PREPAREDNESS
LEADERSHIP
COUNCIL
INTERNATIONAL

A changing global threat environment, coupled with increasingly interdependent societies and aging infrastructures, is a dangerous combination that must be address by today's preparedness leaders.

October 2014

REPORT:

Explosives

Prevent, Detect, Deter

"Left of Boom"

Catherine L. Feinman

Foreword by Charles Guddemi

Published by The IMR Group, Inc.
Distributed by DomesticPreparedness.com
Severna Park, Maryland

Explosives
"Left of Boom"

By Catherine L. Feinman

Foreword by Charles Guddemi

The Preparedness Leadership Council International

The Preparedness Leadership Council International (PLC), formerly the DomPrep40, is a thought leadership group comprised of insider practitioners and opinion leaders who offer advice and recommendations on topics relevant to emergency planners, responders, receivers, local-state-federal authorities, nongovernmental organizations, and the private sector. Focusing primarily on prevention, protection, response, recovery, and mitigation, the PLC is tasked to develop quantifiable and qualitative feedback from surveys and roundtable discussions that is gathered from and shared with a broad multidiscipline, multijurisdictional audience of operational professionals and policy advisors. Information is shared via the publications: DomesticPreparedness.com (online and mobile), DPJ Weekly Brief (email newsletter), and the *DomPrep Journal* (PDF download).

DomesticPreparedness

DomPrep is a thought-leadership information service for the preparedness community. Created in 1998, DomPrep offers content – provided by practitioners, subject matter experts, and DomPrep Advisors – to more than 25,000 first responders, medical receivers, emergency planners, local-state-federal authorities, nongovernment organizations, and private sector professionals.

Downloadable reports, articles, audio-video clips, podcast interviews, and information gathered from Executive Briefings are widely used by the multidiscipline, multi jurisdictional audience that DomPrep serves. The professionals who help plan for, respond to, and recover from any emergency incident or special event are invaluable to their communities. As such, all open-access and premium content (registration required) is available to these professionals free of charge.

Note: All comments provided in this report reflect the opinions of the individuals and do not necessarily represent the views of their agencies, departments, companies, or organizations. Quotes within the report without acknowledgment were made anonymously by survey respondents.

IMR Group Inc., 517 Benfield Road, Suite 303, Severna Park, MD 21146, USA; phone: 410-518-6900; email: subscriber@domprep.com; also available at www.DomesticPreparedness.com

TABLE OF CONTENTS

~ This page was left blank intentionally ~

ACKNOWLEDGMENTS

This is the first report generated by the newly created Preparedness Leadership Council International (PLC) and it needed to be right. I believe we reached that objective and, for that, I am grateful to many people.

The PLC recently transitioned from the DomPrep40. The difference between those two organizations is that DomPrep40's Executive Briefing series came to tell and present a report. The PLC model, though, organizes working groups of subject matter experts and comes to ask. I have the privilege of thanking 31 distinguished subject matter experts who met in Washington, D.C., on 12 June 2014, plus 521 DomPrep professional readers and more than 500 private citizens for responding to surveys and sharing thoughts, insights, perspectives, and concerns, which are shared in this report.

That input was generated through the probing and questioning skills of Charles Guddemi, who is a well-known federal law enforcement professional to whom I hold the greatest respect. When I asked him to be the lead on the Explosives Working Group, he agreed, but only if this work would make a difference. I am certain the many actionable items included in this report will do just that for practitioners and policymakers. Thank you, Charlie.

Also, a special thank you to the author of this report, DomPrep's editor, Catherine Feinman. Cathy had a tremendous amount of data to sift through while looking for a "so-what." She captured it by making the report not just about improvised explosive devices, but also about a greater and nagging question, "Where do we balance security versus privacy?" The analytics presented show the reader that U.S. citizens feel threatened and trust/expect their government authorities to keep them safe, while still respecting the nation's Constitution. Good job, Cathy.

Plus, thank you to our underwriters, BioFire Defense, Emergent BioSolutions Inc., FLIR Systems Inc., QuickSilver Analytics, and Thermo Scientific Inc. Without their financial support, this good work would not have been possible. Finally, thank you Susan Collins, Carole Parker, and Lawrence O'Connell for your professional staff support and assistance. You made it happen.

Martin D. Masiuk
Executive Director
Preparedness Leadership Council International

~ This page was left blank intentionally ~

FOREWORD

When asked to lead the Preparedness Leadership Council's Explosives Working Group, I recognized the challenge of narrowing and defining the scope of such a broad topic. By the time an explosion occurs, we are too late – people are dead, infrastructure is destroyed, people are distraught, and national security is destabilized. The only way I would agree to take on this project is if I thought it could make a difference. By focusing on the "left of boom," we have the opportunity to prevent, detect, and deter explosive devices and the people behind them, whose objectives are to cause death and destruction.

To stay left of boom requires taking into account many factors that contribute to the success or breakdown of preventative security measures. Although there is no definitive formula, all of the following should be considered:

- Accurate and effective intelligence sharing to understand the severity of the current threat environment;
- Lessons learned from overseas deployments of agencies such as Department of Defense's Joint Improvised Explosive Device Defeat Organization (JIEDDO);
- The perspective of the "boots on the ground" – law enforcement and first responders – who are responsible for the prevention, detection, and deterrence within their local jurisdictions;
- The importance of the private sector, especially in terms of critical infrastructure;
- Science, technology, and industry's new concepts, laboratory prototypes, and emerging technologies;
- Training to develop effective methods and continuous reinforcement of identifying the proper behavioral indicators, pre-operational surveillance detection, and proper use of deployed technology in the field;
- Legal issues related to the First and Fourth Amendments of the U.S. Constitution; and
- Cybersecurity as the interconnected cyberworld continues to grow.

There are obstacles, though. Gaps in coverage and policies, as well as ongoing funding concerns have led to incident-driven response rather than prevention-driven investment. In the science and technology industry, for example, the development of new technologies is cyclical. Therefore, the explosive detection equipment available now likely will remain unchanged until the next major incident occurs.

In addition, some techniques that law enforcement agencies use to acquire and analyze information are burdened with legal issues. As a result, some pieces of the puzzle may not be as readily available as they once were due to privacy concerns voiced by the public and mainstream media. The best defense is to educate the public and facilitate ways for them to report critical information.

This report provides a snapshot of where the nation stands and guidance on where we need to go based on the roundtable and survey participant's perspectives. With 23 years in law enforcement, I have worked, trained, and travelled with numerous smart and dedicated people that I can count on for support and information. Discussions that began with that network of professionals continue in this report, but should not stop here. Through engagement and discussions within and between agencies and the public, solutions can be created to stay left of boom.

Charles Guddemi
Federal Law Enforcement Officer

SUMMARY

Discussions about improvised explosive devices (IEDs) often begin with the 2001 al-Qaida attacks on the U.S. mainland, the first such attacks since the War of 1812. “Where were you on 9/11?” asked Charles Guddemi, a federal law enforcement officer, as he called the Preparedness Leadership Council International (PLC) roundtable to order at the United States Park Police Anacostia Operations Facility in Washington, D.C., on 12 June 2014. On 9/11, Guddemi was a sergeant at the United States Park Police with duties at the Statue of Liberty and Ellis Island, “When those towers went down, the earth shook on both islands…. And now, most of us spend all of our waking and sleeping hours defending our liberties.”

At the June roundtable, 31 senior subject matter experts representing six communities of interest – defense; first responder (law enforcement, fire, emergency medical services); intelligence; science, technology, and industry; critical infrastructure; and legal – addressed the topic of explosives and IEDs as they relate to pre-incident (“left of boom”) prevention, detection, and deterrence. From this discussion, the PLC created two nationwide surveys for DomPrep’s audience and the general public to provide additional input and comments. The information provided by 521 DomPrep readers and more than 500 members of the public who responded to the survey have informed this report.

Key Issues

I. *Defining Success* – A concept of operations with a clear definition for success is necessary for both government and private sector ventures, with risk reduction and a balance between cost and benefit being key drivers.

II. *Necessary Investments* – Investments in resources and trainings are critical, but it also is important to recognize the capabilities that already exist, but are not being used to full potential because of policy and/or gaps between agencies.

III. *Current & Future Threats* – By understanding supply chains and the high-tech/low-tech continuum for terrorist actions, practitioners and citizens in many disciplines and jurisdictions could help provide early warning to intelligence officials.

IV. *Protection vs. Privacy* – Technology exists or is being developed to provide better surveillance and information gathering, but the nation is divided on whether to place greater emphasis on protecting constitutional rights or protecting life and safety.

~ This page was left blank intentionally ~

I. DEFINING SUCCESS

In the first few minutes of the roundtable, Cathy L. Lanier, chief of police for the Metropolitan Police Department (MPD), shared an MPD case study involving protests directly related to the 2004 annual International Monetary Fund/World Bank (IMF/WB) conference. The main venue for the conference was located just two blocks from the White House, with guests staying at 16 area hotels. The month before the conference, intelligence reports exposed extensive surveillance of IMF/WB by Pakistan-based terror groups – details about the thickness of window glass, timing of lights, pedestrian traffic, and other sensitive data had been exposed. As a result, planners quickly developed a new security plan. Security personnel met with hotel managers to share information that could prevent hotel personnel from falling victim to al-Qaida tactics. These recommendations included:

- Do not hire people without thorough background checks;
- Do not allow cars to approach the front of the hotel before or during the event;
- Conduct bomb sweeps in garages;
- Close underground parking garages located under the event venues, whenever possible; and
- Have a visible police presence at all times in the areas of concern at least two weeks before the event.

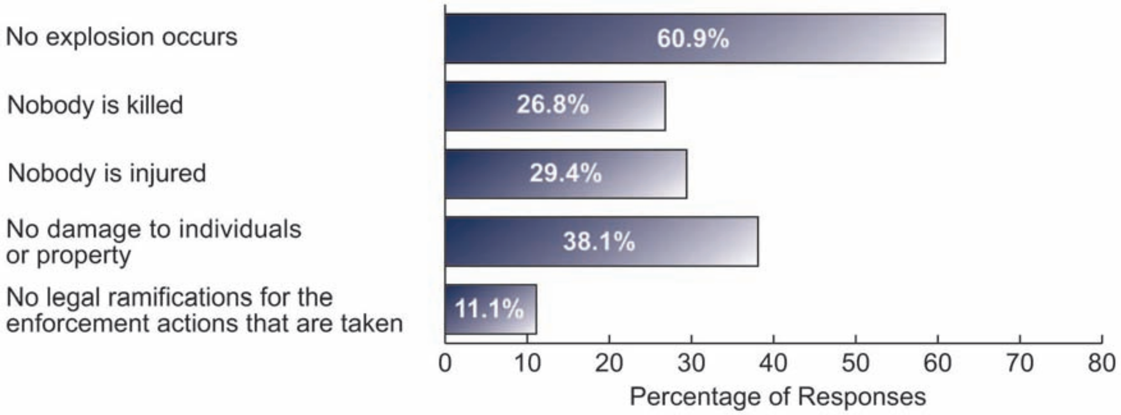
The strong relationships that MPD has with local hotels enabled the agency to use unusual security measures, including: visible police presence, undercover intelligence officers located in and around hotels, physical searches of pedestrians within the restricted area, ban on vehicular traffic for 20 blocks, closure of underground parking garages, and temporary suspension of trash pickups during the event. Although all of those measures met the objectives of detecting, deterring, and preventing an attack, Lanier added that the "success" of that event included not suffering legal ramifications – lawsuits – for the MPD's preventative actions.

