ALL-RISK AND ALL-HAZARD

TERRORISM RESPONSE:

A Checklist and Guide for Fire Chiefs and Community Preparedness Leaders

3RD EDITION

ROAD CLOSED

FBI
BOMB TECH

ATF
AGENT

IAFC
INTERNATIONAL
FIRE CHIEFS
ASSOCIATION
ORG 1873

www.iafc.org

IAFC Terrorism and Homeland Security Committee

To Fire Chiefs and Community Preparedness Leaders:

Welcome to the 3rd Edition of the International Association of Fire Chiefs' publication, *TERRORISM RESPONSE: A Checklist and Guide for Fire Chiefs and Community Preparedness Leaders.* This is a document by first responders (fire chiefs) for first responders following the attacks of September 11, 2001. It is designed to be comprehensive but succinct so that busy leaders may fully and effectively prepare their communities for acts of terrorism, whether foreign or domestic in origin.

Although terrorism was the genesis for the Checklist and Guide and the fire chief was the initial focus, two important points are very clear. One, communities can and should apply the Checklist and Guide to any and all risks that they might face. Two, the audience extends beyond the fire chief and includes local leaders in law enforcement, emergency management, emergency medical services, public health, public administration, public works, and even the private sector.

In addition to the re-emphasis on the all-risk and the multiple-discipline appeal of the Checklist and Guide, this 3rd Edition incorporates several other changes. The instructions have been modified and broadened to include other community preparedness disciplines. Also, the References are accessible through the IAFC web site, providing ease of access and timely updates as changes emerge.

A community stands to benefit greatly when all leaders and officials charged with local public safety and preparedness collectively embrace and use the Checklist and Guide. Working together, you can ensure that your community effectively addresses its risks of terrorism, flood, hurricane, tornado, blizzard, earthquake or any other relevant hazard through the assessment, prevention, preparedness, response and recovery concepts presented here.

When large-scale emergencies and disasters strike a community, they truly are local events. Life safety, treatment of the injured, control of the hazards, responder support and welfare, restoration of order and overall recovery depend on teamwork. We believe that *Terrorism Response: A Checklist and Guide for Fire Chiefs and Community Preparedness Leaders* can serve as an effective tool for fire chiefs and other public safety and emergency preparedness leaders to use jointly within any town, city or municipality that seeks guidance on terrorism and all-hazard preparedness.

TABLE OF CONTENTS

Additional references are available on the IAFC website at: www.iafc.org/hschecklist

INSTRUCTIONS FOR THE FIRE CHIEF AND OTHER COMMUNITY PREPAREDNESS LEADERS

General Information

The Checklist and Guide is designed to enable fire chiefs and other community preparedness leaders to assess, prevent, prepare for, respond to and recover from a terrorist attack or other local calamity. To provide a methodical, clear and comprehensive approach for the user, a Summary Checklist, How-To Guides and References are included.

The **Summary Checklist** outlines the most critical actions to assess, prevent, prepare for, respond to and recover from acts of terrorism. Community leaders may also use this Summary Checklist to perform similar preparedness actions for other relevant hazards and risks by substituting the targeted risk/hazard in place of "terrorist attack" in the checklist. Some risks of a natural threat, such as a tornado, are not preventable but may be mitigated by early warning, safe zones, and other local measures.

The objective in using the Summary Checklist is to accomplish all preparatory tasks in each category so that a completed check-off is possible. Of course, real-life changes in circumstances, threats, risks and even personnel call for periodic reviews of the checklist for each risk category to maintain currency.

The IAFC encourages every fire chief to reach out to the community's law enforcement colleagues and other local preparedness leaders (and vice versa) to establish priorities for each risk and the time frame within which a high degree of completion is to be accomplished. Fire chiefs whose departments have worked through the Checklist and Guide have found that 18 months is a reasonable amount of time to allot for this high degree of completion. Of course, each community will have to establish suitable timeframes for each hazard and risk; thereafter, periodic reviews, updates, drills and exercises will ensure overall community preparedness for terrorism and other local risks.

The **How-To Guides** provide detailed guidance for achieving a level of readiness that warrants a completed check-off. Some elements of the How-To Guides require periodic or ongoing efforts such as training and updating operating procedures. In those cases, a check-off may be appropriate when firm plans for such efforts are in place.

Following the Guide for each topical area, **references*** are listed to provide more detail for preparedness actions. Responsible fire department and community preparedness leaders should use other known and appropriate resources as well.

Instructions

To complete your reviews, we recommend the following:

- Assign this responsibility to one or more department members who are: (1) knowledgeable in terrorism and other emergency preparedness issues; and (2) are at levels to be able to communicate effectively with representatives of other disciplines.

- Consider partnering with another fire department and city/community department to provide mutual support and shared experience.

- Demonstrate your commitment by establishing timelines for completion, including periodic updates to keep you informed of your department's progress.

- Begin by assessing your readiness by checking off the appropriate boxes in the Summary Checklist and corresponding How-To Guides. The checkboxes are arranged according to three time intervals (initial check, mid-point check, and 18-month check) with three possible categories (not yet begun, underway, and complete). At each time interval, note which category applies to your level of readiness.

- Improve your readiness by taking appropriate steps to be able to check off more areas as "complete" at the next scheduled review.

- Keep all materials related to the Checklist and Guide in one place to facilitate subsequent reviews.

A completed checklist confirms your department and community have completed critical preparedness steps. At that point, you should continue your efforts by scheduling periodic updates to maintain readiness (e.g., every 24 months, after a major event occurs, and/or when core documents are updated). Checkboxes are provided for this purpose.

*References are intended to supply additional background or educational resources to support department efforts. They do not represent an IAFC endorsement of any entity's product or services."

SUMMARY CHECKLIST

To assess preparedness, Place appropriate number in each check box for each step described:

1 – Completed, 2 – Underway, 3 – Not yet begun

How to ASSESS Your Department's / Community's Capabilities

Initial Assessment	Mid-Point Assessment	18-Month Assessment	Follow-Up Assessment	
❏	❏	❏	❏	Target Hazards/Critical Infrastructure Protection
❏	❏	❏	❏	Community Risks/Special Events
❏	❏	❏	❏	Relationships/Partnerships/Mutual Aid/Automatic Aid
❏	❏	❏	❏	Intelligence-Sharing/Fusion Center Participation
❏	❏	❏	❏	Response Capabilities for Weapons of Mass Destruction/Chemical, Biological, Radiological, Nuclear and Explosive (CBRNE) Attacks
❏	❏	❏	❏	Cyber-Attack
❏	❏	❏	❏	Communication Plan (Interoperability)
❏	❏	❏	❏	Gap Analysis/Action Plan
❏	❏	❏	❏	Continuity of Operations/Continuity of Government Plan

How to Help PREVENT a Terrorist Attack

Initial Assessment	Mid-Point Assessment	18-Month Assessment	Follow-Up Assessment	
❏	❏	❏	❏	Terrorism Awareness/Recognition Training
❏	❏	❏	❏	Reporting Procedures/Information-Sharing
❏	❏	❏	❏	Security Clearances
❏	❏	❏	❏	Personnel/Facility Security/Critical Infrastructure Protection
❏	❏	❏	❏	Cyber-Security
❏	❏	❏	❏	Other Considerations

How to PREPARE Your Department / Community to Respond to a Terrorist Attack

❏	❏	❏	❏	Training/Drills/Exercises
❏	❏	❏	❏	Equipment
❏	❏	❏	❏	Standard Operating Procedures
❏	❏	❏	❏	Mutual Aid/Automatic Aid
❏	❏	❏	❏	National Incident Management System (NIMS) Adoption and Training
❏	❏	❏	❏	Emergency Operations Plan
❏	❏	❏	❏	Continuity of Operations/Continuity of Government Plans
❏	❏	❏	❏	24x7 Contacts/Resource List

Initial Assessment	Mid-Point Assessment	18-Month Assessment	Follow-Up Assessment	
❏	❏	❏	❏	Community Notification Plans
❏	❏	❏	❏	Evacuation/Shelter-in-Place Plans
❏	❏	❏	❏	Points of Distribution Plan
❏	❏	❏	❏	Citizen Involvement/Community Emergency Response Teams/Fire Corps/Reserve Medical Corps/USAOnWatch
❏	❏	❏	❏	Technical Rescue Response Sustainment
❏	❏	❏	❏	Fire Department and Public Safety Agency Member/Family Preparedness
❏	❏	❏	❏	Incident Access Control
❏	❏	❏	❏	Victim Care and Management/Mass Casualty Plan/Medical Surge Procedure
❏	❏	❏	❏	Mass Fatality Management Plans
❏	❏	❏	❏	Crime Scene Guidelines

How to RESPOND to a Terrorist Attack

❏	❏	❏	❏	Situational Awareness/Frequent Updates
❏	❏	❏	❏	National Incident Management System (NIMS)
❏	❏	❏	❏	Respond According to Standard Operating Procedures
❏	❏	❏	❏	Mutual Aid Agreements
❏	❏	❏	❏	Force Protection (Responder Safety)/Perimeter Security

