TERRORISM RESPONSE

A Checklist and Guide for Fire Chiefs and Community Preparedness Leaders

4th Edition

www.iafc.org

ALL-RISK AND ALL-HAZARD

DEDICATION

IN MEMORY OF THOSE WHO LOST THEIR LIVES AS A RESULT OF THE TERRORIST ATTACKS ON SEPTEMBER 11, 2001.

TERRORISM RESPONSE:

A Checklist and Guide for Fire Chiefs and Community Preparedness Leaders 4th Edition

To Fire Chiefs and Community Preparedness Leaders:

Welcome to the 4th Edition of Terrorism Response: A Checklist and Guide for Fire Chiefs and Community Preparedness Leaders, referred to herein as the Checklist and Guide. This booklet, which was first developed by fire chiefs following the attacks of September 11, 2001, has evolved over the years and continues to provide succinct and up-to-date guidance to prepare busy leaders and their departments and organizations for acts of terrorism and other risks.

Although terrorism was the impetus for the Checklist and Guide, and the fire chief was the initial target audience, two important points are very clear. First, the audience extends beyond the fire chief and includes leaders in law enforcement, emergency management, emergency medical services, public health, public administration, public works, and even the private sector. Second, the Checklist and Guide can be extremely useful in preparing for other risks.

This 4th Edition of the Checklist and Guide incorporates several changes. The recommendations have been greatly simplified to provide essential guidance as opposed to an exhaustive list of recommendations. Also, the references are accessible through the IAFC web site, providing ease of access and timely updates as changes are made.

The Checklist and Guide can be useful in addressing the five homeland security mission areas of **prevention, protection, mitigation, response, and recovery**. With the help of Checklist and Guide, and working together, we can prepare our departments, organizations, and communities to cope effectively with acts of terrorism, active shooters, civil unrest, natural disasters, extreme weather events, public health threats, and other risks.

When large-scale emergencies and disasters strike, they truly are local events. Life safety, treatment of the injured, hazard control, loss limiting, responder safety, and recovery depend on a whole community approach and teamwork. We believe that the Checklist and Guide can serve as an effective tool in developing the whole community approach and teamwork within any town, city or municipality that seeks guidance on terrorism and all-hazard preparedness.

It is the desire of the IAFC Terrorism and Homeland Security Committee, that fire chiefs throughout the country use this document as a catalyst to initiate a dialog in their communities. In addition to evaluating within their own organizations, fire chiefs should champion their jurisdictional prevention, protection, mitigation, response, and recovery activities. Your actions to stimulate community efforts are vital to lessen the impact of overwhelming circumstances.


MONTGOMERY
COUNTY

TABLE OF CONTENTS

Please remember to visit http://www.IAFC.org/hschecklist for up-to-date information.

EXECUTIVE SUMMARY

The Checklist and Guide is designed to assist fire chiefs and other public safety leaders in **preventing, protecting against, mitigating, responding to, and recovering from** acts of terrorism or other risks. To provide a clear and comprehensive approach for the user, a Summary Checklist, How to Guides, References, and informative Appendices are included.

The **Summary Checklist** outlines the most critical actions to assess, prevent, prepare for, respond to, and recover from acts of terrorism and other risks. Community leaders may also use this Summary Checklist to perform similar preparedness actions for other hazards and risks by substituting the targeted risk/hazard in place of “terrorist attack” in the checklist. Whereas natural disasters and extreme weather events may not be preventable, their impact on a community can be mitigated by effective planning, early warning, strong interagency relationships, response training, and other preparedness measures.

The objective in using the Summary Checklist is to accomplish key 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 their local and federal law enforcement partners and other preparedness leaders to establish priorities for each risk and realistic time frames within which to accomplish the various recommendations. Fire chiefs whose departments have worked through the Checklist and Guide have found that 18 months is a reasonable amount of time for a high degree of completion. Of course, each community will have to establish suitable timeframes for each hazard and risk; thereafter, periodic reviews, updates, exercises and training 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.

Informative **Appendices** provide useful references, guides, and templates. Appendix A can be used when putting together Contact Lists. Appendix B provides a Terrorism Planning Assessment Matrix. Appendix D discusses What Every Fire Department Should Evaluate for Terrorism Events. Appendix E is a Terrorist Attack Checklist, and Appendix F provides a template for assessing Complex Coordinated Attack Scenario Capabilities.

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.**


LOS ANGELES
FIRE
DEPARTMENT

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
☐	☐	☐	☐	Relationship / Partnerships / Mutual Aid / Automatic Aid / EMAC
☐	☐	☐	☐	Intelligence-Sharing / Fusion Center Engagement
☐	☐	☐	☐	Response Capabilities for WMD / CBRNE Attacks
☐	☐	☐	☐	Cyber Security Awareness
☐	☐	☐	☐	Communication Plan (Interoperability)
☐	☐	☐	☐	Gap Analysis / Action Plan
☐	☐	☐	☐	Continuity of Operations (COOP) / Continuity of Govt. (COG) Plans

How to Help PREVENT a Terrorist Attack

Initial Assessment	Mid-Point Assessment	18-Month Assessment	Follow-Up Assessment	
☐	☐	☐	☐	Terrorism Awareness / Recognition Training
☐	☐	☐	☐	Suspicious Activity Reporting Procedures
☐	☐	☐	☐	Security Clearances for Appropriate Staff
☐	☐	☐	☐	Personnel / Facilities Security / Critical Infrastructure Protection
☐	☐	☐	☐	Cyber Security Awareness
☐	☐	☐	☐	Other Considerations?