Avoiding Death, Injury & Property Damage

For risk management and risk mitigation, defining "success" can vary between agencies and for different events. In the IMF/WB case, Lanier pointed out that there were many requests from the American Civil Liberties Union and other civil liberties organizations for injunctions to remove physical barriers and/or halt other preventative law enforcement activities. Such requests are an ongoing issue for security agencies.

Figure 1

How do you define "success" as it relates to detecting, deterring, and preventing attacks? (Choose one or more of the following)



"Success," as it relates to counterterror and counterinsurgency operations or to explosives and IEDs, is especially difficult to define in a nation with diverse populations and perceptions. In many cases, success or failure often is determined by how the incident is portrayed by the media. The DomPrep survey results found that, when it comes to detecting, deterring, and preventing attacks, some respondents (29.4 percent) define "success" as no one being injured, others (26.8 percent) when no one is killed, and others when there is no damage done to individuals or property (38.1 percent). However, the majority of respondents (60.9 percent) define success as no explosion at all (Figure 1), "A successful prevention is one where there is little public recognition that a situation existed."

No explosion and little or no public recognition of a potential incident may raise other concerns for leadership and intelligence agencies because, if a threat is not recognized, then there may be no perceived need to continue funding or supporting efforts to address similar threats. Some respondents go a step further by defining "success" as: apprehending the guilty party; holding perpetrators accountable and not releasing them back to their homelands; publicizing prosecutions with sentences that eliminate the opportunity for further actions; and/or breaking up the "cell" that planned the attack.

Although no explosion, no deaths, no injuries, and no property damage are the best scenario, some respondents stated that they would consider any of the scenarios listed in Figure 1 a success depending on the circumstances. Sometimes the best outcome is to minimize the extent of damage, reduce the effect on people and infrastructure, and avoid legal ramifications for actions taken (11.1 percent).

Lessons Before, During & After 9/11

The 9/11 attacks had a significant effect on the psyche of U.S. citizens. Any perception that such attacks only happen in other countries was shattered, and pressure to do anything and everything necessary to protect the homeland was enormous. More than a decade later, the memories of that tragic day and the events that followed are beginning to fade. The influx of federal money for preparedness efforts has dwindled, or all but disappeared. In the absence of another 9/11 – whether because the terrorists have not made the attempt or because preventative efforts have been successful – there is less support for and funding of new efforts. This leaves soft targets such as hotels and large public venues more challenging to protect.

Before 9/11, London officials had implemented changes to security and response doctrine following the 1995 sarin nerve gas attack in the Tokyo underground to address the threat of IED attacks. It was at that time the mindset of planers changed from "might happen" to "will happen," and this new acceptance drove new measures. For example, firefighters were trained to wear chemical protection suits and drive underground trains out of tunnels in case of a terrorist attack.

Then, on 7 July 2005, the London transportation system was the target of a series of suicide bombs, referred to as the "7/7" bombings. Although the Irish Republic Army (IRA) had repeatedly bombed London over previous decades during the IRA uprising, the 2005 bombings were different. The IRA primarily targeted infrastructure to influence political change, whereas the 7/7 attacks were deliberate acts of terrorism designed to murder and maim a large number of people. Sir Ken Knight, CBE, former fire commissioner for the city of London, described the 7/7 attacks – with 52 deaths and more than 700 injured as a result – as "iconic" because the terrorists wanted to make the biggest impact (with a well-known target) and they achieved that goal.

According to Knight, responders in London realized after the 7/7 attacks that they need to be involved in the planning and risk assessment as threats and technologies change. London's homegrown suicide bombers are educated and, although they live and work in the United Kingdom, they now are turning against their own communities. To deter such attacks, London has made a significant investment in closed-circuit television (CCTV). The 7/7 attacks also inspired changes outside the United Kingdom. In New York, for example, a baggage inspection program was implemented in the city's subway system within about 48 hours to protect against a similar attack on U.S. soil.

Incidents in other parts of the world also were cause for change. For example, two separate incidents at the same hotel in Jakarta, Indonesia, resulted in worldwide changes for Marriott International Inc. Six years after the 2003 car bomb attack in front of the JW Marriott Hotel, a florist who had worked at the hotel for 5 years detonated two bombs on 17 July 2009 – one inside the same hotel that was attacked in 2003 and one in the building across the street. The attack exposed a gap in Marriott's security procedure – the security team did not screen current employees who entered the building.

To address that gap, Marriott created its own intelligence unit to conduct threat assessments before construction of any new buildings. Due to high turnover of personnel, the hotel chain continuously trains its security officers using a program that tests personnel and provides certification for accomplishments. In addition, Marriott adapted the "see something, say something" program for its hotels and personnel.

Jack Suwanlert, director of global safety and security for Marriott International Inc., noted that, "We spend so much money on dogs, on expensive explosive detectors, and on better barriers, but the best tool is security awareness…. The best way to stop the boom is to stop [terrorists] during the [pre-attack] surveillance activities." Marriott, which operates in 80 countries and often serves as a connector between the United States and local authorities, learned other valuable lessons from the 2013 Boston bombings. For example, in addition to first aid and cardiopulmonary resuscitation training, hotel staff now must also train for triage, trauma, and treatment procedures.

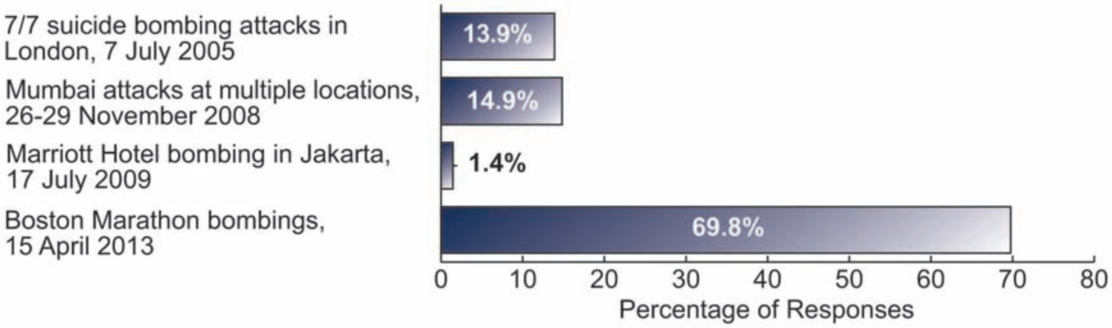
In a nationwide survey, respondents did not recognize much change resulting from the incidents that occurred overseas since 9/11, but felt that each was significant for reviewing and updating security plans (Figure 2):

- The 7/7 suicide bombings in London on 7 July 2005, as well as the 2006 transatlantic liquid explosive aircraft plot, had lasting security implications for coordinated suicide attacks on the transportation infrastructure.

- The Mumbai attacks at multiple locations on 26-29 November 2008 were significant because they demonstrated a coordinated physical attack scenario. This scenario is a concern for many municipalities about additional multiple attacks – both conventional and asymmetric – in urban environments.

Figure 2

Since the 9/11 attacks on the United States in 2001, which specific incident do you believe has spurred the greatest change in U.S. preparedness efforts?



- The Marriott and Ritz-Carlton Hotel suicide bombings in Jakarta, Indonesia, on 17 July 2009 (1.4 percent), as well as the 5 August 2003 car bomb that was detonated outside a Marriott Hotel lobby in Jakarta, caused international travel concerns to that area.

- Boston Marathon bombings on 15 April 2013 (69.8 percent) were a pivotal moment for U.S. citizens because that incident put the threat inside the borders. The Boston incident illustrated "how ordinary citizens/legal immigrants could be 'sleeper' agents for our enemies." Once again, this incident may have renewed awareness that IED attacks can occur on U.S. soil, but more preventative actions are still necessary.

Other incidents cited by respondents that have spurred change in some agencies since 9/11 include: the "shoe bomber" in 2001; the "underwear bomber" in 2009; the attempted car bombing in Times Square, New York, in 2010; the Aurora, Colorado, theater shooting in 2012; the upsurge of radical Islam; as well as wars and instability in multiple locations around the world. Some changes highlighted in the survey were positive – including increased value in medical response planning as well as greater emphasis on pre-event screening and trans-event presence. However, other changes – primarily resulting from significant reductions in homeland security and preparedness funding – have been negatively perceived. Such funding changes affect planning efforts across the nation, especially at the local level.

Pictured Left to Right: **Brigadier General Bruce Prunk**, Special Assistant, Air National Guard; **Kevin Finnerty**, Supervisory Special Agent, Bomb Technician, FBI; **Ken Comer**, Former Deputy Director Intelligence & Analysis, Joint IED Defeat Organization; **Robert MacLean**, Acting Chief of Police, U.S. Park Police; **Cathy Lanier**, Chief of Police, Metropolitan Police Department; and **Sir Ken Knight** Former Chief Fire & Rescue Advisor, England

Some respondents claim that none of the incidents listed in Figure 2 have spurred changes in preparedness, that government efforts are wrongly focused, and that the United States is still "grossly unprepared." Although changes in security posture may not have seemed significant to respondents, there is a consensus that U.S. awareness of existing threats is increasing. Despite this growing awareness, support for specific preventative efforts that may infringe on personal privacy is divided.

II. NECESSARY INVESTMENTS

Intelligence agents and first responders with the right "tools" are able to gather a tremendous amount of actionable information. For example, the Metropolitan Police Department in Washington, D.C., have shifted away from traditional source or confidential informant development focused on the narcotics trade, and now train all personnel in source development for all types of crimes. As a result, homicides have decreased more than 50 percent in the past five years. By emphasizing community policing, and having officers regularly walk through neighborhoods and speak to residents they are more likely to share information about suspicious activity, which otherwise often go undetected. Firefighters could serve as another resource for gathering intelligence from the public, but they often are underutilized in this capacity.

