324 West Pike Street
P.O. Box 897
Lawrenceville, Georgia 30046-0897
Tel: (770) 339-4277 Fax: (770) 339-2334

**District 3 Unit 5: DeKalb**
Paul J. Wiesner, MD
445 Winn Way
P.O. Box 987
Decatur, Georgia 30031-1701
Tel: (404) 294-3700 Fax: (404) 294-3715

**District 4: LaGrange**
Michael Brackett, MD
122 Gordon Commercial Dr., Suite A
LaGrange, Georgia 30240-5740
Tel: (706) 845-4035 Fax: (706) 845-4350

**District 5 Unit 1: South Central**
Lawton Davis, MD
2121-B Bellevue Road
Dublin, Georgia 31021-2998
Tel: (478) 275-6545 Fax: (478) 275-6575

**District 5 Unit 2: North Central**
Joseph R. Swartwout, MD
811 Hemlock Street
Macon, Georgia 31201-2198
Tel: (478) 751-6247 Fax: (478) 751-6099

**District 6: East Central**
Frank Rumph, MD
1916 North Leg Road
Augusta, Georgia 30909-4437
Tel: (706) 667-4255 Fax: (706) 667-4365

**District 7: West Central**
Zsolt Koppanyi, MD, MPH
P.O. Box 2299
Columbus, Georgia 31902-2299
Tel: (706) 321-6300 Fax: (706) 321-6126

**District 8 Unit 1: South**
Lynne Feldman, MD, MPH
P.O. Box 5147
Valdosta, Georgia 31603-5147
Tel: (229) 333-5290 Fax: (229) 333-7822

**District 8 Unit 2: Southwest**
J. Paul Newell, MD
1109 N. Jackson Street
Albany, Georgia 31701-2022
Tel: (229) 430-4127 Fax: (912) 430-5143

**District 9 Unit 1: East**
Diane Weems, MD
P.O. Box 14257
Savannah, Georgia 31416-1257
Tel: (912) 356-2233 Fax: (912) 356-2868

**District 9 Unit 2: Southeast**
John T. Holloway, MD
1101 Church Street
Waycross, Georgia 31501-3525
Tel: (912) 285-6010 Fax: (912) 284-2980

**District 9 Unit 3: Coastal**
David Page, MD, MPH
1609 Newcastle Street
Brunswick, Georgia 31520-6796
Tel: (912) 264-3907 Fax: (912) 262-2315

**District 10: Northeast**
Claude A. Burnett, MD, MPH
220 Research Drive
Athens, Georgia 30605
Tel: (706) 583-2870 Fax: (706) 548-5181

## Website Links

### State

**Georgia Division of Public Health – District Health Officers**
http://health.state.ga.us/regional/directors.shtml

**Georgia Office of Homeland Security**
http://www.gahomelandsecurity.com

**Georgia Emergency Management Agency**
http://www.gema.state.ga.us

**Georgia Division of Public Health - Emergency Preparedness**
www.health.state.ga.us/programs/emerprep

**Georgia Water and Pollution Control Association - Water System Security**
http://www.gwpca.org/Security/safety.htm

### County

**Georgia Fire/Emergency Listings**
http://www.the911site.com/911lk/georgia.shtml

**DeKalb County Board of Health**
http://dekalbhealth.net

**Atlanta-Fulton County Emergency Management Agency**
http://www.afcema.net

**Red Cross Atlanta**
http://www.redcrossatlanta.org

## Emergency Response Organizations:

### Federal

#### Federal Emergency Management Agency (Regional Offices)

Kenneth O. Burris, Jr.
Regional Director
(770) 220-5224

Mary Lynne Miller
Deputy Regional Director
(770) 220-5216

3003 Chamblee Tucker Road
Atlanta, Georgia 30341
Tel: (770) 220-5200 Fax: (770) 220-5230

**Division Directors:**

Greg Burel
Director Administration and
Resource Planning Division (ARP)
(770) 220-5272

A. Todd Davison
Director of Flood Insurance and
Mitigation Division (FI&MT)
(770) 220-5401

Kelvin Kelkenberg
Director of Office of National
preparedness (ONP)
(770) 220-5454

Paul W. Fay
Director of Readiness, Response
and Recovery Division (RRR)
(770) 220-5316

### State

Mike Sherberger
Director
(404) 635-7001

Georgia Emergency Management Agency
P.O. Box 18055
Atlanta, Georgia 30316-0055
1-800-TRYGEMA
(404) 635-7000

### County

DeKalb County Board of Health
445 Winn Way
Decatur, Georgia 30030
Tel: (404) 294-3700

Atlanta-Fulton County Emergency
Management Agency
130 Peachtree Street SW, Suite G-157
Atlanta, Georgia 30303
Tel: (404) 730-5600 Fax: (404) 730-5625

## Police Departments

Atlanta Police Department
675 Ponce de Leon Avenue NE
Atlanta, Georgia 30308
Emergency Number: 911
Non-Emergency Number: (404) 853-3434

Fulton County Police Department
130 Peachtree Street SW
Atlanta, Georgia 30303
Emergency Number: 911
Non-Emergency Number: (404) 730-5700