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

Initial Assessment	Mid-Point Assessment	18-Month Assessment	Follow-Up Assessment	
☐	☐	☐	☐	Standard Operating Procedures
☐	☐	☐	☐	NIMS Adoption and Training
☐	☐	☐	☐	Emergency Operations Plan
☐	☐	☐	☐	Mutual Aid / Automatic Aid / EMAC
☐	☐	☐	☐	Multi-Casualty Response Plans
☐	☐	☐	☐	Fire Dept and Public Safely Agency Member / Family Preparedness
☐	☐	☐	☐	Active Shooter Response Plans Rescue Task Force (RTF) Plans
☐	☐	☐	☐	Bomb / IED Response Plans
☐	☐	☐	☐	CBRNE Response Plans
☐	☐	☐	☐	Technical Rescue Response Sustainment
☐	☐	☐	☐	Equipment
☐	☐	☐	☐	Crime Scene Guidelines
☐	☐	☐	☐	Terrorism Training & Exercises
☐	☐	☐	☐	Continuity of Operations / Continuity of Gov't Plans
☐	☐	☐	☐	24x7 Contacts / Resource List
☐	☐	☐	☐	Community Notification Plans
☐	☐	☐	☐	Evacuation / Shelter-in-Place Plans
☐	☐	☐	☐	Points of Distribution Plans
☐	☐	☐	☐	Citizen Involvement / CERT / Fire Corps / Reserve Med Corps / Neighborhood Watch
☐	☐	☐	☐	Family Assistance Center Plans
☐	☐	☐	☐	Incident Access Control
☐	☐	☐	☐	Victim Care and Management / Mass Casualty Plan / Medical Surge Procedure
☐	☐	☐	☐	Mass Fatality Management Plans

How to RESPOND to a Terrorist Attack

Initial Assessment	Mid-Point Assessment	18-Month Assessment	Follow-Up Assessment	
☐	☐	☐	☐	Situational Awareness / Information-Sharing Procedures
☐	☐	☐	☐	National Incident Management System (NIMS) Compliance
☐	☐	☐	☐	Standard Operating Procedures for Terrorism Response
☐	☐	☐	☐	Mutual Aid Agreements
☐	☐	☐	☐	Force Protection (Responder Safety) / Perimeter Security
☐	☐	☐	☐	Media / Crisis Communication
☐	☐	☐	☐	Evacuation Plans / Shelter-in-Place Management
☐	☐	☐	☐	Continued Service Delivery
☐	☐	☐	☐	Responder Safety and Wellness
☐	☐	☐	☐	Technical Response – Special Operations, Hazardous Materials, etc.
☐	☐	☐	☐	Victim Care and Mgmt / Mass Casualty Plan / Medical Surge Procedure
☐	☐	☐	☐	CERT / Community Responders
☐	☐	☐	☐	Crime Scene Guidelines

How to RECOVER from a Terrorist Attack

Initial Assessment	Mid-Point Assessment	18-Month Assessment	Follow-Up Assessment	
☐	☐	☐	☐	Medical Screening Program for Responders
☐	☐	☐	☐	Documentation / Reporting
☐	☐	☐	☐	Fire Dept / Comm. Resource Assess
☐	☐	☐	☐	Post-Incident Analysis
☐	☐	☐	☐	Community Recovery
☐	☐	☐	☐	Media Relations

Guide to ASSESSING Threats and Capabilities

☐ 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.

☐ Community Risks / Special Events

- IDENTIFY OTHER COMMUNITY RISKS UNIQUE TO YOUR AREA, INCLUDING LOCAL SPECIAL EVENTS:
    - Ceremonies and parades
    - Dignitary visits and events
    - Sporting events
    - State and local fairs
    - Other annual or semi-annual event
- 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, flood, tornadoes, and blizzards
    - Civil unrest
    - Other local and regional threats

☐ Continuity of Operations Plan (COOP) / Continuity of Government (COG) Plans

- 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 several Presidential directives, notably Presidential Policy Directive 8 (PPD-8), the 2006 Post-Katrina Emergency Management Reform Act (PKEMRA), and the 2013 National Infrastructure Protection Plan (NIPP).

PPD-8 uses four categories of hazards: terrorism, catastrophic natural disasters, cyber-attacks and pandemics.

Significant changes to PPD-8 as compared with 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.

For more information, visit http://www.fema.gov/learn-about-presidential-policy-directive-8.

☐ Cyber-Security Awareness

- 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.

☐ 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.

☐ Intelligence Sharing / Fusion Center Engagement

- Fire departments should know where their fusion center is, who represents the fire service, and ensure that information-sharing is efficient between the fusion center and their department. Channels also need to exist to share information received.

- 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.
    - If your fusion center supports the Terrorism Liaison Officer (TLO) Program, identify a member within your department to attend the training and designate him or her as the point of contact for terrorism information-sharing.
    - 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.

- Care should be taken regarding the distribution of Unclassified/For Official Use Only information. Information should only be distributed within your own organization to personnel who have a need to know. Personnel should be trained to honor and respect the importance of not forwarding information outside your own organization unless specific authorization is given by the primary distributing agency. Other organizational information and materials, such as operating procedures and preplans, should be given the same consideration.

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

☐ 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 agencies
    - 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

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

- ASSESS YOUR DEPARTMENT'S/COMMUNITY'S ABILITY TO RESPOND TO THE TERRORIST ATTACKS USING 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).