Federal Action & Protection

The U.S. Department of Defense Joint IED Defeat Organization (JIEDDO), which was created in 2006 from the U.S. Army's IED Task Force, has spent about $20 billion to counter the IED threat. IEDs are a never-ending and constantly changing threat and, according to Kenneth Comer, former deputy director for intelligence and analysis at JIEDDO, "No solution in that $20 billion was ever permanent, and none ever will be." For every change in tactics that JIEDDO made, adversaries were able to adapt within months. There has been a constant give and take – for every action a reaction. "We were only successful when we stopped treating [IEDs] as a law enforcement problem and started treating it as a military problem," said Comer.

The U.S. Department of Homeland Security's (DHS) Federal Protective Service (FPS) is DHS's law enforcement arm for federal facilities throughout the nation, and FPS representatives now sit on committees and are involved in working groups to help implement policies and ensure that civil rights are not violated. One challenge, though, is that certain FPS-secured facilities are open to the public – for example, the Ronald Reagan Federal Trade Center in Washington, D.C., which hosts up to 75,000 visitors in a single day. To protect such venues, FPS uses an array of preventative measures, including: itemizers, x-rays, magnetometers, off-site delivery screening, and explosive detection K-9 units.

For the United States Park Police, open venues such as the Lincoln Memorial pose significant screening challenges as well. At such venues, law enforcement officers rely on the public and other civilian employees who work nearby to use their situational awareness skills as the "eyes and ears" of law enforcement. Unfortunately, it can be challenging to balance incident response with public perception: (a) no reaction is perceived as underreacting or not doing the job; or (b) action that is later determined to be unnecessary is perceived as overreacting. Robert MacLean, acting chief of the United States Park Police, along with some of his law enforcement colleagues would “rather be criticized for overreacting for a suspicious package incident.”

Another federal agency, the U.S. Department of the Interior, owns roughly one-fifth of the country’s land – including major critical infrastructure facilities like the Hoover Dam. Such facilities, of course, must be highly secured yet they also must remain open to many daily visitors, who may have little awareness of potential threats against critical infrastructure facilities. Glenn Smith, assistant director of security for the U.S. Department of Interior, said, “I feel we are the monkeys in the middle because we’re not DHS and, if you are not DHS in the federal government, you get zero buy off on security issues. And yet, we are not a state and local [agency], so we can’t get support from DHS on our security issues.” Another challenge for Smith is having to explain the purpose of a security team within the department to new leadership that changes every few years.

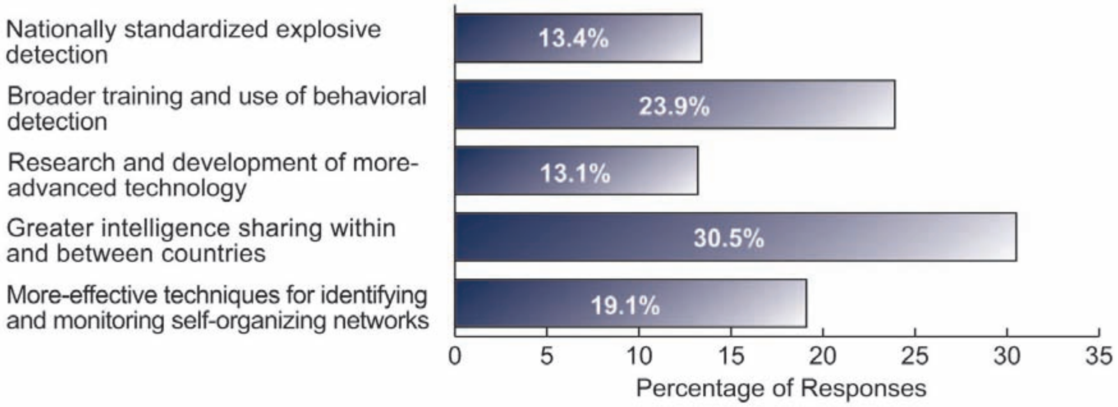
Training Across Disciplines

For consistency in IED training, the Federal Bureau of Investigation and Department of Defense co-manage a single school for training all bomb technicians across disciplines. However, after graduation, it is the responsibility of the individuals and agencies to continue training and professional development. Of approximately 430 bomb squads – with more than 3,000 bomb technicians – across the United States, the majority are part-time squads, which may not maintain an adequate level of training and professionalism as events, tactics, and technology changes. “If you cannot sustain or justify a full-time explosive ordnance disposal (EOD) element, perhaps you should rethink that or join into [a joint] agreement,” said Sergeant William Qualls, of the Massachusetts State Police EOD unit.

However, equipment and training are only part of the solution. According to Qualls, “The best tool is your intellectual toolbox, your ability to be flexible, and operate when changes arise.” Before the Boston Marathon bombings in 2013, Massachusetts State Police officers had taken advanced EOD proactive training based on operational lessons learned and best models from their UK, Israeli, and Navy EOD partners. However, even with a wealth of information about behavioral detection programs, exclusion zones, and layered security in Israel, there is a delicate balance between security in a police state and security at family-friendly events like the Boston Marathon. Qualls noted that,

Figure 3

On a federal level, what investment do you believe would be most beneficial in preventing future attacks involving explosive devices?



even K-9 handlers might not have prevented the attack because of how the bombs were packaged and how quickly they were deployed.

When asked about the investment that would be most beneficial in preventing future attacks using explosive devices (Figure 3), intelligence sharing topped the list (30.5 percent), followed by training and use of behavioral detection (23.9 percent). Although intelligence sharing often includes the exchange of information among and between federal, state, and local partners, private citizens are beginning to play a greater role in this process. One survey respondent suggested formalizing citizen training by developing a “see something, say something” training program that could be conducted in office buildings, schools, and community centers and taught by the American Red Cross, fire and law enforcement officers, or other public safety personnel.

Although behavioral detection can be effective, it also must be implemented properly with well-trained personnel. Responses about effective techniques for identifying and monitoring self-organizing networks (19.1 percent), nationally standardized explosive detection (13.4 percent), and research and development of advanced technology (13.1 percent) were almost evenly split. Risk management-based programs, situational awareness, and public education can all help raise awareness about the types of threats the nation faces.

K-9 teams are another effective way to detect explosives, but there is no standard for such training. To address this concern, the FPS currently is working with the DHS Office of Security to nationally standardize K-9 training with a 12-week program. Training by the FPS includes what to look for, how to gather intelligence, whom to contact, and how to record/report the information. Due to an increase in personal suicide bombs worldwide, K-9 teams now are available in D.C. that specialize in locating explosives on humans, which can be very different than searching packages and other items. In addition, the National Capital Region has centralized dog teams to conduct random sweeps in facilities throughout the region.

There are many benefits to K-9 explosive detection, but there also are some limitations. For example, ventilation systems in mass transit hubs can make it difficult for dogs to track a moving source inside a subway, train station, or airport hallway. Dogs also require interval rest periods, whereas equipment can operate uninterrupted for many hours. In addition, chemical releases could prevent the use of K-9 teams because of health risks to the dogs and their handlers.

Other detection technologies suggested by respondents include: walkthrough metal detectors (which are, however, limited for detecting explosive components); x-ray single and multigenerator detection algorithms; field screening tests; biometric technology (fingerprints and facial recognition technology); and even a national identification card. For any piece of such equipment, it is not enough to just know how to use it, there also must be a full understanding of what the system can and cannot do as well as backup expertise when possible.

Many survey respondents shared a concern over border control, but had very different ideas on how to improve such security efforts – from enforcement of existing regulations and laws to locking land borders with solid walls (“like the Great Wall of China”). Regardless of the efforts to improve security at the borders, public-private collaboration is needed at all levels.

All countries, large and small, may be able to provide intelligence on and tactics for dealing with potential threats. Many other countries have been dealing with the threat of explosives for many years, some on a daily basis. Unfortunately, lessons learned overseas are not always transferring to domestic issues. One respondent to the survey warned that, “Our high opinion of ourselves invites attack.”

The consensus among respondents is that there is no single investment or strategy that would prevent future IED attacks. The necessary measures depend on the situation and must be flexible to address evolving threats, as well as to quickly fill gaps in capabilities. However, without consistent funding of these programs and strategies, agencies are restricted in their ability to detect, deter, and prevent. U.S. funding efforts in the past have been more reactionary than proactive. For example, the large influx of federal money that flowed into the homeland security sectors following 9/11 has all but disappeared. Although there is a tremendous amount of detection instrumentation and potential training sources available, such equipment often is expensive and, if not purchased for multiple purposes or users, may be seldom used.

Gaps Between Federal & Local Agencies

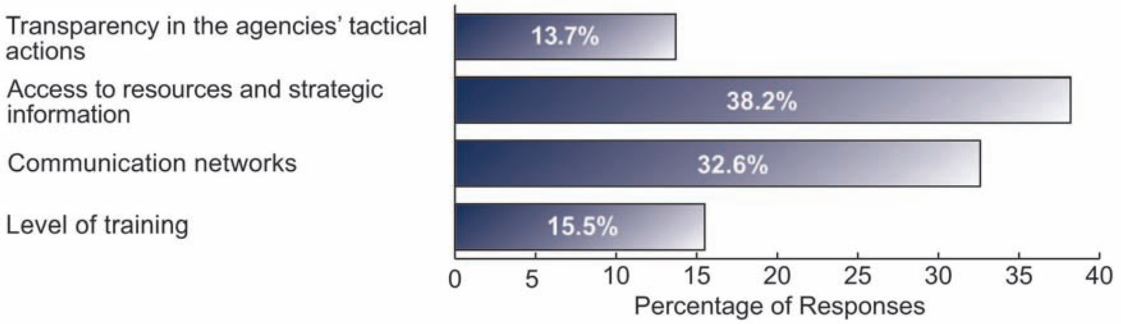
> *"There is some technology out there, but policy and [concepts of operation] need to be in play. Consumables and maintenance are a big factor, but the biggest reason they fail is the training. It is the human factors we need to continually look at and reevaluate."*
>
> *–Charles Guddemi, federal law enforcement officer*

DHS has divided the U.S. critical infrastructure sector into 16 different parts. As referenced earlier, open public access to facilities is an issue, but trusted relationships with the private sector have helped over the years. The federal government has shifted "from a need-to-know to a need-to-share culture" – providing more access to the private sector, which has knowledge of the application of security efforts. By discussing intelligence with the private sector, DHS can help the private sector partners better understand the process. Simple resources such as brief training videos can help build a culture of awareness from the hourly employee to the top security director. In the federal government, professionals must prepare for the possible, but the private sector often only has resources to plan for the probable.

Survey respondents reported that access to resources and strategic information (38.2 percent) and communication networks (32.6 percent) are the biggest gaps between federal and local agencies (Figure 4). Quick turnover rates of personnel in various agencies make it difficult to establish consistent contacts and build steady relationships. Also, the communication platforms that are used by federal and local agencies during incidents may vary, so interoperability and compatibility of methodologies, resources, and standard operating procedures are critical. One solution is combining resources into regional teams – for example, bomb squads – to ensure that resources are available and personnel are trained and able to respond when needed. Not working with partner organizations often results in wasted resources, duplication of efforts, animosity, and increased risks.

