

CRITICAL RESEARCH/INNOVATION FOCUS AREA DOCUMENT

Improvised Explosive Device (IED) Warnings

**Dr. Ruth Doherty
Counter Improvised Explosive Devices (C-IED)
U.S. Department of Homeland Security, Science and
Technology (S&T) Directorate**

**May 4, 2009
Version 1.0**

Please note that as more details are available, DHS will post updated research/innovation focus area overviews on the FutureTECH website. This is a pre-decisional draft document of the NSTC Subcommittee on Domestic IEDs. Please contact Dr. Ruth Doherty, ruth.doherty@dhs.gov for more information.

Who?

Identify any DHS component stakeholders that contain or represent potential end users. Also name any Capstone IPT (refer to http://www.dhs.gov/xres/programs/gc_1234200779149.shtm and the article entitled "Making it Easier to Work with DHS"), if any, which identified a capability gap related to this research/innovation focus area.

The U.S. Department of Homeland Security (DHS) leads for CIEDs are the Office for Bombing Prevention and United States Secret Service (USSS). The corresponding DHS Science and Technology (S&T) Capstone IPT that identified capability gaps related to this focus area is entitled "Counter-IED."

The threat of an improvised explosive device (IED) attack is shared almost universally by U.S. communities, private sector enterprises and public sector agencies and across the 18 sectors of the nation's critical infrastructure and key resources (CI/KR) owners and operators. Consequently, the community of interest for this research effort includes public officials and agency leads across the range of U.S. jurisdictions and communities at the federal, state, regional and local levels.

What?

Describe a required technology/capability. Describe how a technology will provide the capabilities and functional improvements needed to address the DHS need. Do not describe a specific technical solution. Instead, describe a conceptual technology for illustrative purposes. Define typical missions that the proposed technology could be utilized to accomplish.

Government officials, civic leaders, media representatives, law enforcement officials and emergency managers need to properly delineate and issue hazard/risk warnings to the public prior to an imminent or suspected IED attack and provide appropriate protective actions and post-attack instructions.

Specific stakeholders in this effort include:

- Office of the President and White House Staff
- Department of Homeland Security
- DHS/FEMA
- Department of Justice
- Equivalent agency heads at the state, regional and local levels
- Governors' offices nationwide
- Local elected officials, e.g., Mayors and County Executives
- Local law enforcement, public safety and emergency management officials

The development of a data structure and analysis program (and accompanying training materials) that will support federal, state, local, tribal and private sector partners having specific roles and responsibilities within their communities for public safety and security against IED attacks is required. Development of hazard and risk warnings to the public in imminent threat of or immediately after a terrorist IED attack will incorporate the following requirements:

- Detailed responses and methodologies to appropriately inform and protect the public during terrorist explosive attacks. This should involve members of professional press and media with local officials and emergency managers.

Please note that as more details are available, DHS will post updated research/innovation focus 2 area overviews on the FutureTECH website. This is a pre-decisional draft document of the NSTC Subcommittee on Domestic IEDs. Please contact Dr. Ruth Doherty, ruth.doherty@dhs.gov for more information.

- Consistent and repeatable methods to inform and employ the public in identifying suspicious circumstances or abnormal conditions in local communities that could serve as warnings to local authorities of terrorist attack planning or potential IED events
- Development and testing of guidelines for government and civic leaders in issuing effective emergency communications in the event of an IED attack
- Technology that will rapidly provide accurate status information from forensic and law enforcement agencies to government officials and leadership, and public safety and security personnel with near real-time updates
- Pre-planned responses and messages that have been crafted, analyzed, tested and rehearsed by civic officials and members of the media and press corps to provide accurate instructions and reassurances to the public
- Development of local models and simulation-based games to exercise first responders and local government leaders in potential scenarios and test courses of action to support and protect local populations
- Development of simulations to analyze effects on transportation and public infrastructures, local economies and tempo of civic life in the event of an IED attack or terrorist campaign employing IEDs, and to analyze and test alternate approaches to managing the consequences

References:

- a. HSPD-19 Section 4(a, d)
- b. HSPD-19 Implementation Plan (draft) Task Ref: 2.3.4, 3.

Why?

Describe the analysis and rationale for requiring a new technology/capability. Describe why existing technologies cannot meet current or projected requirements. Describe what new technologies/capabilities are needed to address the gap between current capabilities and required capabilities.

The United States has little experience in dealing with an immediate threat of attack that could affect individual American citizens in their own communities. Likewise, civic officials have very little awareness or training in how to instruct the public properly regarding the safety measures they should take during terrorist attacks or similar extraordinary events. Officials' experience is generally centered on managing public information and security during serial murders or kidnappings; civil unrest, gang violence and inner city crime waves; and rare events exemplified by the 1979 Three Mile Island event, the Unabomber attacks from 1978 to 1995, and the anthrax and sniper attacks in the Washington, D.C., metropolitan area in 2001 and 2002 respectively. Criminologists or terrorism experts serving local law enforcement or the FBI have formulated most instructions to the public and senior law enforcement officials have issued them.

The ability to provide information quickly and accurately is critical to preserving public confidence at the local level and generating awareness, cooperation and support of the public in identifying abnormal or suspicious events that might indicate imminent danger or precursor activities to an IED attack.

There are two challenges involved in this effort: 1) protecting the public from initial and successive IED events especially in the face of a general lack of official knowledge of the unfolding scenario;

Please note that as more details are available, DHS will post updated research/innovation focus 3 area overviews on the FutureTECH website. This is a pre-decisional draft document of the NSTC Subcommittee on Domestic IEDs. Please contact Dr. Ruth Doherty, ruth.doherty@dhs.gov for more information.

and 2) maintaining public confidence in the face of potential threats. Public confidence is important in preserving public conviction at the local level and generating awareness, cooperation and support of the public at the local level in identifying abnormal or suspicious events that might indicate imminent danger or precursor activities to an IED attack.

When?

If a technology/capability is intended as a countermeasure to a threat, summarize the threat to be countered and how the technology could be used (i.e., concept of operations). If applicable, provide a schedule/timeframe to capture when the technology/capability is needed in order to address the DHS gap.

The terrorist threat facing our nation's critical and civic infrastructure can take many forms including vehicle bombs, suicide attacks or combinations thereof. This includes attacks such as those seen in the Beslan School or the Moscow Theater, which combine armed attackers, hostages and IEDs. In the event that IED attacks were to occur – or worse, that a campaign of terrorist use of explosives employing such methods were to be launched on U.S. soil – authorities must quickly provide the American people with accurate information about the nature of the threat. Authorities also must provide guidance on protective actions and precautions that Americans might take to improve security in their communities and reduce the risks to them and their families.

Where?

Describe the projected threat environment in which the technology/capability may be potentially deployed.

If terrorists stage a coordinated attack or multiple attacks against the American people using IEDs, vehicle-borne improvised explosive devices (VBIEDs) or suicide bombers against targets within communities and public gathering places, the problems presented will be significantly more complex and will likely have national implications. In a free and open society, it is impossible to ensure the constant safety of people and the certain protection of targets against terrorist attacks. Nevertheless, there are in fact steps that authorities can and should take at the local, regional and national levels to inform the public and manage the security problem posed by terrorism.

Please note that as more details are available, DHS will post updated research/innovation focus 4 area overviews on the FutureTECH website. This is a pre-decisional draft document of the NSTC Subcommittee on Domestic IEDs. Please contact Dr. Ruth Doherty, ruth.doherty@dhs.gov for more information.