☐ 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 service 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, private colleges, universities, and other politically sensitive facilities that may be targets of terrorism
  - 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

References for ASSESSING Threats and Capabilities

☐ Chemical, Biological, Radiological, Nuclear and Explosive Attacks

- The Departments of Homeland Security and Commerce have developed the National Strategy for CBRNE Standards, which describes the federal vision and goals for the coordination, prioritization, establishment, and implementation of CBRNE equipment standards by 2020. https://www.whitehouse.gov/sites/default/files/microsites/ostp/chns_cbrne_standards_final_24_aug_11.pdf
- FEMA Center for Domestic Preparedness. FEMA's Center for Domestic Preparedness (CDP), located in Anniston, Alabama, is DHS's only federally chartered Weapons of Mass Destruction (WMD) training center. https://cdp.dhs.gov/

☐ Continuity of Operations Planning

- FEMA Continuity of Operations Planning. https://www.fema.gov/planning-templates
- NFPA 1600: Standard on Disaster/Emergency Management and Business Continuity of Operations Program. http://www.nfpa.org/codes-and-standards/document-information-pages?mode=code&code=1600

☐ Critical Infrastructure Protection

- The Department of Homeland Security provides strategic guidance to public and private partners, promotes a national unity of effort, and coordinates the overall Federal effort to promote the security and resilience of the nation's critical infrastructure. https://www.dhs.gov/topic/critical-infrastructure-security
- The National Infrastructure Protection Plan provides the foundation for an integrated and collaborative approach to achieve the vision of: "[a] Nation in which physical and cyber critical infrastructure remain secure and resilient, with vulnerabilities reduced, consequences minimized, threats identified and disrupted, and response and recovery hastened." https://www.dhs.gov/national-infrastructure-protection-plan
- Emergency Management and Response – Information Sharing and Analysis Center (EMR ISAC) https://www.usfa.fema.gov/operations/ops_cip_emr-isac.html
- The National Infrastructure Coordinating Center (NICC) is the dedicated 24/7 coordination and information sharing operations center that maintains situational awareness of the nation's critical infrastructure for the federal government. https://www.dhs.gov/national-infrastructure-coordinating-center

☐ Federal Bureau of Investigation

- The FBI is a great source of information regarding CBRNE threats and resources. Each FBI field office has a WMD Coordinator. The special agent assigned as the WMD Coordinator is a great resource to the fire community and other first responders. To locate your FBI field office, got to: https://www2.fbi.gov/contact/fo/fo.htm

☐ **National Planning Framework**

- National Planning Framework. http://www.fema.gov/national-planning-frameworks

☐ **National Preparedness Guidelines**

- National Preparedness Guidelines. https://www.dhs.gov/national-preparedness-guidelines

☐ **National Response Framework**

- National Response Framework Resource Center. http://www.fema.gov/national-response-framework

- Lessons Learned. https://www.fema.gov/lessons-learned-information-sharing-program
- Naval Postgraduate School Homeland Security Digital Library, https://www.hsdl.org

Please remember to visit http://www.IAFC.org/hschecklist for up-to-date information.


15C

Guide to Helping **PREVENT** a Terrorist Attack

☐ 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.

☐ 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 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

The availability of U/FOUO information generally meets the needs of local communities for planning and situational awareness. However, the importance of sensitive and classified information for these purposes should not be overlooked by fire chiefs. Obtaining security clearances for the fire chief and a designated staff member should be considered.

- Discuss the need for security clearances with local, state and federal law enforcement agencies for designated personnel when necessary to receive classified information.

- Build and maintain strong working relationships with local, state, and federal partners to ensure timely information-sharing regarding threats and risks. The issuance of security clearances doesn't replace the critical need for fire and police officials to continually meet, communicate and train together.

☐ 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 to look for secondary explosive devices or other terrorist threats as demonstrated at the Columbine incident.
    - 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.

References for Helping PREVENT a Terrorist Attack

- If You See Something, Say Something™ Campaign
  - https://www.dhs.gov/see-something-say-something
- 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
  - Global Terrorism Database. http://www.start.umd.edu/gtd/
- Model Fire, Building, Life Safety and Associated Codes and Standards (nationally recognized)
  - National Fire Protection Association, http://www.nfpa.org
  - International Code Council, http://www.iccsafe.org
- NCTC Joint Counterterrorism Assessment Team
  - https://www.nctc.gov/jcat.html
- Ready.gov
  - http://www.ready.gov
- State and Local Fusion Centers
  - https://www.dhs.gov/state-and-major-urban-area-fusion-centers
- Terrorism Liaison Officers
  - http://www.tlo.org

Please remember to visit http://www.IAFC.org/hschecklist for up-to-date information.

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

☐ **Citizen Involvement/Community Emergency Response Teams (CERT) / Fire Corps / Medical Reserve Corps / Neighborhood Watch**

- 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.

☐ **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-scripted messages.

☐ **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.)

☐ **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. Departments should ensure adequate supplies of specific personal protection equipment (PPE) or the ability to replace contaminated gear after an event.
- 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.

☐ Crime Scene Guidelines

- ESTABLISH SOPS FOR RESPONDING TO A CRIME SCENE.
    - The scene of a terrorist attack will be a crime scene, requiring special protocols and other considerations.
    - Work with law enforcement agencies to develop appropriate procedures for your department.

☐ 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.

☐ 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.

☐ 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 individuals with disabilities and access and functional needs, 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.
- Emergency management should ensure congruent facilities have adequate plans for evacuation or sheltering in place to include hospitals, nursing homes, assisted living facilities, and detention centers.
- 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.

☐ **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 or peer support 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.