Figure 4

What do you see as the biggest gap between federal and local agencies?



Similarly, government-to-government communication on strategy and its enablers needs to be two-way. Some respondents stated that communication of needs from the local and state levels to DHS is nonexistent, whereas others stated that communication is lacking from the federal level to the local level. Joint programs and initiatives between the federal, state, and local agencies would lessen this gap and build knowledge and skills at all levels about developing threats that could affect any agency. In addition to building cohesion and trust, a consortium of fire, law enforcement, and explosive ordinance disposal personnel would ensure that overlap of resources is available in the event of an incident.

Transparency in the agencies' tactical action plans is another issue that resonates between survey respondents (13.7 percent). Every agency has the ability to bring something to the table to coordinate resources and work together for a common goal. "From the local level, it is not always clear what is expected of us and, conversely, we often do not know what to expect when we forward a notice to a higher level." Without such transparency, some agencies may "take on strategic challenges that are far above their capabilities and responsibilities." It is critical at all levels to understand and act upon how missions connect, overlap, and complement. Solutions exist, but some agencies do not want to acknowledge that other agencies may have a better solution.

Some respondents (15.5 percent) stated that the level of training should vary. "The problem with adding more training is that, if the local agencies don't normally have reason to act on specialized training, they will forget most of what they learned. If we can make a smoother connection between the local, state, and federal agencies, then local agencies who know the land and the federal specialists can get the job done much more smoothly."

III. CURRENT & FUTURE THREATS

The threat has shifted from Iraq and Afghanistan to other parts of the world. The Terrorist Explosive Device Analytical Center (TEDAC), which was established in 2003, is a joint explosives organization that includes: U.S. Department of Defense, U.S. Department of Justice, and international partners. TEDAC pre-deploys personnel to various parts of the world to gather information that could be used to thwart future attacks. As a result, two bomb-makers who moved to the United States have already been caught. The trend is that, although device design and delivery mechanism change, almost anyone can make and transport them. One noticeable shift in tactics is toward the use of nonmetal, nondetectable devices that can create a hyperbolic reaction, but cannot be identified by metal detectors.

Real & Perceived Threats

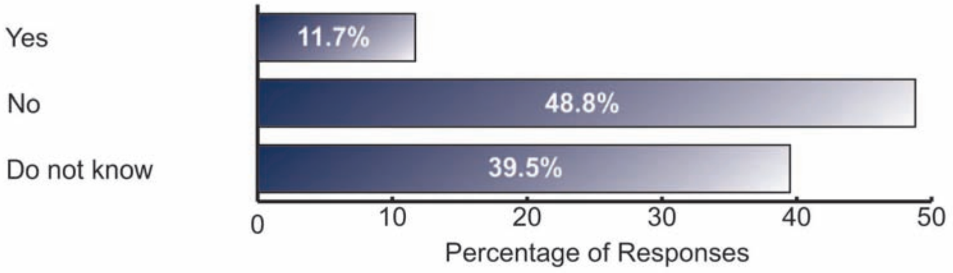
When Bruce Prunk, brigadier general and special assistant in the Air National Guard, was stationed in Iraq, nine of his Office of Special Investigations and security force defenders were killed and more than 100 wounded. His takeaway from that experience was that, "They will target us as responders, they will target us on the intel side, they will target us as the bomb technicians…. There are many lessons learned at the Department of Defense, and they are all learned the hard way." So the threats remain real even when an explosion does not occur.

DHS uses forward intelligence to determine whether what they see overseas – viable devices, ability to construct the devices domestically – could be a viable threat to the United States. According to two roundtable panelists, there is nothing in the operational environment in the United States to stop someone from starting a domestic bombing campaign, given the right motivation and determination. Customs officers have been successful in keeping people out who pose a threat, but tactics running the gamut from high-tech to low-tech are something they must adjust to on a daily basis. It is rare, though, that they see anything that is completely new.

Although New York City and Washington, D.C., are prime terrorist targets, the more difficult it is to attack these two cities, the more likely it is that terrorists will target other, more vulnerable cities. In this circumstance, basic crime prevention can still be effective for IEDs. The real threat is the people behind the weapons, so it is critical to never underestimate the adversary. The U.S. Constitution limits many protective measures that are being used overseas. Domestic law enforcement agencies also are

Figure 5

Do you believe the current federal policy is effective in addressing a terrorist threat involving improvised explosive devices?



limited by citizens' perceptions – some think that more should be done, while others think that less should be done. Each time an incident occurs, open-source (or leaked) information about the detection method, radicalization, and device construction ensure that adversaries will change their tactics for future attacks.

Kevin Hay, chief of police for George Washington University Police Department and member of the International Association of Chiefs of Police (IACP) college and university section, explained that, in 2012, colleges were clearing entire campuses because of nonspecific bomb threats that were placed to cancel commencement, to avoid finals, or for other reasons that ultimately did not involve an explosive device. Of the hundreds of cases of telephoned, emailed, or mailed bomb threats, there was almost no correlation to a device. Between 2007 and 2011, 82 incidents involved a device, of which 20 were actual bombs, 28 were hoax devices, and 34 were recoveries of devices like pipe bombs. Only three of those cases involved advance notice, and they were all linked to the hoax devices. The lessons learned were that: (a) real threats often do not include advance warning; and (b) false alarms still have the ability to drain on resources.

Few respondents (11.7 percent) believe that the current federal policy is effective in addressing a terrorist threat involving IEDs, and even fewer stated that they are as effective as they should be (Figure 5). Of course, some people think it "can't be too bad since I haven't heard about very many successful IED detonations," but others understand the need to keep improving methods as well as to eliminate the possible stumbling blocks in carrying out the policies.

Among those who do not believe the current policy is effective (48.8 percent), the reasons varied greatly:

- Policy cannot stop someone who is determined to cause harm.
- Certain cities have been hardened, but at the cost of leaving other areas more vulnerable.
- The cost to businesses needs to be considered.
- The IED threat is too broad and open ended.
- Policies exist, but lack oversight and are not effectively engaged and enacted.
- Policies are reactive rather than proactive.
- New technologies require excessive testing and regulation, while obsolete technologies remain with increasingly stringent expectations.
- Policy does not have a firm and clear commitment and mission.

More than one-third of respondents still are unsure (39.5 percent) if current policy is effective: “The fact that an IED has not exploded is not proof to me.” Many respondents reported that the nation has just been “lucky” that there has not been another attack like the one on 9/11. Border security, accountability of bomb-making materials, and accessible information were some of the reasons provided: “It is a game of statistics. Sooner or later one of the threats will penetrate.”

Greatest Risks & Threats to the Nation

As the nation develops new methodologies to identify suspicious behaviors, the adversaries sometimes compensate by “descending the technology ladder” to get past advanced threat-detection technology. The nation’s open media and open access create vulnerabilities, so security plans sometimes must change to make them less predictable. When tactical information cannot be protected and law enforcement is under scrutiny, it is even more difficult to provide adequate protection.

IEDs can range from basic devices such as pipe bombs and pressure cooker bombs to commercial airplanes. David Cohen, former deputy chief of intelligence for the City of New York Police Department (NYPD), stated that, “The greatest threat we face in many respects is complacency.” According to Cohen, the primary domestic targets in the global war on terror are still New York City and Washington, D.C. Between 9/11 and June 2014, there were 16 plots targeting New York City, five plots alone in the 18 months prior to June 2014, so the threat has not diminished. The terrorists on

9/11 used very simple instruments – box cutters – and there were no more than 500 al-Qaida operatives around the world. Today, there are more than 12,000 al-Qaida operatives in Syria alone. In addition, today's terrorist organizations are different than before 9/11 for three main reasons: complex communication networks, effective command and control, and a central body.

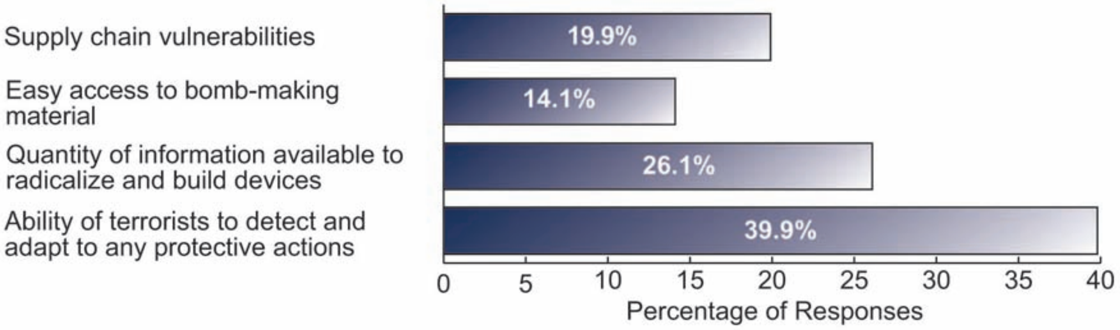
Although most people were not aware of al-Qaida affiliates before 9/11, there are now at least 18 – including al-Qaida in the Islamic Maghreb (AQIM), al-Qaida in the Arabian Peninsula (AQAP), al-Shabaab, Boko Haram, al-Nusra Front, and Islamic State of Iraq and the Levant (ISIL) – and that number continues to rapidly grow. These al-Qaida affiliates, their associated franchises, and the aligned homegrown terrorists all pose a great threat to the United States. Under normal circumstances, such terrorist organizations would disappear but, instead, they are increasing in support. In particular, the al-Qaida-inspired homegrown threat has increased since 2005, enabled by Internet propaganda that is able to recruit from abroad. The current threat likely will exist into the next generation, with native-born and immigrant citizens being radicalized, then returning to their home countries. This so-called "Syrian effect" has been seen in the United Kingdom and other parts of the world.

Risk assessments should include: understanding the environment, acknowledging what is important, knowing about the threat actors, and determining what is vulnerable. Kevin Hodges, vice president of security solutions for Watermark Risk Management International and former chief master sergeant in the U.S. Air Force, stated, "One of the biggest issues that we see is that often the people who are tasked with the missions – the charters of protection of people and things – is that they do not understand their environment." To keep the issue of IEDs on the left of boom, knowing the adversaries also is critical. For example, some terrorist tactics are moving toward smaller scale, lone-wolf attacks that are more difficult to detect in advance.

Defining risk includes defining and quantifying successes and failures. After an incident, agencies tend to purchase many gadgets that sit in warehouses without the funding and personnel to sustain the technology. Those who are successful in the "left-of-boom" arena have a strong on-foot force that can spot abnormal activities. People in that force, who know what "normal" looks like, are vital for determining if something or someone might be a threat.

Figure 6

In your opinion, which of the following poses the greatest risk to the nation for possible attack?