Initial Assessment	Mid-Point Assessment	18-Month Assessment	Follow-Up Assessment	
❏	❏	❏	❏	Notifications
❏	❏	❏	❏	Media/Crisis Communication
❏	❏	❏	❏	Evacuation/Shelter-in-Place Management
❏	❏	❏	❏	Continued Service Delivery
❏	❏	❏	❏	Responder Safety and Wellness
❏	❏	❏	❏	Technical Response
❏	❏	❏	❏	Victim Care and Management / Mass Casualty Plan / Medical Surge Procedure
❏	❏	❏	❏	Citizen/Community Responders
❏	❏	❏	❏	Crime Scene Guidelines

How to RECOVER from a Terrorist Attack

❏	❏	❏	❏	Medical Screening Program for Responders
❏	❏	❏	❏	Documentation/Reporting
❏	❏	❏	❏	Fire Department/Community Resource Assessment
❏	❏	❏	❏	Post-Incident Analysis
❏	❏	❏	❏	Community Recovery
❏	❏	❏	❏	Media Relations

Guide to ASSESSING Threats and Capabilities

Target Hazards / Critical Infrastructure Protection

❏ IDENTIFY TARGET HAZARDS WITHIN THE COMMUNITY. For homeland security purposes, target hazards include the community's critical infrastructure and key resources, which if attacked would cause a large disruption in daily life, cripple public services and instill fear in local residents and the nation as a whole. Emergency-services agencies, including fire departments and communication centers, are part of the critical infrastructure.

  ❏ Private facilities such as chemical and nuclear plants, company headquarters, shopping malls, financial institutions, privately run healthcare facilities, sports venues, places of worship and private colleges and universities

  ❏ Public facilities such as post offices, emergency-services agencies, national monuments and icons, publicly run healthcare facilities and state or community colleges and universities

  ❏ Utilities such as water sources, including dams, reservoirs and water treatment plants; power generation and distribution facilities; and communication firms (including their transmission towers)

  ❏ Transportation modes such as highways and shipping facilities, bus depots, railway lines and stations, waterways and ports, and airports, with particular attention to portions where access and rescue will be most difficult (e.g., trestles over water and tunnels)

  ❏ Pipelines and bulk storage facilities such as natural gas lines, petroleum lines and tank farms

Community Risks / Special Events

❏ IDENTIFY OTHER COMMUNITY RISKS UNIQUE TO YOUR AREA, INCLUDING LOCAL SPECIAL EVENTS:

  ❏ Athletic events

  ❏ Ceremonies and parades

  ❏ State and local fairs

  ❏ Other annual or semi-annual events

❏ IN ADDITION TO ASSESSING THE THREAT OF A TERRORIST ATTACK, CONSIDER OTHER COMMON RISKS AND HAZARDS FOR WHICH THE CHECKLIST AND GUIDE MAY PROVE HELPFUL:

  ❏ Wildland fires

  ❏ Weather-related disasters such as hurricanes, floods, tornadoes, and blizzards

  ❏ Civil unrest

  ❏ Other local and regional threats

Relationships / Partnerships / Mutual Aid / Automatic Aid

❏ ESTABLISH RELATIONSHIPS AND PARTNERSHIPS WITH OTHER PUBLIC-SAFETY AGENCIES—particularly emergency management, law enforcement and non-fire-based EMS—and government leaders to learn what everyone's assets and capabilities are. Train and exercise together on a regular basis to enhance everyone's response capabilities. Participants should be:

  ❏ Local, state and federal law enforcement agencies

  ❏ Military response partners

  ❏ Public health agencies

  ❏ Mutual aid consortia

  ❏ Public works agencies

  ❏ Local and state elected officials

  ❏ Utilities such as electricity, water, sewer and gas

  ❏ Other regional resources that would respond to a terrorist attack

Intelligence Sharing / Fusion Center Participation

❏ ENGAGE IN INTELLIGENCE SHARING WITH LAW ENFORCEMENT AGENCIES TO ASSESS AND COMMUNICATE LOCAL RISKS ON AN ONGOING BASIS.

  ❏ Establish a secure system for receiving threat information from local, state and federal law enforcement agencies.

  ❏ Participate in local fusion center activities to facilitate communication with other public safety agencies on a regular basis. If your department does not have the resources to participate directly, build a relationship and communicate regularly with another fire and emergency service representative in the fusion center.

  ❏ Communicate with the FBI via your local FBI weapons of mass destruction (WMD) coordinator and the FBI's Joint Terrorism Task Force.

Guide to ASSESSING Threats and Capabilities cont

❏ **Response Capabilities for WMD / Chemical, Biological, Radiological, Nuclear and Explosive (CBRNE) Attacks**

    ❏ ASSESS YOUR DEPARTMENT'S/COMMUNITY'S ABILITY TO RESPOND TO THE POSSIBLE TYPES OF TERRORIST ATTACK, E.G., WEAPONS OF MASS DESTRUCTION (I.E., CBRNE).

        ❏ Assess your department's ability to identify the type of attack as well as your ability to mitigate it.

        ❏ Factor into your assessment the number of personnel available, as well as their training levels for such a response, the types of equipment your department has available and your response procedures.

        ❏ Assess your ability to maintain a response to a CBRNE attack for more than one operational period (e.g., 12, 24, 48, 72 hours).

❏ **Cyber-Attack**

    ❏ DEFINE WHAT COULD HAPPEN TO YOUR DEPARTMENT AND YOUR COMMUNITY DURING A CYBER-ATTACK, and assess your department's ability to withstand such an attack. Decide how you will communicate information if a cyber-attack or breach of information technology security occurs.

❏ **Communication Plan (Interoperability)**

    ❏ CREATE AND IMPLEMENT AN EFFECTIVE COMMUNICATION PLAN, INCLUDING THE OPERABILITY OF YOUR SYSTEM AND THE INTEROPERABILITY OF YOUR SYSTEMS WITH THOSE OF OTHER AGENCIES.

        ❏ Decide how you will alert your members, other agencies, government officials and the general public about a terrorist attack.

        ❏ Decide how you will communicate information on a local, regional, state and federal basis.

        ❏ Decide who will communicate such information, how it will be communicated (e.g., voice, data, or audio), to whom and why.

        ❏ Assess your department's wireless voice and data system to make sure it will continue to function properly.

        ❏ Work with service providers to build contingency plans.

❏ **Gap Analysis / Action Plan**

    ❏ DEVELOP A GAP ANALYSIS THAT MEASURES THE COMMUNITY'S RISK AGAINST YOUR DEPARTMENT'S ABILITY TO RESPOND. Determine which gaps your department will need to fill and which you will need to work around.

        ❏ Develop an action plan to fill necessary gaps either internally or through mutual aid and to accommodate gaps that will not be filled.
        ❏ Develop a system to update this analysis and plan on an annual basis.

❏ **Continuity of Operations Plan / Continuity of Government Plan**

    ❏ ASSESS YOUR DEPARTMENT'S/COMMUNITY'S CONTINUITY OF OPERATIONS PLAN AS WELL AS YOUR COMMUNITY'S CONTINUITY OF GOVERNMENT PLAN, IF SUCH PLANS EXIST, TO MAKE SURE THEY WILL SECURE A CONTINUITY OF ESSENTIAL FUNCTIONS IF ANY SECTION, INCLUDING LEADERSHIP, BECOMES DISABLED AFTER A TERRORIST ATTACK.

> **NOTE:** In the past, for states to obtain federal funding for terrorism response—and for the states to pass that money to the localities—the states needed to comply with programs established under Homeland Security Presidential Directive/HSPD-8. HSPD-8 directed the federal government to establish and achieve an all-hazards national-preparedness goal. When preparing to respond to a terrorist attack, communities needed to measure their capabilities against these requirements. To assist in this process, the U.S. Department of Homeland Security created the Target Capabilities List (TCL) and Universal Task List. DHS measured capabilities against the National Preparedness Guidelines and 15 national planning scenarios.
>
> Presidential Policy Directive /PPD-8 on national preparedness has replaced HSPD-8 but is meant to reaffirm its general policy direction as well as that of the 2006 Post-Katrina Emergency Management Reform Act (PKEMRA) and 2009 National Infrastructure Protection Plan (NIPP).
>
> PPD-8 retains the all-hazards, risk-based approach of HSPD-8, though it uses four categories of hazards: terrorism, catastrophic natural disasters, cyber attacks and pandemics.
>
> Other significant changes from previous directives are:
>
>   ❏ Strong emphasis on an "all-of-nation," "all-hazards" approach that fuses federal, state and local response (including the private sector)
>
>   ❏ Capability-based planning that is similar to the TCL but emphasizes flexibility in planning and response
>
>   ❏ Measureable, specific goals (including a comprehensive assessment strategy)
>
>   ❏ Re-focusing government resources on mitigation and resilience
>
>   ❏ Reducing the burden of heavy paperwork and other requirements
>
> *PPD-8 was in the development process at the time of this revision. Please visit www.dhs.gov for more information.*

References for ASSESSING Threats and Capabilities

❏ **Chemical, Biological, Radiological, Nuclear and Explosive Attacks**

❏ www.mipt.org

The Memorial Institute for the Prevention of Terrorism provides access to descriptions of various types of terrorist attacks. A password is required but available free of charge to public-safety personnel.