☐ Homeland Security Grants

- There are numerous Homeland Security grant programs that will cause Fire Departments to engage with local and State partners. The Department of Homeland Security distributes grant funds to enhance the ability of regional authorities to prepare, prevent and respond to terrorist attacks and other disasters. Localities use grants for planning, equipment, training and exercise needs.

- In the past 10 years, the federal government has awarded state and local governments more than $35 billion for planning, response and recovery efforts related to terrorist attacks, natural disasters, and other events. These grants have provided funding for a variety of purposeful activities, including training exercises for mass shootings to the replacement of first-responder radios. These include the Homeland Security Grant Program (HSGP), State Homeland Security Grant Program (SHSGP), Emergency Management Performance Grant (EMPG), and Urban Area Security Initiative (UASI).

☐ 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.

☐ 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).
    - Be familiar with local, regional, and state mutual aid resources and coordinating authorities.
    - Put all mutual aid and automatic aid agreements in writing.
    - Define a trigger point for requesting 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 communications.
    - 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.)

☐ **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.

☐ **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.

☐ **Social Media**

- Social media plays an important role in the daily lives of many and the way they receive their news. Fire Chiefs should consider the benefits social media can provide first

responders prior to an actual event and use it to provide accurate and timely information. Social media can be the quickest way to communicate not only to the public but also to press outlets. Social media can also be an excellent source of information-gathering. Do not under estimate the value of prompt communications to the successful mitigation of an incident or your Department's reputation. If Departments lack the resources to access social media, efforts should be made to work and coordinate with governmental communication offices or other communication professionals.

☐ **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 agencies in a Joint Information Center (JIC).
    - Implement an SOP for the protection of sensitive information during verbal communications.

☐ **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 unaffiliated volunteers (volunteers who spontaneously offer their help in the wake of a disaster).

☐ **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.)

☐ **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.

NOTE: Fire Chiefs that need additional resources to assist with response or recovery should understand their ability to get help through automatic aid, mutual aid, the Emergency Management Assistance Compact (EMAC) and if federal resources are needed how to contact the State to request those resources. To request a resource, use the CSALTT acronym:

C	Capability – What will the resource be used for / doing?
S	Size – Physical descriptor of the resource.
A	Amount – How many of them do you need?
L	Location – What is the specific address where the resource is needed?
T	Type – Either the FEMS resource type or the general descriptor of what it is.
T	Time – How long will the resource be needed and when do you need it?

Fire Departments should work to foster relationships with the Logistics officers in your State that can assist with obtaining resources from Statewide Mutual Aid or through the Emergency Management Assistance Compact (EMAC).


OKLAHOMA
US&R
Task Force

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

- **Citizen Involvement**
  - Community Emergency Response Team (CERT) Program. http://www.fema.gov/community-emergency-response-teams
  - Fire Corps. http://www.firecorps.org
  - Medical Reserve Corps. https://www.medicalreservecorps.gov/HomePage
  - National Neighborhood Watch. http://www.nnw.org/

- **Community Readiness**
  - http://www.ready.gov

- **Continuity of Operations Planning**
  - FEMA Continuity of Operations Planning. https://www.fema.gov/planning-templates

- **Disaster Mortuary Operational Response Teams**
  - http://www.phe.gov/preparedness/responders/ndms/teams/pages/dmort.aspx

- **Family Support Planning**
  - FEMA's COOP Planning, https://www.fema.gov/continuity-operations

- **First Responder Grants**
  - FIRE and SAFER grant information https://www.fema.gov/staffing-adequate-fire-emergency-response-grants

- **Homeland Security Grants**
  - http://www.fema.gov/grants

- **Member and Family Preparedness**
  - Federal Disaster Assistance, https://www.disasterassistance.gov/
  - Federal Emergency Management Agency, http://www.fema.gov
  - Federal "Ready" Program, http://www.Ready.gov

- **Mutual Aid**
  - Emergency Management Assessment Compact (EMAC), http://www.emacweb.org
  - Guidance and Sample Agreements – International Association of Fire Chiefs, http://www.iafc.org/mutualaid

- **National Fire Academy Courses on Response to Terrorism and Emergencies**
  - http://www.usfa.dhs.gov/nfa/

- **National Incident Management System (NIMS)**
  - http://www.fema.gov/national-incident-management-system

- **National Response Framework**
  - http://www.fema.gov/national-response-framework

- **National Terrorism Advisory System**
  - https://www.dhs.gov/national-terrorism-advisory-system

- **Preparing for Disaster for People with Disabilities and Other Special Needs**
  - FEMA Resource Record Details, http://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, http://www.rand.org/pubs/conf_proceedings/2006/CF176.pdf
  - National Fire Fighter Near Miss Reporting System, http://www.firefighternearmiss.com
  - National Strategy for Homeland Security, http://www.whitehouse.gov/homeland/book

- **Standards, Training and Grant Information for Emergency Responders**
  - Responder Knowledge Base, http://www.rkb.us
    A login name and password are required but are available free of charge to public safety agencies.

- **State and Federal Resources**
  - Emergency Management Assistance Compact, http://www.emacweb.org
  - National Guard Chemical, Biological, Radiological, Nuclear, and Explosive (CBRNE) Enhanced Response Force Package (CERFP)
  - National Guard Civil Support Team, http://www.nationalguard.mil/Home.aspx
  - National Response Framework, http://www.fema.gov/national-response-framework
  - U.S. Northern Command, www.northcom.mil
  - U.S. Fire Administration AHIMT Technical Assistance Program, https://www.fema.gov/fema-technical-assistance-program

- **Training**
  - Homeland Security Exercise and Evaluation Program, https://www.fema.gov/media-library/assets/documents/32326
  - U.S. Bomb Data Center - Bomb Arson Tracking System (BATS) link to an online video about the database, http://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, http://www.iafc.org/files/wellness_fitness_smfd.pdf

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

Please remember to visit http://www.IAFC.org/hschecklist for 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.