Many factors pose a threat to domestic security capabilities and must be considered, including but not limited to: supply chain vulnerabilities (19.9 percent), access to bomb-making material (14.1 percent), information available to radicalize and build devices (26.1 percent), and the ability of terrorists to detect and adapt to measures directed against them (39.9 percent) (Figure 6). Supply chain vulnerabilities include critical infrastructure – soft targets such as electrical grids, ports and borders, fuel storage depots, mass transit systems, medical systems and facilities, communications networks, schools, and public venues. In an open society with many stakeholders, protecting all possible targets is very difficult, “Vulnerability is generally recognized by those who will take both positive and negative action. Unfortunately, updating the response with proper equipment, training, and staffing may not be recognized until after an event.”

Once terrorists know the U.S. plans, they change their tactics to create the largest impact. Anyone with motive, means, and opportunity to kill, coupled with a willingness to die, make threats more difficult to prevent, detect, and deter – especially when they use their ability to hide, practice, and train among a resident target population until activated. As stated in the motto from Naval School, Explosive Ordnance Disposal, IED division, “The complexity of the device is limited only to the ingenuity or incompetence of the bomber.” The wealth of information available on the Internet makes it extremely difficult, if not impossible, to thoroughly monitor every site that contains a bomb recipe. Furthermore, humans are highly adaptable, so it is important to address the conditions that lead to radicalization, and thereby reduce the potential pool of actors.

Explosives Roundtable Discussion, U.S. Park Police Anacostia Operations Facility

Although helpful for disseminating valuable information, media outlets also pose a risk to the nation's security. Either deliberately or inadvertently, traditional and social media outlets broadcast protection methods, capabilities, potential targets, vulnerabilities, incident details, and specific locations that include satellite images from different angles. Even law enforcement and other planning and response agencies share the types of detection tools they are using and how they work. According to Guddemi, "We are our own worst enemy when it comes to operational security. We have too many people who are too quick to get in front of a camera." Of course, the public has a right to know some information, but not details that will compromise life and safety.

IV. PROTECTION VS. PRIVACY

From an intelligence perspective, the United States Park Police had to protect approximately 14,000 events in 2013 that were accompanied by protests and/or potential threats – the latter originating both domestically and abroad. The Park Police regularly collaborate with intelligence fusion centers to determine what threats may present themselves, based on various actions. That information then must be provided to operational levels in order to know how many personnel are needed, when protection is warranted, and where security must be increased. Although citizens may consider some preventive measures as overreacting, such measures do in fact help prevent and deter attack.

Vulnerabilities & Detection Technology

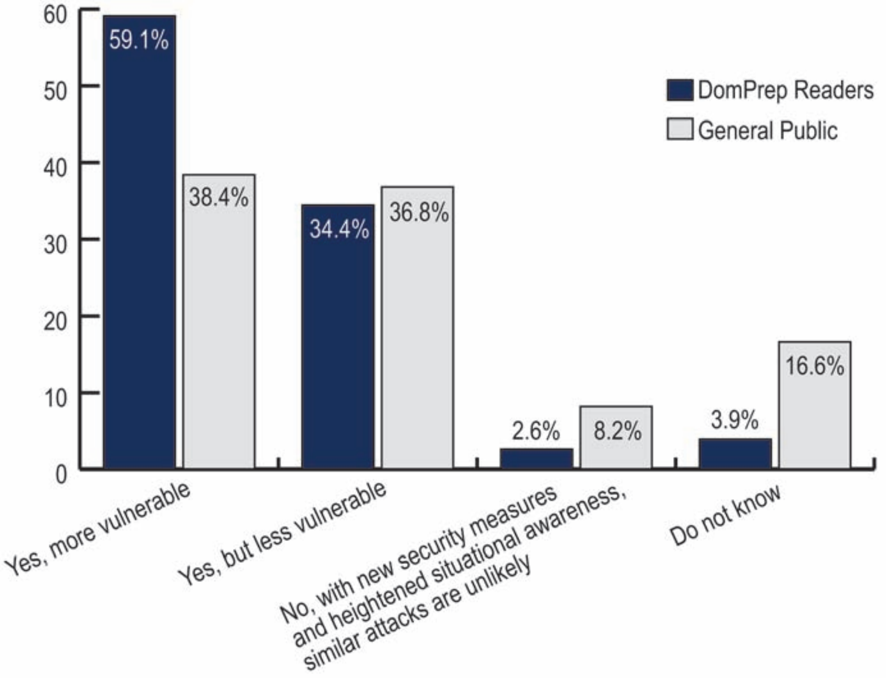
In light of the Boston Marathon attack, an overwhelming majority of respondents (DomPrep: 93.5 percent; Public: 75.2 percent) believe that other U.S. special events and high-profile facilities are vulnerable to attack by adversaries using IEDs (Figure 7). Interestingly, about 20 percent more DomPrep readers (who are all involved in emergency preparedness and response fields) than public respondents stated that the nation is actually more vulnerable than before the Boston attack.

Since 9/11, many budgets and grants were allocated to science and technology but, according to Richard Lareau, chief scientist for at the DHS/S&T Transportation Security Lab, there is still no “silver bullet.” Next generation detection technology is being developed and current systems are being updated but, for now, all current capabilities need to be part of the toolbox. First responders must be equipped quickly, but the equipment needs to be developed properly, with an understanding of existing strengths and weaknesses.

Stephen Surko, a program manager of DHS’s Science and Technology Directorate Explosives Division stated, “My biggest challenge in the Explosives Division is developing and transitioning technology advances that deliver capabilities not required by current [concepts of operation].” In effect, the Explosives Division, which is primarily focused on detection, helps bridge the gaps between technology capabilities and the customers. For standoff detection, there are new technologies for detecting both trace (smaller than the size of a fingerprint) and bulk (one pound or more) quantities of explosives: Laser Induced Acoustics (LIA) demonstrates how explosive molecules have a unique acoustic signature; laser techniques for detecting explosives

Figure 7

In light of the Boston Marathon attack, do you think other U.S. special events and high-profile facilities are vulnerable to attack by adversaries using improvised explosive devices?



under clothing; multiple standoff trace detection methods; Vehicle Eye Safe Trace (VEST) to offer protection at Level 4 facilities; short-range laser detection of trace explosives; and portable pup tents that can be placed over suspicious items and offer limited ballistic material protection.

When detection tests result in false positives, the users may not know what to do if the material cannot be found in the library. This along with other stress factors leads to a significant concern about the resilience of law enforcement and other emergency personnel: (a) these personnel have many things to look for; (b) they need the right tools and abilities; and (c) sometimes the expectations of them are set too high.

In the United States, there is an abundance of information about the modeling and implementation of homemade explosives and, compared to some countries, the materials are relatively easy to access. As William Qualls of the Massachusetts State Police explained, "Probably every week, if not every day, there's a homemade explosives synthesis going on within the United States, but it's more for curiosity by individuals who have too much time on their hands."

In the NYPD, officials established "Operation Nexis," which examined incidents that occur overseas to see what "ingredients" were used in the attack. Then a specialized unit would identify any company or local store owner that sold, produced, or moved that particular material. After identifying the possible sources, a team of detectives would visit those companies and stores to advise the owners how their products were being used in terrorist incidents abroad. "There is no substitute for gumshoe work," said Cohen. In New York and other cities around the country, the human element is critical – intelligence gathered by people who blend in with the population and provide daily reports on who is watching a facility and what they are saying.

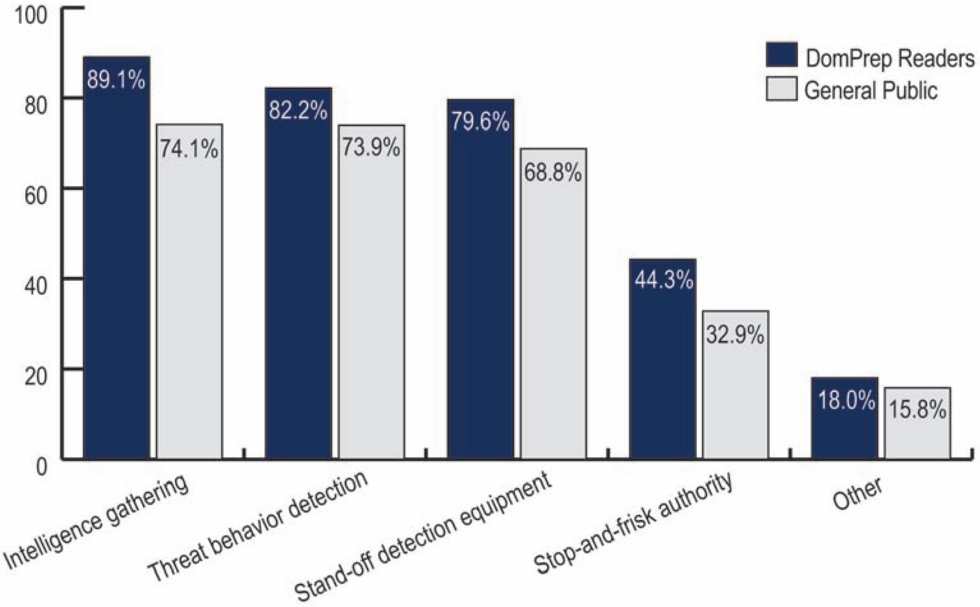
In addition to technology and materials, analytics are critical for preventing an attack, but are often lacking. Jordan Heilweil, president of Total Recall Corporation, explained, "Analytics are probably the most overpromised and underdelivered portion of the CCTV solution." Although many analytics may work in a laboratory setting, there are limitations and various things to consider, including: whether the analytics will be used live or forensically; a portal to monitor direction of travel; basic motion detection when there is no reason for motion; and thermal cameras for waterside use. Face recognition advancements and other sophisticated devices also can be powerful if the proper portals are established.

Rodney Hudson, president of QuickSilver Analytics Inc., agreed and added that accurate analytics requires accurate sampling. Many errors occur in the sampling process, so it is imperative to retrieve the best possible sample and not waste valuable resources on unnecessary or invalid testing.

Some technology bridges the gap between response personnel and the public/private sectors to improve the decision-making process. Justin Kelley, managing director for MSA Security, described one prevention method as an X-ray screening system that transmits an image in real time to a remote operation center's hazmat and bomb technicians. The technician then determines whether the machine detected a threat. In doing so, the responsibility passes from the operator to the expert, while still enabling two-way communications.