❏ **Continuity of Operations Plans**

❏ FEMA Continuity of Operations Programs, www.fema.gov/government/coop/index.shtm

❏ **Critical Infrastructure Protection**

❏ Emergency Management and Response – Information Sharing and Analysis Center (EMR ISAC) www.usfa.dhs.gov/fireservice/subjects/emr-isac/index.shtm

❏ National Infrastructure Protection Plan, www.dhs.gov/nipp

❏ Sector-Specific Plans www.dhs.gov/files/programs/gc_1179866197607.shtm

❏ DHS National Infrastructure Coordinating Center

(NICC), E-Mail: nicc@dhs.gov

Part of the National Operations Center, the NICC monitors the nation's critical infrastructure and key resources on an ongoing basis. During an incident, the NICC coordinates information-sharing among infrastructure and key resource sectors.

❏ **Federal Bureau of Investigation**

❏ Field Office Locator, www.fbi.gov/contact/fo/fo.htm

Once you begin to work with your FBI WMD coordinator, you will gain access to law enforcement information on the FBI's website, including intelligence bulletins and investigator guides.

❏ **Gap Analysis**

❏ Emergency Management Accreditation Program (National Fire Protection Association 1600), www.emaponline.org

❏ **National Planning Guides**

❏ 15 National Planning Scenarios, www.llis.gov

(A password is necessary but available free of charge to public safety agencies.)

❏ National Preparedness Guidelines, http://www.fema.gov/pdf/emergency/nrf/National_Preparedness_Guidelines.pdf

❏ National Response Framework Resource Center, www.fema.gov/emergency/nrf/

❏ Naval Postgraduate School Homeland Security Digital Library, www.hsdl.org

❏ Target Capabilities List, www.llis.gov

❏ Universal Task List, www.llis.gov

❏ Responder Knowledge Base, www.rkb.us

❏ **NIMSCAST**

❏ NIMS Compliance Assistance Support Tool, www.fema.gov/nimscast/

* Please remember to visit www.IAFC.org/hschecklist for the most up-to-date information

Guide to Helping PREVENT a Terrorist Attack

❏ **Terrorism Awareness / Recognition Training**

❏ ADOPT AND PROVIDE A TERRORISM-AWARENESS TRAINING PROGRAM FOR FIRE DEPARTMENT/ PUBLIC SAFETY AGENCY MEMBERS AND THE PUBLIC ON HOW TO RECOGNIZE POTENTIAL TERRORIST ACTIVITY WITHIN THE COMMUNITY.

❏ TRAIN MEMBERS TO UNDERSTAND THE TERRORIST THREAT TO THE COMMUNITY AND WHAT IMPACT THAT THREAT HAS ON YOUR PERSONNEL IN TERMS OF BEING BOTH RESPONDERS AND POTENTIAL VICTIMS.

❏ Make sure members understand they are potential targets of primary and secondary (or further) attacks. Train them to look for secondary explosive devices or other terrorist threats on scene.

❏ Educate members to identify what constitutes suspicious behavior and to report suspicious activity within the community (or within the department) during day-to-day operations and when off duty, as they are in a unique position to observe community activities on a daily basis. (The Terrorism Liaison Officer (TLO) program is a useful tool.)

❏ Work with local law enforcement agencies to train the public on observing and reporting suspicious activity within the community.

❏ Collaborate with local, state and federal law enforcement agencies; non-fire-based EMS systems; public health agencies; hospitals; public works departments; and other relevant community groups to understand and expand each other's roles in preventing a terrorist attack.

❏ **Reporting Procedures / Information-Sharing**

❏ DEVELOP AND IMPLEMENT PROTOCOLS FOR RECEIVING AND REPORTING TERRORIST THREAT INFORMATION.

❏ Establish a protocol for receiving terrorist threat information from local, state and federal law enforcement agencies. Make sure the information will be secure, so law enforcement officials are comfortable sharing information with you.

❏ Distribute appropriate threat information to department members on an as-needed basis.

❏ Consider notifying mutual aid partners of appropriate threat information.

❏ Establish a standard operating procedure for vetting and reporting information on suspicious activity department members observe in the community and within your department to law-enforcement agencies at all levels, including your local/regional FBI office.

❏ Work with local law enforcement agencies to establish a community reporting system, such as a dedicated phone number, for the public to report suspicious activity.

❏ Where appropriate, work to obtain representation in local fusion centers, and/or request regular briefings from local Joint Terrorism Task Forces (JTTFs).

❏ Security Clearances

❏ AN EFFECTIVE COMMITMENT TO ASSESS, PREVENT, PREPARE FOR, RESPOND TO, AND RECOVER FROM ATTACKS OF TERRORISM REQUIRES SECURITY CLEARANCES ONLY IN RARE INSTANCES. WORK WITH LOCAL, STATE AND FEDERAL LAW ENFORCEMENT AGENCIES TO OBTAIN SECURITY CLEARANCES FOR DESIGNATED PERSONNEL WHEN NECESSARY (FOR EXAMPLE, WHEN WORKING IN A FUSION CENTER).

❏ BUILD AND MAINTAIN STRONG WORKING RELATIONSHIPS WITH LOCAL, STATE AND FEDERAL PARTNERS TO ENSURE TIMELY INFORMATION-SHARING REGARDING THREATS AND RISKS.

❏ Department Personnel / Facility Security / Critical Infrastructure Protection

❏ DEVELOP AND IMPLEMENT PROTOCOLS FOR SECURING DEPARTMENTAL PERSONNEL, FACILITIES, INFRASTRUCTURE AND OPERATIONS.

　❏ Conduct background checks on all personnel according to applicable law.

　❏ Issue and require the use of identification cards for all personnel.

　❏ Properly secure all facilities, dispatch areas and radio towers.

　❏ Establish and implement a visitor policy.

　❏ Secure all uniforms, badges, communications equipment and gear.

　❏ Ensure the security of all secondary areas, such as fuel and other supplies, warehouses and repair shops.

　❏ Ensure sensitive files are locked.

　❏ Secure intelligence information received from law enforcement sources. Security should extend to receiving, storing, and disposal of information.

❏ Information Technology and Cyber-Security

❏ STRENGTHEN YOUR DEPARTMENT'S/COMMUNITY'S ABILITY TO WITHSTAND A CYBER-ATTACK AND SAFEGUARD SENSITIVE INFORMATION:

　❏ Adhere to IT standards, including the use of personal passwords.

　❏ Do not post more information on your department's website or on other sites than is necessary. In particular, do not post pictures of or specific information about critical structures within your community.

　❏ Ensure sensitive electronic files are "locked".

　❏ Secure intelligence information received from law enforcement sources. Security should extend to receiving, storing, and disposal of information.

　❏ Develop a means of communication that does not require information technology or mass-communication methods, such as a messenger service.

References for Helping PREVENT a Terrorist Attack

❏ **If You See Something, Say Something ™ Campaign**

　❏ www.dhs.gov/files/reportincidents/see-something-say-something.shtm

❏ **Information Technology Standards**

　❏ National Institute of Standards and Technology's Information Security Handbook, http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf

　❏ NCTC Worldwide IncidentsTracking System, https://wits.nctc.gov

　❏ Recognize Potential Terrorism, www.fbi.gov/page2/aug04/preventterror080204.htm

　❏ Security Clearances,

❏ **Model Fire, Building, Life Safety and Associated Codes and Standards (nationally recognized)**

　❏ National Fire Protection Association, www.nfpa.org

　❏ International Code Council, www.iccsafe.org

❏ **Ready.gov**

　❏ www.ready.gov

❏ **State and Local Fusion Centers**

　❏ Interagency Threat Assessment and Coordination Group (ITACG), www.ise.gov/interagency-threat-assessment-and-coordination-group-itacg

❏ **Terrorism Liaison Officers**

　❏ www.tlo.org

* Please remember to visit www.IAFC.org/hschecklist for the most up-to-date information

Guide to PREPARING Your Department / Community to Respond to a Terrorist Attack

❏ Training / Drills / Exercises

❏ CREATE PLANS TO COORDINATE AND PARTICIPATE IN TRAINING, DRILLS AND EXERCISES ON A REGULAR BASIS. USE THE RESULTS AND LESSONS LEARNED TO MODIFY DEPARTMENTAL AND COMMUNITY PLANS AS NECESSARY.

　❏ Conduct these activities within your department and with stakeholders at the local, regional and federal levels.

　❏ Conduct a combination of tabletop, functional and full-scale exercises, depending on the time and resources available.

　❏ Relate these activities to the terrorist threats facing your community.

　❏ Adhere to appropriate federal guidelines and incident command structure for responding to a terrorist attack. (Please see the references for more information.)

❏ Equipment

❏ PROCURE OR MAKE SURE YOUR DEPARTMENT/COMMUNITY HAS ACCESS TO THE PROPER EQUIPMENT TO RESPOND TO A CBRNE ATTACK. Sustain this equipment by testing, maintaining and replacing the equipment as necessary.