☐ Citizen / Community Responders

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

☐ 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.

☐ Crime Scene Guidelines

- UTILIZE ESTABLISHED SOPS FOR RESPONDING TO A CRIME SCENE.

☐ 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.

☐ 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.

☐ Media / Crisis Communication

- UTILIZE YOUR MEDIA AND CRISIS COMMUNICATIONS PLANS.

    - Appoint a PIO as soon as possible.
    - Participate in the activities of the Joint Information Center (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.
    - Monitor social media for information gathering.

☐ 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.
    - Assign a department member or officer to each mutual aid crew to act as a guide.
    - Coordinate and control mutual aid resources.
    - Manage spontaneous resources as appropriate.

☐ 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.

☐ Notifications

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

☐ Responder Safety and Wellness

- MAINTAIN RESPONDER SAFETY AND WELLNESS.
    - Enforce the use of personal protective equipment (PPE).
    - Provide appropriate decontamination.
    - Provide proper relief, rehabilitation, counseling and after-action evaluations (or hot washes).
    - Implement your Critical Incident Stress Management (CISM) program/peer support plan.
    - Provide wellness and support resources to family members through the family assistance center.

☐ Situational Awareness / Frequent Updates

Fire Chiefs need to reach out to local law enforcement and the intelligence community (regional, state, and federal) prior to an actual terrorism or similar event. This has not been the case in too many communities throughout the country. A partnership must be established and regularly supported between the fire service and law enforcement. Fire and law enforcement conferring for the first time at an incident command post should not be the norm. Relationships and trust need to be built to more effectively lead an incident to a successful outcome.

- 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.

☐ Technical Response

- COORDINATE THE TECHNICAL RESPONSE THAT WILL BE NECESSARY.

    - Obtain any needed specialty responses.
    - Manage spontaneous 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.

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, http://www.usfa.dhs.gov/downloads/pdf/publications/fa-282.pdf
  - Updated guidance is available from many sources.

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

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

Please remember to visit http://www.IAFC.org/hschecklist for up-to-date information.


26
8172

A Guide to **RECOVERING** from a Terrorist Attack

National Disaster Recovery Framework reference (http://www.fema.gov/national-disaster-recovery-framework)

☐ Community Recovery

- National Disaster Recovery Framework
  http://www.fema.gov/media-library/assets/documents/24647

- 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.

☐ 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.

  - Develop a process to assess and report damage to department facilities, infrastructure, apparatus, and equipment.
  - 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.)

☐ Media Relations

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

☐ 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 as outlined in your CISM plan or peer support group plans.
    - Provide timely advice and support to responders' family members.

☐ Post-Incident Analysis

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

References for **RECOVERING** from a Terrorist Attack

- **Incident Analysis**
  - Lessons learned and after-action reports can be found on FEMA's Information Sharing System. http://www.llis.gov.

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

Please remember to visit http://www.IAFC.org/hschecklist for up-to-date information.


3

APPENDIX A

EMERGENCY CONTACT LIST I: GOVERNMENT OFFICIALS

Mayor/City Manager_____

Fire Chief_____

Police Chief_____

Sheriff_____

Public Health_____

Public Works_____

Local Building Official_____

State Fire Marshal_____

Emergency Manager, Local_____

Emergency Manager, State_____

State Emergency Operations Center_____

Local Emergency Operations Center_____

Local Chapter, American Red Cross_____

Critical Incident Stress Management Program_____

FBI Counterterrorism Field Officer_____

Fusion Center_____

Transportation_____

Hospitals_____

Critical Infrastructure (water, electric, gas, cable)_____

Schools_____

Medical Examiner_____

Volunteer/VOAD_____

Other_____

Emergency Contact List II: Federal Emergency Support Functions (ESFs)
For more detail: http://www.fema.gov/media-library-data/20130726-1825-25045-0604/emergency_support_function_annexes_introduction_2008_.pdf

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_____

Jurisdictional ESFs: _____

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	Terrorism Planning Assessment Matrix			High level of leadership
Assessment	No assessment done	Limited assessment completed and some relationship 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

Date_____ Minimum Level Optimum Level

APPENDIX C

GLOSSARY AND ACRONYMS

In the interest of space, the information listed in this Appendix is limited to key terms. For a more complete list, please visit: http://www.fema.gov/national-response-framework.

ACTIVE SHOOTER: An active shooter is an individual actively engaged in killing or attempting to kill people in a confined and other populated area. In most cases, active shooters use firearms and there is no pattern or method to their selection of victims.

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.

COMPLEX COORDINATED ATTACK (CCA): A synchronized hostile attack conducted by two or more semi-independent teams of trained attackers at multiple locations in close succession, and employing one or more of the following: firearms, explosives, or fire as a weapon.

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, predelegated 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 INCIDENT STRESS MANAGEMENT (CISM): An intervention program developed specifically for dealing with traumatic events. It can include pre-incident preparedness to acute crisis management to post-crisis follow-up. Its purpose is to enable first responders to return to their daily routine more quickly, and help avoid further traumatic impact in their lives.

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 was replaced by Presidential Policy Directive 8 (PPD-8, referenced below). This directive established policies to strengthen the preparedness of the United States to prevent and respond to threatened or actual domestic terrorist attacks, major disasters, and other emergencies by requiring a national domestic all-hazards preparedness goal, establishing mechanisms for improved delivery of Federal preparedness assistance to State and local governments, and outlining actions to strengthen preparedness capabilities of Federal, State, and local entities.