DeKalb Police Department
3630 Camp Circle
Decatur, Georgia 30032
Emergency Number: 911
Non-Emergency Number: (404) 294-2000

## State Fire and Rescue Services

DeKalb County Fire and Rescue Services
3630 Camp Circle
Decatur, Georgia 30032-1304
(404) 294-2032

Fulton County Fire and Rescue Services
3977 Aviator Circle
Atlanta, Georgia 30336
(404) 505-5700

## Atlanta Fire and Rescue Departments: (404) 853-7000

| | |
|---|---|
| **2nd BATTALION** | 1711 Marietta Blvd. NW 30318 |
| **FIRE STATION 8** | 1711 Marietta Blvd. NW 30318 |
| **FIRE STATION 9** | 3501 M.L. King Jr., Dr. SW 30331 |
| **FIRE STATION 16** | 1048 Simpson Rd. NW 30314 |
| **FIRE STATION 22** | 817 Hollywood Rd. NW 30318 |
| **FIRE STATION 28** | 2040 Main St. NW 30318 |
| **FIRE STATION 38** | 2911 Bankhead Hwy. NW 30318 |
| | |
| **3rd BATTALION** | 170 10th St. NE 30309 |
| **FIRE STATION 1** | 71 Elliot St. SW 30313 |
| **FIRE STATION 4** | 125 Ellis St. NE 30303 |
| **FIRE STATION 12** | 1288 DeKalb Ave. NE 30307 |
| **FIRE STATION 15** | 170 10th St. NE 30309 |
| **FIRE STATION 23** | 1545 Howell Mill Rd. NW 30318 |

| | |
|---|---|
| **4th BATTALION** | 2825 Campbellton Rd. SW 30311 |
| **FIRE STATION 5** | 2825 Campbellton Rd. SW 30311 |
| **FIRE STATION 7** | 535 W. Whitehall St. SW 30310 |
| **FIRE STATION 14** | 1203 Lee St. SW 30310 |
| **FIRE STATION 17** | 1489 R.D. Abernathy Blvd. SW 30310 |
| **FIRE STATION 20** | 590 Manford Rd. SW 30310 |
| **FIRE STATION 25** | 2349 B.E. Mays Dr. SW 30311 |
| **FIRE STATION 31** | 2406 Fairburn Rd. SW 30331 |
| | |
| **5th BATTALION** | 447 Boulevard SE 30312 |
| **FIRE STATION 2** | 1568 Jonesboro Rd. SE 30315 |
| **FIRE STATION 10** | 447 Boulevard SE 30312 |
| **FIRE STATION 13** | 447 Flat Shoals Ave. SE 30316 |
| **FIRE STATION 18** | 2007 Oakview Rd. SE 30317 |
| **FIRE STATION 30** | 10 Cleveland Ave. SW 30331 |
| **FIRE STATION 34** | 3671 Southside Industrial Pkwy. SE 30354 |
| | |
| **6th BATTALION** | 3201 Roswell Rd. NE (30305) |
| **FIRE STATION 3** | 3500 Peachtree Rd. NE 30326 |
| **FIRE STATION 19** | 1063 N. Highland Ave. NE 30306 |
| **FIRE STATION 21** | 3201 Roswell Rd. NE 30305 |
| **FIRE STATION 26** | 2970 Howell Mill Rd. NW 30327 |
| **FIRE STATION 27** | 4260 Northside Dr. NW 30327 |
| **FIRE STATION 29** | 2167 Monroe Dr. NE 30324 |
| **FIRE STATION 39** | 4697 Wieuca Rd. NW 30342 |

## Local Red Cross Chapters

Metro Atlanta Chapter/Fulton Service Center
1955 Monroe Drive NE
Atlanta, Georgia 30324
Tel: (404) 876-3302 Fax: (404) 874-2993

East Metro Service Center
3486 Covington Highway
Decatur, Georgia 30032
Tel: (404) 296-0505
emetro@arcatl.org

Gwinnett Service Center
850 HI-Hope Road
Lawrenceville, GA 30043
Tel: (770) 963-9208
gwinnett@arcatl.org

Northwest Metro Service Center
324 Victory Drive
Marietta, GA 30060
Tel: (770) 428-2695
nwmetro@arcatl.org

South Metro Service Center
1115 Mount Zion Road
(formerly Morrow Industrial Boulevard)
Suite E
Morrow, GA 30260
Tel: (770) 961-2552
smetro@arcatl.org

## Acknowledgements

This document would not have been possible without he significant effort of the following Homeland Security Advisory Group (HSAG) members: William F. Brumund (HSAG Chairman), Jeffrey P. Colbath, David A. Lee, Mary A. Madden, Michael J. O'Leary, and Shawn D. Smith. The entire Homeland Security Advisory Group participated in the preparation of this document by providing reviews and comments on the draft. In addition, the following Metro Atlanta staff members of BENS were invaluable because of their encouragement and their assistance in working on this Primer: Conrad H. Busch and Aimee L. Yrlas. Thanks also go to Betty Triebert of Golder Associates for incorporating the many edits and revisions of the document and preparing the final document.

Thanks are also due to the support, encouragement, and review provided by numerous professionals in the Georgia Division of Public Health and the Centers for Disease Control and Prevention.

Printed February 2004