Figure 8

Which of the following "tools" should law enforcement have access to in order to prevent low-frequency, high-consequence incidents, including the detonation of explosive devices? (Check all that apply)



Acceptable & Unacceptable Tools

For preventing low-frequency, high-consequence incidents, law enforcement officers having certain "tools" – intelligence gathering (DomPrep: 89.1 percent; Public: 74.1 percent), threat behavior detection (DomPrep: 82.2 percent; Public: 73.9 percent), and stand-off detection (DomPrep: 79.6 percent; Public: 68.8 percent) – is generally acceptable to both DomPrep readers and the public, with DomPrep readers having a slightly higher acceptance rate (Figure 8). One tool that causes more hesitation on both sides is police officers having stop-and-frisk authority (DomPrep: 44.3 percent; Public: 32.9 percent).

Information leaks need more transition, explanation, and expansion at the National Security Agency do not seem to have a large impact on whether people in the United States support intelligence-gathering practices. Although there is acknowledgment that gathering intelligence is beneficial, some respondents have concerns about how this information is being analyzed and processed into actionable intelligence. Another concern is that capabilities, resources, and legal authorities tend to trend up or down depending on the level of perceived threat, "It seems that, because of this, we are always behind on delivery of a consistent and effective set of mechanisms to intervene early enough in the threat development process to deter attacks," commented one survey respondent.

Many survey respondents are in favor of threat behavior detection programs that look for patterns and identify specific suspicious behaviors. Asserted by one respondent, "We need to stop random searches and profile as the Israelis do. Their security works much better than ours and certainly is more tested." A variety of stand-off detection equipment can be integrated into detection programs, including: closed-circuit television, cameras with biometric capabilities; radiation detectors; nitrogen sniffers; thermal imaging; drones; facial recognition; explosive trace detection; human portals (similar to airport walk-through scanners); and sensors that can detect explosives remotely.

Respondents seem to have more resistance to stop-and-frisk authority than to the other tools listed, "Low frequency events should not become no-personal-rights events." One reason provided is that, "Stop and frisk authority is easily abused and should only be accomplished under strict conditions and only to the level deemed necessary based on sound intelligence or confirmed information." Another respondent pointed out that, "We already have stop and frisk (Terry v. Ohio 392 U.S. 1, 88 S.Ct. 1968) upheld by the U.S. Supreme Court. Any broader law would be redundant and serve to trample on the Constitution (which is already seriously wounded)."

Although a few respondents stated that none of the tools listed in Figure 8 should be used, others suggested "all of the above." Another tool added to the list is adequate training on various topics including: "what-if" scenarios, soft-target awareness, surveillance, countersurveillance, buffer-zone protection, crowd control, interoperable agency command and control, communications, and mission-specific training. High-volume events, including the use citizen volunteers, can be used as training events; because citizens can be "part of the solution and part of the problem," they should be included in planning efforts.

Other tools that respondents consider to be acceptable include: photo identification checks of everyone attending an event; countersurveillance; behavioral rules such as no backpacks and removal of jackets plus screening at the point of entry as necessary (such as at airports); pre-issued special passes with coding; authorization to block all cellphone calls in a vulnerable area to prevent remote-triggering of explosives; Joint Hazard Assessment Teams (JHAT), which are multidisciplined teams of first responders (law, fire/EMS, health department, and EOD), each with a particular expertise; mobile detection devices; body cameras on law enforcement officers; detectors or K-9 dogs placed at entrances to check for explosives; patrol by plainclothes officers at the event to check for suspicious activity; increased police presence; enhanced interrogation; extensive evaluation of the facility or area being used; wire taps; fingerprinting of anyone caught for a minor offense; and rigorous pre-event checks.

Right to Privacy vs. Right to Not Be Blown Up

In theory, anything can be detected and identified but, in reality, that is not necessarily the case. Time is constantly working against the technology development process because there needs to be sufficient time to create standards, advertise, compete, and test the products. Terrorists, on the other hand, have the ability to change their tactics almost immediately. Because the United States is not under attack every day, many U.S. citizens want to maintain privacy and convenience, more so than in places like Iraq, where attacks occur every day.

Consultations are needed with partners, subject matter experts, and agency attorneys to discuss the threat and determine if actions are within the laws outlined in the Fourth Amendment of the U.S. Constitution:

> "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

"Did our founding fathers foresee or anticipate the types of threats that you all deal with now? Did they envision the technology that you have been able to bring to bear on trying to diffuse, detect, and prevent this type of attacks? The answer is, 'No'," said Randolph Myers, a senior attorney for the Office of the Solicitor, U.S. Department of Interior, who has assisted the United States Park Police in First Amendment activity litigation. Judges and policymakers may not be familiar with the technologies and threats, so they must be educated on these threats, solutions, and reasons.

There are procedures for what can and cannot be submitted in court so, before taking law enforcement action, agency leaders should seek counsel – for example, legal counsel reviewed United States Park Police CCTV activation policy and, because other agencies had no similar policy, it was adopted by multiple agencies in the D.C. area. Robert MacLean of the United States Park Police stated, "We are persistent and undeterred in what we truly believe is our mission down to our core values: Protecting the visitor and protecting the resource, which for us are symbols of democracy."

Glenn Gerstell, partner at Milbank, Tweed, Hadley & McCloy, is a lawyer in the private sector with experience as a member on the National Infrastructure Advisory Council. Gerstell said there is a duality between the public wanting to feel safe yet them not wanting the security mechanisms to be too intrusive. He shared three observations:

- There is a tremendous amount of knowledge and expertise among security professionals, who do a good job of securing events and coordinating with private sector partners, although not all personnel within the private sector.
- The public does not truly understand and appreciate what security professionals do behind the scenes, which leads to tensions related to the First and Fourth Amendments – an "us-versus-them mentality."
- The private sector would like to see a constant focus on engaging the public at all levels, sharing knowledge, and bridging cultural barriers but, without senior private sector buy-in, it is difficult to succeed.

Sir Ken Knight replied to this discussion by stating, "I sense that there is not quite the same mistrust of the civil liberties issue about CCTV in England than there might be in some places in the United States. People [in England] are pretty comfortable that it's adding, not detracting, from their safety. The civil liberties balance for most of the people I talk to is the civil liberty about not being blown up."

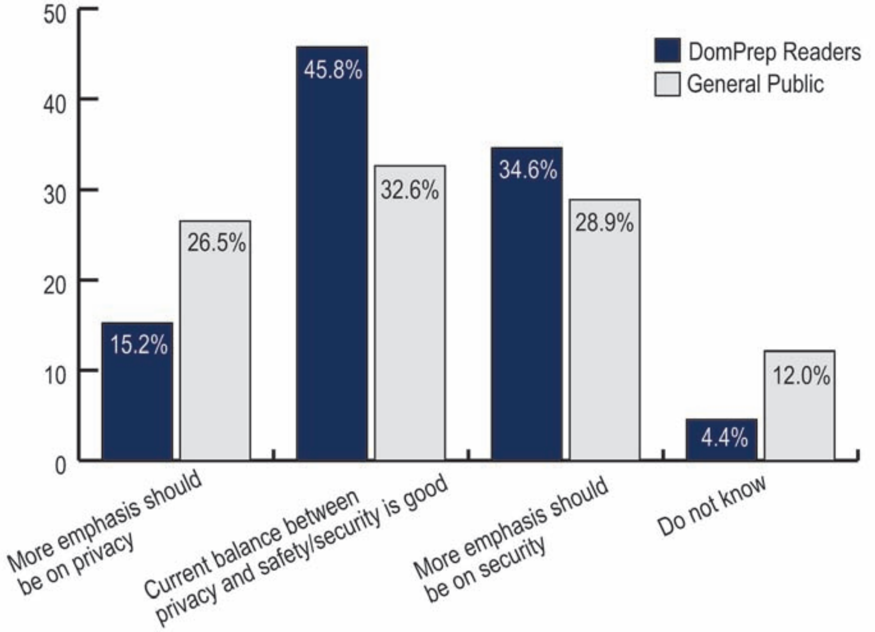
This leads to the tough question, "Should government authorities place greater importance on individual privacy or community safety/security when formulating prevention strategies?" The results were in favor of the current balance, or more security than privacy (Figure 9).

Those arguing for more emphasis on privacy (DomPrep: 15.2 percent; Public: 26.5 percent) primarily expressed concerns about constitutional rights:

- "Nothing will help that wouldn't result in a reduction of our First and Fourth Amendment protections. A dedicated terrorist with enough ingenuity would find a way to circumvent most police precautions."
- "They who can give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety." (Benjamin Franklin, 17 February 1775)

Figure 9

In your opinion, should government authorities place greater importance on individual privacy or community safety/security when formulating prevention strategies?



- "A 100% safe environment is a 0% free environment."
- "Anytime we give up a freedom for enhanced security, what was relinquished will seldom be recovered."
- "Yes, there are serious threats, but our freedom must come first."
- "I believe our privacy is under attack, and is being ignored in far too many cases. There must be a balance, but I think we have given up far too much in the wake of 9-11, and it's time for the pendulum to swing back toward an appreciation of privacy."

Some do not believe the threat is significant enough to warrant loss of privacy:

- "Privacy should be maintained until the threat exceeds eminent expectation of potential."
- "There will always be risk. It's not worth losing our freedoms over... Not yet anyway. The threat simply isn't even close to where it would need to be."

And others stated that reducing privacy would not increase security:

- "The right to privacy must be observed. Proper processes are in place to obtain further information upon just cause, but many times expediency is used as the excuse to avoid using the systems in place."
- "No matter how much money and effort goes into an event, smart people who are fully dedicated to their cause can and will figure a way around the security."
- "Reducing privacy does not increase safety. For every element that law enforcement takes away, an equal number of new and harder to police mechanisms will be developed. Following this 'chase the rabbit' approach will only balloon costs and ultimately end in failure. Safety/security comes with the implementation of community empowerment. With a vigilant community comes change."

The arguments for more emphasis on safety/security (DomPrep: 34.6 percent; Public: 28.9 percent) primarily reflected concerns about the level of threat against the United States:

- "Freedom isn't free and, unfortunately, we will probably be giving up a lot of privacy in the future when terrorism hits our homeland like it has in other parts of the world."
- "In our present world with all the electronic information, we need to be concerned about our safety more than privacy at this point in time. We are now a global community and isolationism is a thing of the past."
- "We need to be ready for anything coming from anywhere, even home-grown threats. Anyone worried about privacy should start by staying off Facebook."
- "Terrorists are always coming up with new ways to harm us – so 'oversecurity' is better than 'undersecurity.' However, it is a mighty fine line between securing and stepping on individual rights."
- "At large gatherings, where terrorist attacks are more likely, the public safety community should have broader powers to protect crowds. For the public who are attending these large events, they have to be educated that they will have to sacrifice some level of privacy to enhance their security. We can't have it both ways. Too much is at stake!"

- “I hate to jump on the band-wagon, but the recognition of the Islamic State of Iraq and Syria (ISIS) and the threat it brings is a game changer for our society. Our American culture and society can’t [comprehend] a group so bent on the destruction of our lifestyle that they would willingly die for it.… As we begin to more fully ‘appreciate’ the threat these groups will go to in order to wreak havoc, then we will more likely tolerate the additional ‘invasion’ of privacy required to more carefully monitor these groups.”