　❏ Ensure equipment is appropriate for responding to WMDs and hazardous materials emergencies.

　❏ Ensure equipment is available to protect responders from WMDs and secondary attacks; respiratory protection is of particular importance.

　❏ Ensure communications equipment is available to allow for operability within the department and interoperability with other agencies and government officials. Exercise equipment regularly.

　❏ Pursue grant funding from local, state and federal government sources or private sources to procure and sustain terrorism-response equipment as needed.

❏ Standard Operating Procedures (SOPs)

❏ IMPLEMENT STANDARD OPERATING PROCEDURES FOR YOUR DEPARTMENT/COMMUNITY TO RESPOND TO A TERRORIST ATTACK.

　❏ Target your SOPs to include a CBRNE attack, including detecting the hazard and determining its strength and location, decontamination, management of multiple casualties and victim care and management.

　❏ Implement SOPs on exposure reporting for first responders.

　❏ Implement specific and comprehensive SOPs for voice, data and video communications, including alternate methods in the event mainstream communications capabilities are lost.

　❏ Implement specific and comprehensive SOPs for maintaining responder safety, including action regarding improvised explosive devices and other secondary attacks meant to harm responders.

　❏ Implement specific and comprehensive SOPs for interacting with the media and communicating information to the public, including appointing a public information officer (PIO) and participating with other public safety agencies in a joint information center (JIC).

　❏ Implement an SOP for the protection of sensitive information during verbal communications.

Guide to PREPARING Your Department / Community to Respond to a Terrorist Attack cont

❏ **Mutual Aid / Automatic Aid**

    ❏ ENTER INTO MUTUAL AID AND AUTOMATIC AID AGREEMENTS WITH OTHER FIRE DEPARTMENTS/ PUBLIC SAFETY AGENCIES IN THE REGION TO MAKE SURE YOUR DEPARTMENT HAS ACCESS TO ANY EQUIPMENT, PERSONNEL OR FACILITIES YOU MIGHT NEED (AS IDENTIFIED IN YOUR GAP ANALYSIS).

        ❏ Put all agreements in writing.

        ❏ Define a trigger point for requesting mutual aid.

        ❏ Consider using a standardized system to identify the type of equipment needed, the location and other relevant information.

        ❏ Ensure all internal and external responders have interoperable communication.

        ❏ Learn the local, state and federal reimbursement policies and consider using template reimbursement forms.

        ❏ Train and exercise with mutual aid partners on a regular basis (annually at a minimum).

    ❏ UNDERSTAND THE RESOURCES TO WHICH STATE GOVERNORS HAVE ACCESS.

        ❏ Coordinate with your state governor's homeland security coordinator as well as with the state's National Guard (NG) adjutant general.

        ❏ Coordinate with the state fire marshal's office or designated state fire official.

        ❏ Understand the role of the federal government. If the president declares a disaster or emergency (at the request of a state governor), the National Response Framework dictates the federal government response. (Please see the references for more information.)

> **NOTE:** Governors may request aid from other states through the Emergency Management Assistance Compact (EMAC). The EMAC is a structured mutual aid system among the states that is meant to provide quick and efficient response. It encourages participation by resolving the issues of liability and reimbursement. Governors also have access to their own National Guard and may request assistance from the NG in other states. In addition, governors may request logistical and other resource support from U.S. Northern Command, a branch of the U.S. military.
>
> *Please see the references for more information

❏ **National Incident Management System (NIMS) Adoption and Training**

    ❏ ADOPT AND TRAIN ALL PERSONNEL IN USE OF THE NIMS AND USE IT FOR EACH AND EVERY RESPONSE.

        ❏ Emphasize the use of Unified Command in actual incidents (where appropriate), training and exercises. (See the NIMS for more detail.)

        ❏ Develop a mechanism within your department/community to sustain command (e.g., rotating the incident commander on prolonged incidents).

        ❏ Explore the availability and capability of an incident management team (IMT) within your community and develop plans as appropriate. (More information on IMTs is available in the reference section below).

        ❏ Encourage and assist with training of all city/community agencies, including hospitals, in the NIMS.

        ❏ Your fire department needs to be the center of preparedness for your community.

> **NOTES:** Relationship-building prior to an incident is critical to a well-functioning unified command. Of particular importance is deciding ahead of time who will be in charge at each step of the response—the first among equals— to avoid conflict over authority at the scene.

❏ **Emergency Operations Plan (EOP)**

    ❏ UNDERSTAND YOUR DEPARTMENT'S ROLE IN THE LOCAL (TOWN/CITY/COUNTY), REGIONAL AND STATE EOPS. GOVERNMENTS AT EACH OF THESE LEVELS SHOULD HAVE AN EOP TO COORDINATE THEIR RESPONSE TO A TERRORIST ATTACK. YOUR DEPARTMENT/COMMUNITY SHOULD BE INVOLVED IN CRAFTING THESE EOPS TO MAKE SURE THEY ACCURATELY REFLECT YOUR ABILITIES.

Guide to PREPARING Your Department / Community to Respond to a Terrorist Attack cont

❏ **Continuity of Operations (COOP) / Continuity of Government Plans**

❏ DEVELOP A COOP PLAN IN THE EVENT ANY SECTION OF YOUR DEPARTMENT/COMMUNITY, INCLUDING ITS LEADERSHIP, BECOMES DISABLED, TO ENSURE A CONTINUITY OF ESSENTIAL FUNCTIONS.

   ❏ Review each of your purchase agreements prior to an event to make sure they will meet your needs, and arrange for appropriate backup vendors.

   ❏ Establish an emergency procurement policy in case you need to purchase or lease additional or replacement equipment or apparatus. Determine what the triggers will be for using the policy and for returning to your department's standard procurement system.

   ❏ Arrange to have a number of different vendors available for any equipment or apparatus you might need.

   ❏ Create a succession plan for the leadership of your department. Consider arranging for leaders of other community agencies to step in on a temporary basis.

   ❏ Chart the staffing levels necessary for each critical function of your department and the skill sets your members possess. Determine how you would be able to assign some members to cover different functions if necessary.

   ❏ Prepare to adjust shift schedules to accommodate a long-term response (e.g., moving from 24-hour shifts to 12-hour shifts or making other shift changes as appropriate).

   ❏ Create a list of your department's service priorities so you can curtail or temporarily suspend certain functions as necessary. For example, when responding to a terrorist attack, your department most likely will suspend non-emergency fire prevention and training activities. Also, consider establishing additional screening and response procedures to modify routine EMS responses, such as transportation for minor illnesses and injuries.

   ❏ Arrange for alternate locations for any displaced operations.

   ❏ Work with private and public utility companies to determine how your department will have continued access to water and power.

❏ STORE COPIES OF YOUR COOP PLAN AND OTHER CRITICAL FILES IN A SAFE PLACE (OR SAFE PLACES), IN CASE YOUR FACILITIES BECOME DISABLED.

❏ FAMILIARIZE YOUR DEPARTMENT'S LEADERSHIP AND THE LEADERSHIP OF OTHER AGENCIES WITH THE LOCAL GOVERNMENT HIERARCHY AS WELL AS THE GOVERNMENT'S CONTINUITY OF GOVERNMENT PLAN, WHICH SHOULD ENSURE THE CONTINUATION OF ESSENTIAL GOVERNMENT FUNCTIONS IF ANY PART OF THE LEADERSHIP BECOMES DISABLED.

❏ **24x7 Contacts / Resource List**

❏ MAINTAIN A LIST OF CONTACTS AND RESOURCES THAT YOUR DEPARTMENT MAY CONTACT 24 HOURS A DAY, 7 DAYS A WEEK AFTER A TERRORIST ATTACK.

   ❏ Include government leaders, heads of other public safety agencies, other community partners and resources such as vendors.

   ❏ Update this list on a regular basis or use an automated system (e.g., the water-utility representative at the emergency operations center). (See Appendix A for sample contact lists.)

❏ **Community Notification Plans**

❏ WORK WITH LOCAL LAW ENFORCEMENT AGENCIES, LOCAL GOVERNMENT LEADERS AND LOCAL MEDIA OUTLETS TO ESTABLISH A COMMUNITY NOTIFICATION SYSTEM ON TERRORIST THREATS (e.g., reverse 9-1-1, television and radio alerts via the Emergency Broadcast System, Amber alerts).

   ❏ Assess the technology that is available to distribute such notifications, including private cell-phone companies.

   ❏ Factor in any potential language or other communications barriers (e.g., those who do not speak fluent English or those who are deaf).

   ❏ Consider using pre-worded messages.

❏ **Evacuation / Shelter-in-Place Plan**

❏ DEVELOP AN EVACUATION PLAN WITH LOCAL LAW ENFORCEMENT AND OTHER APPROPRIATE AGENCIES, INCLUDING LOCAL/REGIONAL PUBLIC TRANSPORTATION DEPARTMENTS

   ❏ Consider who will need to be evacuated, including those who will require assistance. Plan to check all occupancies in areas that are likely to be affected by the terrorist attack (e.g., those who are downwind of an attack).