GAP ANALYSIS: A technique used to determine what steps need to be taken in a process in order to move from its current state to its desired, future state.

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: The National Preparedness Goal identified five mission areas, in which it groups the 32 core capabilities (the distinct critical elements needed to achieve the goal). https://www.fema.gov/mission-areas

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 2013 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.

PPD-8 is organized around six elements.

- The National Preparedness Goal states the ends we wish to achieve.
- The National Preparedness System describes the means to achieve the goal.
- National Planning Frameworks and Federal Interagency Operational Plans explain the delivery and how we use what we build.
- An annual National Preparedness Report documents the progress made toward achieving the goal.
- An ongoing national effort to build and sustain preparedness helps us maintain momentum.

RECOVERY: The National Disaster Recovery Framework is a guide that enables effective recovery support to disaster-impacted States, Tribes, Territorial and local jurisdictions. It provides a flexible structure that enables disaster recovery managers to operate in a unified and collaborative manner. It also focuses on how best to restore, redevelop and revitalize the health, social, economic, natural and environmental fabric of the community and build a more resilient Nation. https://www.fema.gov/national-disaster-recovery-framework

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
CERT	.....	Community Emergency Response Team
CISM	.....	Critical Incident Stress Management
COG	.....	Continuity of Government
COOP	.....	Continuity of Operations Plan
DMORT	.....	Disaster Mortuary Operational Response Team
EMAC	.....	Emergency Management Assistance Compact
EOP	.....	Emergency Operations Plan
FEMA	.....	Federal Emergency Management Agency
HSPD	.....	Homeland Security Presidential Directive
ICS	.....	Incident Command System
IED	.....	Improvised Explosive Device
IMT	.....	Incident Management Team
IT	.....	Information Technology
JIC	.....	Joint Information Center
JTTF	.....	Joint Terrorism Task Force
NG	.....	National Guard
NICC	.....	National Infrastructure Coordination Center
NIMS	.....	National Incident Management System
NRF	.....	National Response Framework
NTAS	.....	National Terrorism Advisory System
PIO	.....	Public Information Officer
POD	.....	Point of Distribution
PPD	.....	Presidential Policy Directive
PPE	.....	Personal Protective Equipment
SOP	.....	Standard Operating Procedure
TLO	.....	Terrorism Liaison Officer
UC	.....	Unified Command
U/FOUO	.....	Unclassified/For Official Use Only
USNORTHCOM	.....	U.S. Northern Command
UTL	.....	Universal Task List
VOAD	.....	Volunteer Organizations Active in Disaster

APPENDIX D

WHAT EVERY FIRE DEPARTMENT SHOULD EVALUATE FOR TERRORISM EVENTS

It may be overwhelming to try and consider every possible scenario that a terrorist could perpetrate in any given jurisdiction, but based on history we know that terrorist often use weapons that are readily available.

Those weapons would include guns, explosives and incendiary devices. Armed terrorists with IED support were used in Madrid, London, Mumbai and Paris. All of these events caused the same basic outcome.

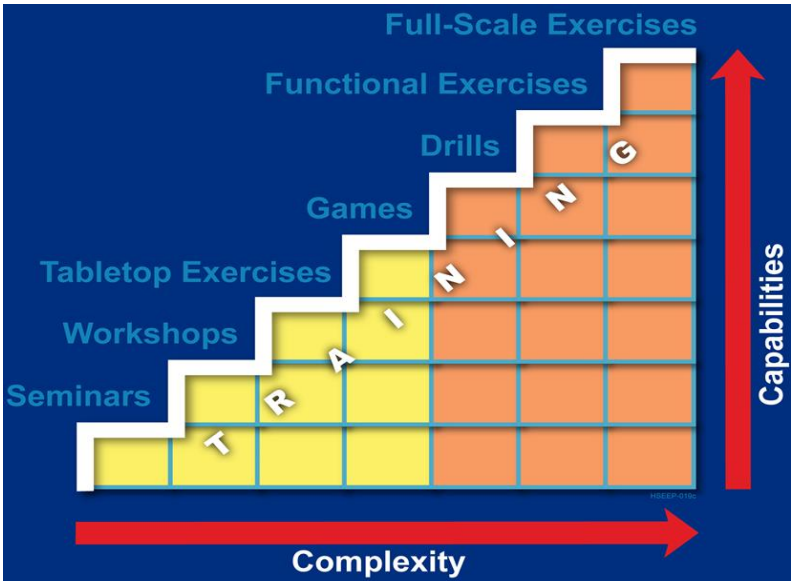
That outcome included mass casualty and mass fatalities in those localities. The question to ask is does your organization have the planning, training and equipment needed to handle such an event and if the answer is no then where would you get the support that is needed to manage such an incident.

These types of events are almost always larger than any one agency can manage by itself.