- “I find it fairly ironic that people are so quick to demand transparency for law enforcement actions yet in the same breath demand privacy for any actions that involve ‘their’ person or equipment (cell phones, computer, etc.). We are increasingly faced with this ‘me’ culture in which people demand what *they* want or what benefits *them*, yet somehow law enforcement and other public officials are supposed to keep them safe without any participation on their part. We’re at the point of having terrorist organizations (ISIS) interacting with the U.S. public on social media, such as the #napaquake exchanges on 8/24/14. It’s incredibly unfortunate that it will take a major crisis on U.S. soil involving a very open, public venue before attitudes will change enough to enable adequate security.”

Other reasons provided for choosing safety/security over privacy included:

- “I have nothing to hide. Do whatever you need to keep the bad guy away.”

- “A little more privacy would be great, however, if we are to achieve the amount of safety/security for our country, then we should expect to give a little for that goal.”

- “Current emphasis on privacy provides increased opportunity for attacks.”

The argument for keeping the current balance between privacy and safety/security (DomPrep: 45.8 percent; Public: 32.6 percent) primarily expressed a need for careful oversight:

- “While the protection of the many trumps the privacy of a few as a rule, there needs to be strict oversight in the techniques used.”

- “The nature of the event and threat should determine (case-by-case) how far it goes.”

- “As a 30-year former federal law enforcement officer, I witnessed first-hand, government efforts to maintain the balance between enhanced national security and intrusion on privacy and civil liberties. In my experience, the government invariably acted in good faith, but sometimes fell short of its statutory and policy obligations because of unprecedented world/national events. This is not an excuse for government agents who occasionally have willfully or deliberately circumvented the rules. I do not condone any subscription to an ‘eye for an eye’ philosophy, and there is no room for that under our legal system. Achieving the proper balance is not simple but, in an era of asymmetric threats, especially from terrorists determined to disrupt the ‘American way of life,’ the public must be willing to trust that homeland security/public safety agencies are conducting themselves in accordance with the law and are executing their responsibilities in good faith. Americans surrender significant aspects of their personal privacy daily while conducting financial transactions; this information is sold and re-sold to other financial organizations and marketing entities virtually without limits. It seems to me that, if we are willing to compromise our privacy expectations to ‘get a good deal,’ we should be willing to make the same compromise if it might detect and lead to the disruption of an act to harm unsuspecting and innocent citizens.”

According to another comment, “The privacy should only be overruled if the safety and security of the community are at risk,” but who determines whether the community is at risk and at what level does it warrant this action? One respondent recommended having expert risk-assessment professionals who can identify nuances and subtleties by conducting security vulnerability assessments and threat risk assessments. However, that raises the recurring conundrum: There will always be some people saying that not enough was done and others saying that too much was done.

With 12.0 percent of the public stating that they do not know whether individual privacy or community safety/security should have greater importance, there is a great opportunity for raising awareness on this topic and opening the dialogue with public outreach efforts. “I think the public needs a great deal of education in not only what [law enforcement] will be doing, but why and how it benefits them to go along with what [law enforcement] needs. Transparency goes a long way in getting people to buy into what needs to be done.”

KEY FINDINGS & ACTION PLAN

A vehicle laden with explosives detonated in front of the Alfred P. Murrah Federal Building in Oklahoma. Planes full of jet fuel crashed into the Twin Towers in New York, the Pentagon in Washington, D.C., and a field in Pennsylvania. Backpacks with pressure cooker bombs exploded near the finish line of the Boston Marathon in Massachusetts. The delivery mechanisms may change, but the threat of attack using explosive devices only grows, as terrorist cells attempt to recruit more support from within the United States and abroad.

In order to stay "left of boom," there must be support for and the means to prevent, detect, and deter potential threats. The nation and its leaders must:

- Define success as it relates to improvised explosive devices (IEDs);
- Determine what level of risk is acceptable;
- Identify and apply lessons from past incidents;
- Invest in and adequately train personnel;
- Implement effective techniques from other countries;
- Close gaps between federal and local agencies;
- Facilitate two-way communication of critical information;
- Evaluate and integrate effective technologies;
- Review, improve, and oversee federal policies;
- Equip law enforcement officers with the right tools; and
- Recognize citizens' right to privacy *and* right to not be blown up.

The topic of IEDs raises much debate for and against specific preventative measures, collection and/or analysis of certain information, and the protection of privacy. The missing piece is top-down as well as bottom-up education, which begins with opening lines of communication.

APPENDIX A
Explosives Roundtable Participants

Chris Cikanovich	President	CEI Consulting Services
David Cohen	Former Deputy Commissioner	New York Police Department Intelligence Division
Ken Comer	Former Deputy Director, Intelligence & Analysis	Joint IED Defeat Organization
David W. Cullin	PH.D., Vice President Research, Development & Programs	FLIR Systems Inc.
Joe Donovan	Senior Vice President	Beacon Capital Partners
Kevin Finnerty	Special Agent	The Federal Bureau of Investigation (FBI)
Glenn Gerstell	Partner	Milbank, Tweed, Hadley & McCloy
Charles Guddemi	Federal Law Enforcement Officer	
Kevin Hay	Chief of Police	George Washington University Police Department
Jordan Heilweil	President	Total Recall Corporation
Kevin Hodges	Vice President, Security Solutions	Watermark Risk Management International
Rodney Hudson	President	QuickSilver Analytics
Justin Kelley	Managing Director	MSA Security
Sir Ken Knight	Chief Fire & Rescue Advisor	London, England
Cathy Lanier	Chief of Police	Metropolitan Police Department
Richard Lareau	Chief Scientist	DHS/S&T Transportation Security Lab
Robert MacLean	Acting Chief of Police	United States Park Police
Robert Messier	Senior Account Manager	Thermo Scientific
Randolph Myers	Senior Attorney	Office of the Solicitor, U.S. Department of the Interior
Lawrence O'Connell	Executive Vice President	International Maritime Security Corporation
Chris Paschel	Branch Director, Intelligence & Counterterrorism	United States Park Police
Bruce Prunk	Brigadier General, Special Assistant	Air National Guard
William Qualls	Sergeant	Massachusetts State Police EOD
Colin Roberts	Engineer	NSWC IHEODTD
Andrea Schultz	Section Chief	Commercial & Government Facilities DHS/NPPD/IP
Glenn Smith	Assistant Director - Security	U.S. Department of the Interior
Tim Stephans	CEO	MESH Coalition
Darius Sultan	Area Commander	DHS/Federal Protective Service
Stephen Surko	P.E., Program Manager	Explosives Division, DHS/S&T Division
Jack Suwanlert	Director of Global Safety & Security	Marriott International Inc.

APPENDIX B
Contributors

Dexter Accardo, Director of Homeland Security and Emergency Preparedness

Timothy Adamczak

Amy L. Altman, Ph.D. Vice President Biodefense, Luminex

Tracy Anderson, Emergency Management Student, American Military University

Erik Angle, RN, MICN, Sutter Roseville Office of Emergency Management

Alan Antenucci

Sachin Bagade

Victor Bai, CEM, President of IAEM Asia Council

Marc Barbiere, Emergency Management Coordinator, Fairfax County Health Department

Brandi Baros, Regional Coordinator, Environmental Health & Safety, Penn State University

Ted Bauer

Abboud Bedro, Threat Assessment and Protective Intelligence at Aegis Group

Lee Bennett

Charles Bishop

Albert Black

Robert Bovey, Adjunct Research Staff, Institute for Defense Analyses

Samuel Boyle, Senior Emergency Management Coordinator, Chicago Department of Public Health, Bureau of Preparedness and Emergency Response

Michael Brandon, Lieutenant, Kernersville Police Department

David Breeding, Col., Director, Claiborne County Office of Emergency Management Homeland Security

Paul Brenner, Senior Vice President, ICF International

Zuzzette Bricker, MS-AJS, BS-HA, Emergency Services Coordinator, Riverside County Fire Department Office of Emergency Services

John Broderick

Tom Bucek

Jim Burdick, Vice President/General Manager, FLIR Systems

Ronald Campbell

Timothy Carroll, Lieutenant, Field Intelligence Liaison Officer, FDNY

Stephen Carter

Frank Caruso

Manuel Ceja, MD, Medical Director, JFK Advanced Medical, JFK International Airport

Carmine Centrella, Program Director, Capitol Region Metropolitan Medical Response System, Hartford, Connecticut Region

Jason C. Chenault, PhD, CEM, CMCO, FaCEM, Senior Director of Emergency Services, University of Pittsburgh Medical Center

Brent L. Christopherson, Assistant Fire Chief, Missoula Rural Fire District

Terrence Cloonan, TKC

David Coatney, Fire Chief

John Contestabile, Assistant Program Manager, Johns Hopkins University/Applied Physics Laboratory

Christina Conti, Public Health Emergency Response Coordinator, Washoe County Health District

John Converse

Lynn Corliss, PHN, Emergency Preparedness Coordinator, Siskiyou County Public Health, Yreka, California

Edward Costello, Lieutenant, Texas A&M University Police Department

Thomas Cotter, Sgt., 25th District, Chicago Police Department

Michael E. Cox, Fire Chief, Anne Arundel County Fire Department

Patrick Cusick, RS, MSPH, Deputy Commissioner, Cleveland Department of Public Health, Division of Environment

Ralph D'Aries

Craig DeAtley, Director, Institute for Public Health Emergency Readiness, MedStar Washington Hospital Center

David DeCapria, Assistant Chief, Penn State University Hazmat Response

Arthur B. Ditzel, Jr., NREMT-P, Supervisor, Emergency Management and EMS Special Operations, New York-Presbyterian Hospital Emergency Medical Service

Shay L. Drummond, RN BSN, Director of Clinical and Environmental Services, Adams County Health Department, Quincy, Illinois

Stephen M. Durbin, Capt., EMS Operations Manager, Municipal EMS

Alex Elie

Dave Ellis

Michael Farash

Joseph E. Farley, RN, CCHP, JPS Health Network

James Flanders

Kristina Freas

Ronald E. Freeman, Training Specialist, Center for Domestic Preparedness, FEMA

Jennifer Frenette

Ioannis Galatas, BrigGen (retired), MD, MA, MC, CBRNE Planner and Instructor, Senior Asymmetric Threats Analyst, Editor-in-Chief at CBRNE-Terrorism Newsletter, Athens, Greece

Thomas Gallagher

Paul Garten, Adjunct Instructor, American Public University System and State University of New York at Canton

Petya Georgieva, Head of English Language Testing Section, Bulgarian Ministry of Defence

Jeff Gerald, SME, LSU

David Gerstner, MMRS Program Manager, Dayton Fire Department, Ohio

Thomas Gilligan, Lieutenant, Loudoun County Sheriff's Office, Virginia

Kay Goss, CEO, GC Barnes Group

Peg Graham

Michael Grasso

Dan Grimes

Wayne Hanes, EMS Outreach Representative, Columbia Southern University

Ross Harper, Product Manager, FLIR Systems

Robert Harter

William Haskell, Project Manager, NIOSH/NPPTL

Gordon Haynes, Lieutenant Lubbock Fire Rescue, Hazmat Team, Technician

Richard Hildreth, Vice President, IAEM Student Chapter, American Military University

Angela Hodge

Eric Holdeman, Director, Center for Regional Disaster Resilience (CRDR), Pacific Northwest Economic Region (PNWER)

Samuel Hood

Russell Hopkins

Scott Howe, RN, Public Health Response Coordinator, Converse/Niobrara County Public Health Departments, Douglas, Wyoming

John Howell, Director of Explosive Technology, DSA Detection, Master EOD Technician

Patrick Hoy

Thomas Hughes, Director of Product Management, SmartShield Technology, Passport Systems, Inc.