   ❏ Identify in advance special-needs individuals and facilities (e.g., convalescent homes).

   ❏ Plan how to evacuate them (e.g., personal vehicles, buses or other transportation modes).

   ❏ Designate shelters to house the evacuees and plan to identify building wardens.

   ❏ Determine when sheltering-in-place would be appropriate and how to communicate with those who are doing so.

   ❏ Practice formulating evacuation notices and sheltering procedures.

   ❏ Work with other public safety agencies to educate the public about evacuations and sheltering-in-place.

   ❏ Work with appropriate animal-welfare agencies on procedures for evacuating or sheltering large animals and house pets.

Guide to PREPARING Your Department / Community to Respond to a Terrorist Attack cont

❏ **Points of Distribution (POD) Plan**

   ❏ COORDINATE WITH LOCAL PUBLIC HEALTH OFFICIALS TO ESTABLISH PODS FOR MASS PROPHYLAXIS.

      ❏ Work with local law enforcement agencies to establish force protection in POD areas.

      ❏ Work with public health officials to establish a system of distributing prophylaxis to fire department families.

❏ **Citizen Involvement/Community Emergency Response Teams (CERT) / Fire Corps / Medical Reserve Corps / USAOnWatch**

   ❏ COORDINATE CITIZEN INVOLVEMENT IN DEPARTMENT/ COMMUNITY/PUBLIC SAFETY ACTIVITIES THROUGH LOCAL CITIZEN GROUPS, CERT PROGRAMS. (MORE INFORMATION IS AVAILABLE IN THE REFERENCE SECTION).

      ❏ Members of these groups may assist your department in public education, preparedness and response.

      ❏ Provide adequate training and regularly scheduled exercises.

❏ **Technical Rescue Response Sustainment**

   ❏ PLAN TO INCORPORATE THE TECHNICAL RESPONSE THAT WILL BE NECESSARY.

      ❏ Plan to obtain any needed specialty responses (e.g., heavy equipment, steel workers, search cameras, urban search and rescue teams).

      ❏ Plan to manage convergent volunteers (volunteers who spontaneously offer their help in the wake of a disaster).

❏ **Fire Department / Public Safety Agency Member / Family Preparedness**

   ❏ ENSURE THAT FIRE DEPARTMENT/PUBLIC SAFETY AGENCY MEMBERS AND THEIR FAMILIES ARE PREPARED FOR A TERRORIST ATTACK.

      ❏ Prepare members for what they will witness in the aftermath of a terrorist attack.

      ❏ Make sure members are physically prepared to respond to a terrorist attack by implementing appropriate wellness/fitness programs.

      ❏ Implement a critical incident stress management (CISM) program. (More information on CISM is available in the reference section).

      ❏ Determine how to provide appropriate information to the families of department members who are responding to a terrorist attack or who may be victims. Consider establishing dedicated telephone numbers for family members to call for information. Also consider partnering with a sister fire department that would act as a clearinghouse for family information.

      ❏ Teach members the circumstances under which they would need to evacuate (including why, how and to where) or shelter-in-place (including why and for how long). Teach them how to prepare their homes for sheltering-in-place (e.g., stocking adequate food, water and medical supplies to last for one week).

❏ **Incident Access Control**

   ❏ PREPARE TO CONTROL ACCESS TO THE INCIDENT SCENE.

      ❏ Determine and implement the credentials to require of anyone responding to the scene. Some states define the credentials required for firefighting and other rescue activities.

      ❏ Learn and follow your state's law in this area. If your state does not have specific requirements, determine what your department's requirements will be.

      ❏ Work with local law enforcement agencies to prepare for perimeter control and responder security.

Guide to PREPARING Your Department / Community to Respond to a Terrorist Attack cont

❏ **Victim Care and Management / Mass Casualty Plan / Medical Surge Procedure**

  ❏ PLAN TO MANAGE AND CARE FOR MASS CASUALTIES AND EMPLOY PROCEDURES TO IMPLEMENT MASS DECONTAMINATION AND ADMINISTER MASS PROPHYLAXIS.

    ❏ Work with law enforcement officials, your local medical director and other local health officers on a plan to keep victims within the area of the attack, if necessary.

    ❏ Work with public health officials on a plan to collect, quarantine, isolate and assess victims.

    ❏ Consider using patient tracking technology.

    ❏ Work with law enforcement agencies on a plan to keep treatment areas secure.

    ❏ Work with law enforcement and other agencies on a plan to connect family members, particularly children who become separated from their parents.

❏ **Mass Fatality Management Plans**

  ❏ PREPARE TO MANAGE MASS FATALITIES.

    ❏ Understand the priorities of your local medical examiner and plan accordingly. Discuss possible use of the Disaster Mortuary Operational Response Team (DMORT) program for assistance.

    ❏ Also discuss the need to have sufficient refrigeration units on hand.

    ❏ Arrange for your local ministerial alliance to be available.

    ❏ Include local funeral directors, along with their state associations, in planning.

❏ **Crime Scene Guidelines**

  ❏ ESTABLISH SOPS FOR RESPONDING TO A CRIME SCENE.

    ❏ The scene of a terrorist attack will be a crime scene, requiring evidence-handling protocols and other special considerations.

    ❏ Work with law enforcement agencies to develop appropriate procedures for your department.

References for PREPARING Your Department / Community to Respond to a Terrorist Attack

❏ **Citizen Involvement**

  ❏ Community Emergency Response Team (CERT) Program, www.citizencorps.gov/cert/

  ❏ Fire Corps, www.firecorps.org

  ❏ Medical Reserve Corps, www.medicalreservecorps.gov

  ❏ USAOnWatch, www.usaonwatch.org

❏ **Community Readiness**

  ❏ www.ready.gov

❏ **Continuity of Operations Plans**

  ❏ FEMA Continuity of Operations (COOP) Programs, www.fema.gov/government/coop/index.shtm

❏ **Disaster Mortuary Operational Response Teams**

  ❏ www.dmort.org

❏ **Exposure Reporting**

  ❏ International Association of Fire Fighters, www.iaff.org/HS/Resi/infdis/How_should_exposures_be_reported.htm

❏ **Family Support Planning**

  ❏ FEMA's COOP Planning, www.fema.gov/government/coop/index.shtm

❏ **First Responder Grants**

  ❏ FIRE and SAFER grant information www.fema.gov/firegrants/

  ❏ Grants and Assistance Programs for Emergency Personnel, www.fema.gov/emergency/grant.shtm

❏ **Member and Family Preparedness**

  ❏ Federal Disaster Assistance, www.disasterhelp.gov

  ❏ Federal Emergency Management Agency, www.fema.gov

  ❏ Federal "Ready" Program, www.Ready.gov

❏ **Mutual Aid**

  ❏ Emergency Management Assessment Compact (EMAC), www.emacweb.org

  ❏ Guidance and Sample Agreements – International Association of Fire Chiefs, www.iafc.org/mutualaid

❏ **National Fire Academy Courses on Response to Terrorism and Emergencies**

  ❏ www.usfa.dhs.gov/nfa/

❏ **National Incident Management System**

  ❏ NIMS Integration Center, www.fema.gov/emergency/nims/index.shtm

❏ **National Response Framework**

  ❏ www.fema.gov/emergency/nrf/

❏ **National Terrorism Advisory System**

  ❏ www.dhs.gov/files/programs/ntas.shtm

❏ **Patient Tracking Technology**

  ❏ EMS Magazine's Resource Guide: Technology in EMS - Patient Tracking Systems, www.emsworld.com/print/EMS-World/EMS-Magazines-Resource-Guide

  ❏ Seattle Fire Department Case Study, www.intermec.com/learning/content_library/case_studies/cs1940.aspx

❏ **Preparing for Disaster for People with Disabilities and Other Special Needs**

  ❏ FEMA Resource Record Details, www.fema.gov/library/viewRecord.do?id=1442

❏ **Responder Safety**

  ❏ RAND Science and Technology Policy Institute, Protecting Emergency Responders: Lessons Learned from Terrorist Attacks, conference report issued 2002, www.rand.org/pubs/conf_proceedings/2006/CF176.pdf

  ❏ National Fire Fighter Near Miss Reporting System, www.firefighternearmiss.com

  ❏ National Strategy for Homeland Security, www.whitehouse.gov/homeland/book/

❏ **Standards, Training and Grant Information for Emergency Responders**

  ❏ Responder knowledge Base, www.rkb.us

    A login name and password are required but are available free of charge to public safety agencies.