- **What are your capabilities?**
- **How do you get what you need?**
- **How can you successfully mitigate the event?**

	Action Items
Interagency Relationships	• Develop relationships with local and state law enforcement agencies. Identify outside agencies that would assist with managing this type of event. Ensure that you have interoperable communications. • Consider developing relations with internal and external partners who are critical to accomplish the mission. Such partners include: Local police department, dispatch center, FBI Local Office, Local and State Fusion Centers https://www.dhs.gov/national-network-fusion-centers-fact-sheet • Establish mutual aid agreements with response partners and neighboring jurisdictions. • Identify and train decision makers that can support your local Emergency Operation Center. • Understand your local government, non-profit, and private sector partner interdependencies in response to terrorist acts.
Situational Awareness/Intelligence	• **Stay informed** Consider developing relations with internal and external partners who are critical to accomplish the mission. Such partners include: Local police department, dispatch center, FBI Local Office, Local and State Fusion Centers https://www.dhs.gov/national-network-fusion-centers-fact-sheet • Share information within your department by adopting a notification system and develop standard operating procedures to train your internal staff. Inform your partner of the action you are taking to improve joint situational awareness. • **Suspicious Activity Reporting** Develop outreach programs to encourage the community to report suspicious activities to trusted sources. https://www.dhs.gov/see-something-say-something • **Overview of the Intelligence Community** Understand the inter-agency communication and working relationship at the local, regional, State, and Federal level.

	Action Items
Planning	**Perform an audit of the plans that you have developed as follows:** • Coordinate planning efforts with local response agencies to understand roles and responsibilities before, during, and after terrorist incidents. • Utilize non-traditional responding agencies or non-profit organizations such as schools, transit authorities, local relief organizations, faith-based partners, private sector to support community response actions to result in evacuation, family reunification, and sheltering-in-place. http://www.nvoad.org/ http://www.fema.gov/blog/2012-08-24/faith-based-community-organizations-whole-community-approach-emergency-management • Apply national standards and templates to fit your jurisdiction needs. • Develop a planning schedule for revisions. • Ensure your community has plans for active shooter response, bomb response, multi casualty, CBRNE, and cyber-attack. https://www.dhs.gov/cybersecurity-training-exercises • Establish a Continuity of Operations Planning Program to ensure agency and government essential functions continue to operate during response and recovery phases.
Training & Exercises	• Align training and exercise program to support developed plans and multi-agency coordination. • Conduct an audit of past training and exercises that has been completed. • Extend training and exercise opportunities to local and regional partners. • Document using Homeland Security Exercise and Evaluation Program (HSEEP)-2013 program guidelines • http://wwwhttp://www.fema.gov/media-library-data/20130726-1914-25045-8890/hseep_apr13_.pdf https://apps.usfa.fema.gov/nfacourses/catalog/search?courseKeywords=emergency+response+to+terrorism • Maintain training records. 

	Action Items
Training & Exercises	**Exercise Types** • **Seminar:** Informal discussion, designed to orient participants to new or updated plans, policies, or procedures. • **Workshop:** Resembles a seminar, but results in tangible products such as a draft plan or policy (e.g., a Training and Exercise Plan Workshop is used to develop a Multi-year Training and Exercise Plan). • **Tabletop Exercise (TTX):** Involves key personnel discussing simulated scenarios in an informal setting. TTXs can be used to assess plans, policies, and procedures. • **Games:** Simulation of operations that often involves two or more teams, usually in a competitive environment, using rules, data, and procedure designed to depict an actual or assumed real-life situation. • **Drill:** Coordinated, supervised activity employed to test a single, specific operation or function within a single entity (e.g., a fire department conducts a decontamination drill). • **Functional Exercise (FE):** Examines and/or validates the coordination, command, and control between various multi-agency coordination centers (e.g., emergency operation center, joint field office, etc.). A functional exercise does not involve any "boots on the ground" (i.e., first responders or emergency officials responding to an incident in real time). • **Full-Scale Exercises (FSE):** Multi-agency, multi-jurisdictional, multi-discipline exercise involving functional (e.g., joint field office, emergency operation centers, etc.) and "boots on the ground" response (e.g., firefighters decontaminating mock victims). 

	Action Items
Equipment needs	▪ Ensure that all of your personnel have the correct type of PPE pertinent to the wearing of local, State and federal laws. Ensure they are trained and certified to use this equipment. ▪ Standardize equipment deployment and use through documented policies and standard operating procedures ▪ http://www.nfpa.org/press-room/news-releases/2007/nfpa-standards-for-first-responder-personal-protective-equipment-adopted-by-us-department ▪ Consider equipping and training personnel to use Tactical Emergency Casualty Care Kits ▪ http://www.naemt.org/education/tecc/tecc ▪ Ensure radios and other communication methods are interoperable with law enforcement agencies. ▪ CBRNE equipment- PPE, Detection and Monitoring and DECON equipment. https://www.osha.gov/SLTC/emergencypreparedness/cbrnmatrix/index.html
Other Key Considerations	• **Public Information:** Do you have a PIO that is trained to deal with large-scale media events? • **Family Assistance:** Can you establish Family Assistance Centers to help with family reunification? • **Mass care:** Mass care is feeding and sheltering displaced persons. You will also need to handle large numbers of responders from other organizations that will come to your event. http://nationalmasscarestrategy.org • **Mass fatality:** Do you have plans and procedures to handle a large number of fatalities? http://www.massfatalities.com/index.html • **Cyber-security:** Have you conducted a Business Impact Analysis to determine the recovery strategies if you lose your technology capabilities? https://www.dhs.gov/topic/cybersecurity

APPENDIX E

TERRORIST ATTACK CHECKLIST

Fire Departments should conduct a self-assessment to determine if they can manage this type of incident and that they can communicate, and operate with multiple response agencies in a safe and effective manner.