References for PREPARING Your Department / Community to Respond to a Terrorist Attack

❏ **State and Federal Resources**

❏ Emergency Management Assistance Compact, www.emacweb.org

❏ National Guard Chemical, Biological, Radiological, Nuclear, and Explosive (CBRNE) Enhanced Response Force Package (CERFP)

❏ National Guard Civil Support Team, www.ngb.army.mil/features/HomelandDefense/cst/factsheet.html

❏ National Response Framework, www.fema.gov/emergency/nrf/

❏ U.S. Northern Command, www.northcom.mil

❏ U.S. Fire Administration AHIMT Technical Assistance Program, www.usfa.dhs.gov/fireservice/subjects/incident/imt/index.shtm

❏ **Training**

❏ Homeland Security Exercise and Evaluation Program, https://hseep.dhs.gov

❏ U.S. Bomb Data Center - Bomb Arson Tracking System (BATS) link to an online video about the database, www.iafc.org/Programs/index.cfm?navItemNumber=569

❏ **Wellness/Fitness**

❏ Guide to Implementing the IAFC/IAFF Fire Service, Joint Labor Management, Wellness/Fitness Initiative, Specially Designed for Small and Medium-Sized Fire

Departments, www.iafc.org/files/wellness_fitness_smfd.pdf

❏ Health and Wellness Guide for the Volunteer Fire Service and Emergency Services, www.usfa.dhs.gov/downloads/pdf/publications/fa_321.pdf

*Please remember to visit www.IAFC.org/hschecklist for the most up-to-date information

Guide to RESPONDING to a Terrorist Attack

This guide represents tasks that your department/community public safety agency should be prepared to do during a response to a terrorist attack. As such, they closely mirror the guide to preparedness. You must have adequate procedures in place for each of these items before an attack hits.

❏ **Situational Awareness / Frequent Updates**

❏ ESTABLISH SITUATIONAL AWARENESS ON SCENE AND COMMUNICATE FREQUENT UPDATES TO THE DISPATCH/COMMAND CENTER.

❏ Identify the hazard in the emergency situation at hand.

❏ Initiate on-scene assessments in coordination with local law enforcement agencies, emergency management officials and other experts to ensure scene security and responder safety, including that no secondary devices or contaminants are on site.

❏ Coordinate the incident command post with the local emergency operations center by sharing up-to-date information on a regular basis.

❏ Conduct on-scene briefings frequently (throughout multiple operational periods) to communicate the common operating picture to responders.

❏ Share and compare information from the local scene with state and federal partners, establishing local, regional and national awareness based on the specific attack and intelligence/information that is available from other areas.

❏ **National Incident Management System**

❏ UTILIZE NIMS. YOUR DEPARTMENT/COMMUNITY SHOULD BE USING NIMS FOR DAY-TO-DAY EVENTS. USING NIMS DURING A RESPONSE TO A TERRORIST ATTACK WILL COORDINATE THE MANY RESOURCES YOU WILL NEED. RESPOND ACCORDING TO LOCAL SOPS.

❏ The type of response will depend on the type of incident: chemical, biological, radiological, nuclear or explosive, or a combination thereof.

❏ Prepare for multiple operational periods. After responding to the initial attack, your department may need to sustain its service delivery at the scene over a long period of time.

❏ Adjust on-scene resource levels as circumstances change.

❏ Consider a temporary change in shift lengths (e.g., from 24 to 12 hours) or other changes that are appropriate to meet the needs of the incident and continuity of operations.

Guide to RESPONDING to a
Terrorist Attack cont

❏ Mutual Aid Agreements

- ❏ UTILIZE YOUR MUTUAL AID AGREEMENTS.
    - ❏ Activate local, regional, state and interstate agreements.
    - ❏ Request a sufficient number of resources to ensure an adequate response to the incident. Do not hesitate.
    - ❏ Assign a department member or officer to each mutual aid crew to act as a guide.
    - ❏ Coordinate and control mutual aid resources.
    - ❏ Manage self-dispatched resources as appropriate.

❏ Force Protection (Responder Safety) / Perimeter Security

- ❏ WORK WITH LAW ENFORCEMENT AGENCIES TO ENSURE FORCE PROTECTION (RESPONDER SAFETY) AND PERIMETER SECURITY.
    - ❏ Establish entry points to the scene.
    - ❏ Enforce your predetermined credentialing system.
    - ❏ Erect fencing or other barriers with assistance from public works personnel.
    - ❏ Assign lookouts for potential secondary devices or attacks.
    - ❏ Control and maintain ingress and egress routes to and from the scene.
    - ❏ Establish airspace restrictions over the scene.
    - ❏ Manage convergent responders and volunteers.

❏ Notifications

- ❏ MAKE NECESSARY NOTIFICATIONS TO:
    - ❏ Local, state and regional law enforcement officials
    - ❏ Federal officials through your local/regional FBI office
    - ❏ Local elected officials
    - ❏ Fire department members
    - ❏ All partner agencies
    - ❏ All municipal services

❏ Media / Crisis Communication

- ❏ UTILIZE YOUR MEDIA AND CRISIS COMMUNICATIONS PLANS.
    - ❏ Appoint a PIO as soon as possible.
    - ❏ Participate in the activities of the JIC, if one is established.
    - ❏ Use your community notification system as necessary in conjunction with emergency management officials. Include instructions on whether to evacuate (why, how and to where) or shelter-in-place (why and for how long).
    - ❏ Establish an off-site family assistance center to provide information on responders to their families and vice versa.
    - ❏ Consider establishing a public assistance center in coordination with community partners.

❏ Evacuation / Shelter-in-Place Management

- ❏ MANAGE EVACUATIONS IN CONJUNCTION WITH LAW ENFORCEMENT AGENCIES.
    - ❏ Check all occupancies in areas that are likely to be affected by the terrorist attack (e.g., those that are downwind of the attack).
    - ❏ Select evacuation sites. Consider how evacuees would get to those sites and any potential barriers they would face (e.g., traffic congestion or exposure to other high-risk targets of attack).
    - ❏ Identify building wardens for evacuation centers.
    - ❏ If citizens are sheltering-in-place, communicate with them regularly and make sure your department or another agency checks on them on a regular basis.

❏ Continued Service Delivery

- ❏ MAKE PROVISIONS FOR CONTINUED SERVICE FOR DAY-TO-DAY EMERGENCIES (E.G., STRUCTURAL FIRES AND EMS CALLS).
    - ❏ Plan for an extended period of time.
    - ❏ Consider recall of off-duty personnel.
    - ❏ Utilize your mutual aid plans to make sure you have enough personnel, equipment and apparatus in reserve.
    - ❏ Assign personnel to act as guides for mutual aid teams.

Guide to RESPONDING to a Terrorist Attack cont

❏ Responder Safety and Wellness

- ❏ MAINTAIN RESPONDER SAFETY AND WELLNESS.
    - ❏ Enforce the use of personal protective equipment (PPE).
    - ❏ Provide appropriate decontamination.
    - ❏ Implement a medical monitoring system.
    - ❏ Provide proper relief, rehabilitation, counseling and after-action evaluations (or hot washes).
    - ❏ Implement your CISM program.
    - ❏ Provide wellness and support resources to family members through the family assistance center.

❏ Technical Response

- ❏ COORDINATE THE TECHNICAL RESPONSE THAT WILL BE NECESSARY.
    - ❏ Obtain any needed specialty responses.
    - ❏ Manage convergent volunteers.

❏ Victim Care and Management / Mass Casualty Plan/ Medical Surge Procedure

- ❏ UTILIZE ESTABLISHED SOPS FOR VICTIM CARE AND MANAGEMENT, INCLUDING MANAGING MASS CASUALTIES AND MEDICAL SURGE.
- ❏ UTILIZE ESTABLISHED SOPS FOR MASS FATALITY MANAGEMENT.

❏ Citizen / Community Responders

- ❏ ACTIVATE YOUR NETWORK OF CITIZEN AND COMMUNITY VOLUNTEERS (Please refer to the references for more information).

❏ Crime Scene Guidelines

- ❏ UTILIZE ESTABLISHED SOPS FOR RESPONDING TO A CRIME SCENE.

References for RESPONDING to a Terrorist Attack

❏ **FEMA Guidance**

- ❏ *Responding to Incidents of National Consequence: Recommendations for America's Fire and Emergency Services Based on the Events of September 11, 2001, and Other Similar Incidents,* www.usfa.dhs.gov/downloads/pdf/publications/fa-282.pdf

❏ **Safety and Health for Responders to CBRNE**

- ❏ HHS Policy & Guidance, www.hhs.gov/ohrp/policy/index.html
- ❏ OSHA and NIOSH Guidance, www.osha.gov/SLTC/emergencypreparedness/cbrnmatrix/index.html

* Please remember to visit www.IAFC.org/hschecklist for the most up-to-date information

A Guide to RECOVERING from a Terrorist Attack

❏ Medical-Screening Program for Responders

❏ ESTABLISH A MEDICAL SCREENING PROGRAM FOR RESPONDERS.

- ❏ Document which personnel were involved in the response.
- ❏ Consult with medical experts and provide medical education and follow-up, including long-term monitoring.
- ❏ Provide initial and continuing stress-management counseling.
- ❏ Provide timely advice and support to responders' family members.

❏ Documentation / Reporting

❏ DOCUMENT AND REPORT ALL RELEVANT INFORMATION.

- ❏ Employ special accounting procedures to ensure accurate loss figures for the fire department.
- ❏ File for reimbursement of appropriate expenses from FEMA and other federal agencies, state agencies and insurance companies.
- ❏ Prepare after-action reports for review and post-incident analysis. Draw from incident documents, reports submitted by response personnel and offices, and witnesses.
- ❏ Implement your department's SOPs on personnel-exposure reporting.

❏ Fire Department / Community Public Safety Agency Resource Assessment

❏ ASSESS RESOURCES.

- ❏ Assign a single point of contact to ensure appropriate testing for reliability of equipment and structural integrity of department facilities and to arrange for needed repairs and replacement. Consider borrowing or leasing needed facilities, equipment or apparatus until the repair/ replacement process is complete.
- ❏ Utilize your predetermined alternate location for displaced operations and alert personnel where to report for duty. Consider asking law enforcement agencies to provide security if necessary.
- ❏ Continue using mutual aid agreements as needed, including sharing personnel, equipment and facilities. (If your needs will be long-term, consider resources beyond these agreements.)

❏ Post-Incident Analysis

❏ PREPARE A POST-INCIDENT ANALYSIS FOR YOUR DEPARTMENT/COMMUNITY. (CONSIDER USING OUTSIDE RESOURCES FOR YOUR ANALYSIS.) PARTICIPATE IN COMMUNITY-WIDE POST-INCIDENTANALYSES AS YOUR RESOURCES ALLOW.

- ❏ Use incident documentation and reports.
- ❏ Evaluate and modify homeland security plans and SOPs as necessary.
- ❏ Coordinate any modifications and upgrades with community response partners and local emergency managers.
- ❏ Consider sharing this analysis with the public (e.g., posting it on the Internet).

❏ Community Recovery

❏ PARTICIPATE IN THE COMMUNITY'S RECOVERY.

- ❏ Brief local government officials on the fire departments/ public safety agencies status and advise them of the department's recovery plans and needs.
- ❏ Once you have taken all appropriate steps to recover internally, reach out to other agencies to offer assistance consistent with the department's recovery needs.
- ❏ Participate in community events to honor responders and victims.
- ❏ Be attentive to community needs the department may be able to meet.

❏ Media Relations

❏ MAINTAIN COMMUNICATION WITH MEDIA OUTLETS ABOUT THE RECOVERY OF YOUR DEPARTMENT AND THE COMMUNITY.

References for RECOVERING from a Terrorist Attack

❏ **Fire Department Recovery**

  ❏ City of New Orleans Fire Department Report: *Recovery and Reconstitution Planning Process after Hurricane Katrina*,

    www.iafc.org/files/downloads/DOC_DLS

❏ **Incident Analysis**

  ❏ After-Action Report and Improvement Plan for Hurricane Gustav & Ike,
    www.gohsep.la.gov/plans/Gustav_Ike_aar.pdf

  ❏ Arlington County After-Action Report on the Response to the September 11 Terrorist Attack on the Pentagon,

    www.arlingtonva.us/Departments/Fire

  ❏ DHS/FEMA Initial Response Hotwash: Hurricane Katrina in Louisiana,
    www.hsdl.org/?view&doc=68442&coll=limited

  ❏ Ethics and SARS: Learning Lessons from Toronto Experience, www.yorku.ca/igreene/sars.html

  ❏ H1N1 After-Action Report,
    www.dshs.state.tx.us/comprep/pandemic/H1N1_AAR.pdf

  ❏ Hurricane Katrina After-Action Report and Recommendations,
    http://msdh.ms.gov/msdhsite/_static/resources/1676.pdf

  ❏ Hurricane Katrina After-Action Report, Nebraska Urban Search and Rescue Task Force One,
    http://lincoln.ne.gov/city/fire/usar/pic

  ❏ Lessons Learned from the Mumbai Terrorist Attacks,

    www.nyc.gov/html/nypd/html/pr

  ❏ Minneapolis Bridge Collapse,
    www.usfa.dhs.gov/downloads/pdf/publications/tr_166.pdf

  ❏ Mumbai terrorist attacks – a case study,
    www.control-risks.com/PDF/mumbai_case_study.pdf

  ❏ Tokyo Subway Sarin Attack – Lessons Learned,

    www.sciencedirect.com/science/article

  ❏ Additional lessons learned and after-action reports can be found on FEMA's Information Sharing System, www.llis.gov

    (A password is required to access all publications but is available free-of-charge upon request.)

Please remember to visit www.IAFC.org/hschecklist for the most up-to-date information

APPENDIX A

Emergency Contact List I: Government Officials

Mayor/City Manager_____

Fire Chief _____

Police Chief _____

Sheriff _____

Public Health _____

Public Works _____

State Fire Marshall_____

Emergency Manager, Local_____

Emergency Manager, State _____

State Emergency Operations Center_____

Local Emergency Planning Committee _____

Local Chapter, American Red Cross_____

Critical Incident Stress Management Program _____

FBI Counter-Terrorism Field Officer _____

Fusion Center_____

Other _____

Emergency Contact List II: Federal Emergency Support Functions (ESFs)

ESF 1: Transportation _____

ESF 2: Communications _____

ESF 3: Public Works and Engineering _____

ESF 4: Firefighting _____

ESF 5: Emergency Management _____

ESF 6: Mass Care, Emergency Assistance, Housing, and Human Services _____

ESF 7: Resources Support _____

ESF 8: Public Health and Medical Services _____

ESF 9: Search and Rescue _____

ESF 10: Oil and Hazardous Materials Response _____

ESF 11: Agriculture and Natural Resources _____

ESF 12: Energy _____

ESF 13: Public Safety and Security _____

ESF 14: Long-Term Community Recovery_____

ESF 15: External Affairs_____

Emergency Contact List III: Local Subject-Matter Experts

Animal Issues _____

Biological Attack_____

Blackouts/Brownouts_____

Chemical Attack_____

Continuity of Government _____

Cyber Attack_____

Emergency Management _____

Explosions/Explosives _____

Finance _____

Hazardous Materials _____

Intelligence/Information-Sharing_____

Media Relations _____

Nuclear Attack _____

Pandemic _____

Power Supply _____

Radiological Attack _____

Riots _____

Special Operations _____

Structural Stability _____

Traffic _____

Water Supply _____

Appendix B
Terrorism Planning Assessment Matrix

	Low level of leadership Minimum Level				High level of leadership Optimum Level
ASSESSMENT	No assessment done	Limited assessment completed and some relationships developed		Key collaboration on a regular basis Response capabilities identified	Completed assessment and detailed gap analysis performed
PREVENTION	Awareness training identified but not conducted Internal reporting procedures only No formal facility security program	Infrastructure protection program and awareness training initiated Informal information sharing coordination	Awareness training in progress Reporting procedures formalized internally	Infrastructure protection program in progress	Awareness and information sharing programs incorporated into comprehensive departmental programs
PREPAREDNESS	General orientation of equipment Individual agency SOP's	Initial training conducted Agency exercises held Informal mutual aid agreements developed Resource and contact lists partially completed	Tabletop exercise held for some staff Inter-agency SOPs developed for planned events NIMS partially implemented	Training conducted for some personnel Mutual aid agreements formalized Resource and contact lists completed	Training conducted for all personnel levels Multi-agency full functional exercises conducted on regular basis Multi-agency NIMS integrated SOPs used daily
RESPONSE	Informal SOPs used for response	Limited situational awareness with external organizations	Formal inter-agency SOP's used	Automatic aid regularly used	NIMS embedded into SOPs used daily Fully integrated Common Operating Picture
RECOVERY	Informal post incident analysis conducted No formal documentation SOPs	Limited accounting and documentation procedures used		NIMS documentation incorporated into daily use Formal CISM SOPs	Formal post incident analysis and after event resource assessment process used

August 2011

Appendix C : Glossary and Acronyms

In the interest of space, the information listed in this Appendix is limited to select terms. Except where noted, definitions are drawn directly from the U.S. Department of Homeland Security's National Response Framework. For a more complete list of homeland security-related terms and acronyms, please visit the National Response Framework Resource Center: www.fema.gov/emergency/nrf/glossary.htm

ASSESSMENT: The evaluation and interpretation of measurements and other information to provide a basis for decision making.

AUTOMATIC AID: A formal agreement through which non-jurisdictional emergency resources automatically respond to an emergency because they are geographically closer. This type of aid is different from mutual aid, which is not automatic but on a case-by-case basis.

CONTINUITY OF GOVERNMENT (COG): Activities that address the continuance of constitutional governance. COG planning aims to preserve and/or reconstitute the institution of government and ensure that a department or agency's constitutional, legislative, and/or administrative responsibilities are maintained. This is accomplished through succession of leadership, pre-delegated emergency authority, and active command and control during response and recovery operations.

CONTINUITY OF OPERATIONS (COOP) PLANS: Procedures to ensure the continued performance of core capabilities and/or critical government operations during any potential incident.

CRITICAL INFRASTRUCTURE: Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. (Often paired with key resources)

EMERGENCY MANAGEMENT ASSISTANCE COMPACT (EMAC): A congressionally ratified organization that provides form and structure to interstate mutual aid. Through EMAC, a disaster-affected State can request and receive assistance from other member States quickly and efficiently, resolving two key issues upfront: liability and reimbursement.