	Action	Resources
Command and Control	Determine what is needed to manage a terrorist event. ☐ Planning ☐ Training ☐ Exercises ☐ Equipment	http://training.fema.gov/emiweb/is/icsresource/index.htm http://training.fema.gov/is/crslist.aspx
Communications	Identify methods of communication to request aid. ☐ Planning ☐ Training ☐ Exercises ☐ Equipment	http://www.iafc.org/files/commComm_GuideRadioCommForFireServ.pdf
Operations	Preparing for all types of response. ☐ Planning ☐ Training ☐ Exercises ☐ Equipment	1. Size up situation 2. Identify contingencies 3. Determine Objectives 4. ID needed Resources 5. Develop Plan 6. Take Action

APPENDIX F

COMPLEX COORDINATED ATTACK SCENARIO CAPABILITY ASSESSMENT WORKBOOK

A Complex Coordinated Attack (CCA) is a synchronized hostile attack conducted by two or more semi-independent teams of trained attackers at multiple locations in close succession, and employing one or more of the following: firearms, explosives, or fire as a weapon.

Instructions for completion

The following worksheets are designed to capture the plans, equipment, training, and exercise requirements necessary to enable a successful response to a specifically defined Complex Coordinated Attack (CCA) scenario. This scenario provides an example of a possible CCA and does not define all possible types of CCAs.

> For planning purposes, the scenario consists of simultaneous—or near-simultaneous—attacks at two venues (examples include: two attacks in a single jurisdiction; two attacks in two different jurisdictions; an attack within the transportation system and at another location; or an attack within a school or place of gathering and against a soft target). The attacks are carried out with assault style rifles and there is an improvised explosive device (IED) at one of the locations. There are at least 100 victims (injured or dead). The attackers may or may not be holding hostages for protection, not negotiation.

Examples (shaded and in italics) for each type of requirement are included. These examples are not meant to be all inclusive or necessarily something that every jurisdiction will need to address.

Planning
List all applicable plans required by your jurisdiction to effectively respond to a CCA. Examples would include strategic, operational, and tactical plans, policies, standard operating procedures, general orders, guides, protocols, mutual aid agreements, checklists, and other publications that comply with relevant laws, regulations, and guidance necessary to perform assigned missions. After identifying necessary planning-related documents, please use columns 2-5 to provide the following information: ▪ **Does the Plan Exist**: Using YES or NO, indicate if the necessary plan, policy, or procedures currently exists. ▪ **Last Updated**: Indicate when the plan, policy, or procedures was last updated. ▪ **Trained:** Using YES or NO, indicate if appropriate personnel have been trained on the plan, policy, or procedures. ▪ **Coordinated:** Using YES or NO, indicate whether the plan, policy, or procedures has been coordinated with other regional entities outside your jurisdiction.

Applicable Plans	Have Plan	Last Updated	Trained	Coordinated
Complex Coordinated Attack Annex to the Emergency Operations Plan				
Mass Casualty Incident Plan				
General Order for Coordinated Tactical Response to Multiple Active Shooter Terrorist Incidents				
Special Weapons and Tactics (SWAT) / Explosive Ordnance Disposal (EOD) Integration Policy				
Police / Fire-EMS Integration Policy / Force Protection Plans				
Rescue Task Force Standard Operating Procedure				

Resources

Include a list of all specialized resources within your jurisdiction necessary to respond to a CCA. This includes equipment, personnel, supplies, facilities, and systems that comply with relevant standards necessary to perform assigned missions and tasks associated with the CCA scenario.

Please use columns 2-5 to provide the following information:

- **Required:** Indicate the quantity of the resource necessary to address a CCA.
- **Available:** Indicate the quantity of the resource that your jurisdiction currently possesses.
- **Trained:** Using YES or NO, indicate if training is provided on the resource.
- **Coordinated:** Using YES or NO, indicate whether the resources is deployable for mutual aid with other jurisdictions.

Required Equipment	Required	Available	Trained	Coordinated
SWAT/Tactical Team				
Bomb Squad/Explosives Team				
Ballistic protection equipment for Fire-EMS				
Low light specialized equipment				
Tactical blow-out kits				
Hazmat Team				

Training and Exercises		
Training and exercises required to prepare responders to address a non-static complex coordinated attack. It is not necessary to include training associated with the plans or equipment indicated in the previous worksheets. For each training, please use columns 2-3 to indicate the following: ▪ **Offered:** Mark this column YES or NO to indicate whether or not the training/exercise is currently offered to your jurisdictions' responders. ▪ **Regional**: Mark this column YES or NO to indicate whether or not the training/exercise, as currently offered, is available/applicable to regional partners		
Required Training or Exercise	**Currently Exist**	**Regional**
First responder training for response to Complex Coordinated Attacks		
Complex Coordinated Attack Seminars for Elected Officials and Senior Leaders		
Multiagency Response Drills		
Unified Command/Area Command Exercise Series		
Tactical Emergency Casualty Care Drills		

APPENDIX G

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. The result of that effort was this document, Terrorism Response: A Checklist and Guide for Fire Chiefs and Community Preparedness Leaders, also known as the Checklist and Guide. Now in its 4th Edition, the Checklist and Guide continues to further that original IAFC vision to deliver practical and current homeland security advice that is flexible and adaptable within the fire service and the broader public safety community.

The authors of this guide were senior fire officers and public safety officials representing a cross-section of the IAFC's membership, expertise, and geographic diversity.

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 Searns

4th EDITION REVISION COMMITTEE
Emergency Services Manager Patrick M. Collins, Prince William County, Virginia
Captain C.A. Leif Ericson, Prince William County VA Department of Fire and Rescue
Assistant Chief Michael Little, Los Angeles Fire Department
Assistant Chief Matt Smolsky, Prince William County VA Department of Fire and Rescue

APPENDIX H

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.


25-4

www.iafc.org