EMERGENCY OPERATIONS PLAN: The ongoing plan maintained by various jurisdictional levels for responding to a wide variety of potential hazards.

FUSION CENTERS: Fusion centers blend relevant intelligence and information analysis to coordinate law enforcement, fire and other public safety efforts in reducing threats to local communities. Fusion centers facilitate information-sharing across jurisdictions and disciplines by providing a conduit between local communities and state and federal agencies.

HSPD-8: Homeland Security Presidential Directive 8, National Preparedness

INCIDENT MANAGEMENT TEAM (IMT): An incident command organization made up of the Command and General Staff members and appropriate functional units of an Incident Command System (ICS) organization. The level of training and experience of the IMT members, coupled with the identified formal response requirements and responsibilities of the IMT, are factors in determining the "type," or level, of IMT. IMTs are generally grouped in five types. Types I and II are national teams, Type III are State or regional, Type IV are discipline- or large jurisdiction-specific, and Type V are ad hoc incident command organizations typically used by smaller jurisdictions.

JOINT INFORMATION CENTER (JIC): A facility established to coordinate all incident-related public information activities. The JIC is a physical location from which external affairs professionals from all the organizations involved in an incident work together to provide emergency information, media response, and public affairs functions. The JIC serves as a focal point for a coordinated and timely release of incident-related prevention, preparedness, response, recovery, and mitigation information to the public. It is the central point of contact for all news media.

KEY RESOURCES: Any publicly or privately controlled resources essential to the minimal operations of the economy and government.

MUTUAL AID: An arrangement among emergency responders to lend assistance upon request across jurisdictional boundaries. Mutual aid usually results from an emergency that exceeds local resource capabilities. Mutual aid may be ad hoc, requested only when such an emergency occurs, or it may be based on a formal agreement for non-jurisdictional assistance. Generally, the fire service utilizes mutual aid; however, other entities, such as utility companies and law enforcement agencies, also use it.

NATIONAL INCIDENT MANAGEMENT SYSTEM (NIMS): Provides a systematic, proactive approach guiding government agencies at all levels, the private sector, and nongovernmental organizations to work seamlessly to prepare for, prevent, respond to, recover from, and mitigate the effects of incidents, regardless of cause, size, location, or complexity, in order to reduce the loss of life or property and harm to the environment. NIMS codified emergency management discipline in six areas, including incident command and management structures, core preparedness activities, resource management, communications, supporting technologies, and the maintenance for these systems over time.

PREPAREDNESS: A continuous cycle of planning, organizing, training, equipping, exercising, evaluating, and improving in an effort to ensure effective coordination during incident response.

PRESIDENTIAL POLICY DIRECTIVIE/PPD-8: Presidential Policy Directive /PPD-8 on national preparedness has replaced HSPD-8 but is meant to reaffirm its general policy direction as well as that of the 2006 Post-Katrina Emergency Management Reform Act (PKEMRA) and 2009 National Infrastructure Protection Plan (NIPP). PPD-8 retains the all-hazards, risk-based approach of HSPD-8, though it uses four categories of hazards: terrorism, catastrophic natural disasters, cyber attacks and pandemics.

RECOVERY: The development, coordination, and execution of service- and site-restoration plans; the reconstitution of government operations and services; individual, private-sector, nongovernmental, and public-assistance programs to provide housing and to promote restoration; long-term care and treatment of affected persons; additional measures for social, political, environmental, and economic restoration; evaluation of the incident to identify lessons learned; post-incident reporting; and development of initiatives to mitigate the effects of future incidents.

TERRORISM: Under the Homeland Security Act of 2002, terrorism is defined as activity that involves an act dangerous to human life or potentially destructive of critical infrastructure or key resources; is a violation of the criminal laws of the United States or of any state or other subdivision of the United States in which it occurs; and is intended to intimidate or coerce the civilian population, or influence or affect the conduct of a government by mass destruction, assassination, or kidnapping. See Section 2 (15), Homeland Security Act of 2002, Public Law 107–296, 116 Stat. 2135 (2002).

TERRORISM LIAISON OFFICER (TLO): An individual who has been trained to report suspicious activity encountered during the course of his or her normal activities. While some of these individuals are members of local law enforcement agencies, others such as firefighters, paramedics, utility workers, and railroad employees are also participants.

Acronyms

CBRNE	Chemical, Biological, Radiological, Nuclear and Explosive	NG	National Guard
CERT	Community Emergency Response Team	NICC	National Infrastructure Coordination Center
CISM	Critical Incident Stress Management	NIMS	National Incident Management System
COOP	Continuity of Operations Plan	NRF	National Response Framework
DHS	U.S. Department of Homeland Security	NTSA	National Terrorism Advisory
DMORT	Disaster Mortuary Operational Response Team	PIO	Public Information Officer
EMAC	Emergency Management Assistance Compact	POD	Point of Distribution
EOP	Emergency Operations Plan	PPD	Presidential Policy Directive
FEMA	Federal Emergency Management Agency	PPE	Personal Protective Equipment
FBI	Federal Bureau of Investigation	SOP	Standard Operating Procedure
HSPD	Homeland Security Presidential Directive	TCL	Target Capabilities List
ICS	Incident Command System	TLO	Terrorism Liaison Officer
IED	Improvised Explosive Device	UC	Unified Command
IMT	Incident Management Team	USNORTHCOM	U.S. Northern Command
IT	Information Technology	UTL	Universal Task List
JIC	Joint Information Center	WMD	Weapons of Mass Destruction
JTTF	Joint Terrorism Task Force		

Appendix D : About the Authors

In the spring of 2007, the IAFC Board of Directors envisioned a unified national strategy, in which the fire and emergency service defines its role and responsibilities in homeland security. A team of members representing various IAFC sections and committees convened at a Homeland Security Summit to create a document that would be flexible and adaptable within the fire service and the broader public safety community.

The authors of this guide were fire chiefs representing a cross-section of the IAFC's membership, fire-service expertise, and geographic diversity. They were selected to represent the following IAFC sections and committees:

- **EMERGENCY MANAGEMENT COMMITTEE**
  Chief Jerry Rhodes, Cunningham (Colo.) Fire Protection District, Committee Chair
  Chief Gerard Dio, Worcester (Mass.) Fire Department

- **EMERGENCY MEDICAL SERVICES SECTION**
  Chief John Sinclair, Kittitas Valley (Wash.) Fire & Rescue, IAFC Board Member
  Chief Dan Hermes, Pleasantview (Ill.) Fire Protection District

- **HAZARDOUS MATERIALS COMMITTEE**
  Assistant Chief Tim Butters, City of Fairfax (Va.) Fire Department,
  Committee Chair Chief Ron Kanterman, Merck Emergency Services, Rahway, N.J.

- **METROPOLITAN FIRE CHIEFS SECTION**
  Chief Keith B. Richter, Contra Costa County (Calif.) Fire Protection District,
  Section President Russell Sanders, National Fire Protection Association, Section Executive Secretary

- **SAFETY, HEALTH AND SURVIVAL SECTION**
  Deputy Director Ricky Brockman, U.S. Navy Fire & Emergency Services, Washington, DC,
  Section Organizational Liaison
  Commissioner David H. Fischler, Ret., Suffolk County (N.Y.) Department of Fire, Rescue and Emergency Services,
  Section Director At-Large

- **TERRORISM AND HOMELAND SECURITY COMMITTEE**
  Chief P. Michael Freeman, Los Angeles County (Calif.) Fire Department, Committee Chair
  Chief James H. Schwartz, Arlington County (Va.) Fire Department

- **VOLUNTEER AND COMBINATION OFFICERS SECTION**
  Chief Timothy S. Wall, North Farms (Conn.) Volunteer Fire Department, Section Chair
  Chief Michael Varney, Ellington (Conn.) Volunteer Fire Department

- **DEVELOPMENT ASSISTANCE**
  Holly Gray Stearns

Appendix E : About the IAFC

Overview

The IAFC represents the leadership of firefighters and emergency responders worldwide; our members are the world's leading experts in firefighting, emergency medical services, terrorism response, hazardous materials spills, natural disasters, search and rescue, and public safety policy. Since 1873, the IAFC has provided a forum for fire and emergency service leaders to exchange ideas, develop professionally and uncover the latest products and services available to first responders.

Mission

The mission of the IAFC is to provide leadership to current and future career, volunteer, fire-rescue and EMS chiefs, chief fire officers, company officers and managers of emergency service organizations throughout the international community through vision, information, education, services and representation to enhance their professionalism and capabilities.

Photo credits:
Federal Emergency Management Agency (FEMA) News Photos www.fema.gov/photolibrary
U.S. Department of Homeland Security
International Association of Fire Chiefs (photo contest submittals)
Metropolitan Washington Airports Authority
National Sheriffs Association

Notes

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

Notes

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

Notes

International Association of Fire Chiefs

4025 Fire Ridge Drive, Suite 300
Fairfax, VA 22033

703-273-0911 • www.iafc.org