Gordon S. Hunter, Major, COANG, Deputy Commander 8th Civil Support Team (WMD)

Curtis Jack

Chris Johnson, Emergency Management Program Manager, Virginia Mason Healthcare

Mark Johnson

Scott Johnson, Deputy Chief, Canton Fire Department/ Massachusetts State HazMat Team

Pete Judiscak, Principal Consultant/Owner, Safety Pete Consulting LLC

Hassan M. Kagoni, CPT, CM US ARMY

Shawn S. Kelley, Director of Strategic Services, International Association of Fire Chiefs (IAFC)

Mac Kemp, Deputy Chief, Leon County EMS

Douglas Kinney, Senior Manager, Continuity and Resilience Practice, BDA Global

Leonard Kotkiewicz, Vice President, AECOM

Damir Kulisic, MSc in Chemical Engineering, Senior Lecturer, Police College, Zagreb, Republic of Croatia George, Lane, Chemical Security Analyst, New Orleans Fire Department

Marlene Lane

Dean Larson

Ray Leblanc, CHEP, Emergency Preparedness Coordinator, Exeter Hospital

Clark Lee

Arthur Levy, Owner, Apogee Communications Group

Leonard A. Levy, Associate Dean for Education, Planning and Research, Director, Institute for Disaster and Emergency, Preparedness, Professor of Family Medicine/Public Health/Biomedical Informatics, Nova Southeastern University College of Osteopathic Medicine, Fort Lauderdale, Florida

Richard Losurdo

Sean Madison

Rolf Madole

Jason Mahoney, Emergency Preparedness Coordinator, St. Vincent Healthcare, Billings, Montana

Paulo Malizia, Colonel, Brazilian Army Technological Center

William Maniaci, Retired Law Enforcement, Reno, Nevada

Joe Manous, Institute for Water Resources

Dennis Marcello, SFC (Retired), U.S. Army

Louis Marciani

Naney Maruyama

Matthew Matosic

William Maynard

Alan B. McCoy, Emergency Department Tech, Northlake Methodist Hospital, Gary, Indiana

Gayle McKeige

Kathleen McKinna, Public Health Emergency Response Coordinator, Goshen County (Wyoming) Public Health

Randy McLeland

Tom McMahon

Joseph McNiff

Marvin Meinders

Robert Messier, Senior Account Manager, ThermoFisher

Connie Metias, Emergency Management Coordinator, Sherman Oaks Hospital, Encino Hospital Medical Center

Howard E. Michaels, MD, Medical Director, San Jose Fire

Ryan Moeller

Richard Morman, Deputy Chief of Police, The Ohio State University Police

Kenneth Morris, Battalion Chief, Burlington Fire Department

Richard C. Moseley

Robert Mueck

C. Randal Mullett

James A. Murphy, Major, Plymouth County (Massachusetts) Sheriff's Department

Joseph Nadzady

Lawrence A. Nelson, MS NMCEM, Director, Emergency Management, Eastern New Mexico University

Michael O'Connell

Sudhir Oberoi, Health Physicist, Radiation Protection Services, Oregon Health Authority, State of Oregon

Jason Ortiz, Territory Manager, CROSSMARK

Ray Pena, Professional Emergency Manager, Consultant

Christopher Petrillo

Dickens Pierre-Louis

Carter Pittman

Ian Pleet

Donald Ponikvar, Senior Vice President, Defense Group Inc.

Aaron Sean Poynton, Director of Global Safety & Security Business, Thermo Fisher Scientific

John F. Putt, President, Operational Consulting Group

Ronald W. Raab, Ph.D., Professor, Integrated Science and Technology, James Madison University

Joseph Ramirez

David Reddick, Co-Owner, Bio-Defense Network

Patrick Repman, City of Midland Fire Department, District Chief, Deputy Emergency Management Coordinator

Mark Reuther, Vice President, Proengin Inc.

Kelli Russell, MPH, RHEd, Beaufort County Health Department, Washington, North Carolina

Stephen Sabo

Wilborn Sargent

Richard Schoeberl

Dennis R. Schrader, Senior Manager, Integrity Consulting Solutions

Donna Shipman, Training Officer, Granger Fire Department, Washington State

Paula Smith, PhD, Director Disaster Task Force/ Special Operations, Catastrophic Planning & Management Institute

Joseph L. Smith, Director & Senior Vice President, Applied Research Associates Inc.

Preston Smith, III, Anti-Terrorism Officer, Army Cyber Command

Douglas Spencer

Barry Stanford

Brian Stewart, Captain, Glynn County Fire Department

Terry Storer

Lew Stringer

Maureen Sullivan, Emergency Preparedness and Response Laboratory Supervisor, Minnesota Department of Health

Tim Sullivan

Darius Sultan

Nancy Swan, Director of Children's Environmental Protection Alliance (Children's EPA)

Peter Szlezak

Clinton Thetford

Keith Thomas

Dennis Tomczyk, National Center for Biomedical Research and Training, Louisiana State University

Elliot Torres

Lee Trevor, RN, CPIINS, CHEP, Disaster Preparedness Coordinator, TriStar Summit Medical Center, Hermitage, Tennessee

Jim Truman

Samuel Urbaniak

Chris von Wiesenthal, Captain, Special Operations - Hazmat Coordinator/Rescue Specialist, CY-Fair Fire Department, Harris County (Houston), Texas

Michael Joseph Walsh, Director, Emergency Management, Town of Charlemont, Massachusetts

Grace Washbourne

Tyrone Wells

Clint Wichert, Product Manager, Explosives, FLIR Systems Inc.

Mark Wilhelm, Emergency Preparedness Manager, Einstein Healthcare Network

Skip Williams

Terry Wilson, RN, MSN-PHRC, Fremont County Public Health, Riverton, Wyoming

Mary Wolfe

Harold R. Wolgamott, Emergency Services Director, City of Gonzales, California

Kelly Woods Vaughn, Managing Director, Infragard National Members Alliance (INMA)

Phyllis Worrell

Don Wyatt

Carl Yetter, Firefighter III/Hazmat Technician, Anne Arundel County Fire Department-Special Operations

Scott Ziegler

Jean-Christophe Zink, MD, Deputy Director of Emergency Room of Colmar Hospital, CBRNe referent Medical Firefighter, SDIS 68

APPENDIX C
Preparedness Leadership Council (PLC)

Executive Committee

Marko Bourne
Principal, Booz Allen Hamilton

Vayl S. Oxford
National Security Executive Policy Advisor, Pacific Northwest National Laboratory (PNNL)

Kenneth P. Rapuano
Director of Advanced Systems and Policy, The MITRE Corporation

Stephen Reeves
Major General USA (Ret.)

James Schwartz
Chief, Arlington County Fire Department

Robert Stephen
Executive Director, Gryphon Scientific LLC

Craig Vanderwagen, M.D.
Senior Partner Martin Blanck and Associates

Policy Committee

Elizabeth B. Armstrong
Chief Executive Officer, International Association of Emergency Managers (IAEM)

Ann Beauchesne
Vice President, National Security & Emergency Preparedness Department, U.S. Chamber of Commerce

Ellen Carlin
Principal, Carlin Communications

Amy Kircher
Director, National Center for Food Protection & Defense (NCFPD)

Linda Langston
President, National Association of Counties (NACo)

John Morton
Senior Strategic Advisor

Laura Saporito
Policy Analyst, Homeland Security & Public Safety Division, National Governors Association (NGA)

PLC Members

Amy Altman
Vice President Biodefense, Luminex

James J. Augustine, M.D.
Emergency Physician, Clinical Associate Professor, Department of Emergency Medicine, Wright State University

William Austin
Homeland Security Coordinator, Connecticut Capitol Region Council of Governments

Megan Clifford
Deputy Director, Infrastructure Assurance Center, Argonne National Laboratory

John Contestabile
Assistant Program Manager, Homeland Security, Johns Hopkins University/Applied Physics Lab

David W. Cullin, Ph.D
Vice President, Research, Development & Programs, FLIR Systems Inc.

Craig DeAtley
Director, Institute for Public Health Emergency Readiness, MedStar Washington Hospital Center

Richard Giusti
Battalion Chief, San Antonio Fire Department (SAFD)

Kay C. Goss
Chief Executive Officer, GC Barnes Group LLC

Charles J. Guddemi
Federal Law Enforcement Officer

David G. Henry
Homeland Security Consultant, Midwest Region

Jack Herrmann
Senior Advisor & Chief, Public Health Programs, National Association of County & City Health Officials (NACCHO)

Robert P. Kadlec, M.D.
Managing Director, RPK Consulting LLC

Douglas Kinney
Business Continuity/Continuity of Operations Consultant, BDA Global LLC

Stanley Lillie
Brigadier General, U.S. Army (Ret.)

Anthony S. Mangeri, Sr.
Manager of Strategic Relations for Fire Services & Emergency Management, American Public University System

David M. Olive
Founder & Principal, Catalyst Partners LLC

Richard Reed
Senior Vice President, Disaster Cycle Services, American Red Cross

Glen Rudner
Instructor, Security & Emergency Response Training Center

Jeff Runge, M.D.
Managing Member, Vigilant LLC

Dennis R. Schrader
Senior Manager, Integrity Consulting Solutions

Matt Scullion
Vice President Sales & Marketing, BioFire Defense

Timothy Stephens
CEO, MESH Coalition

Maureen Sullivan
Supervisor, Emergency Preparedness & Response Laboratory Unit, Minnesota Department of Health Public Health Laboratory

Mike Wernicke
Vice President, Commercial Development & Operations, Emergent BioSolutions Inc.

Kelly Woods Vaughn
Managing Director, Infragard National Members Alliance (INMA)

Thomas K. Zink, M.D.
Associate Professor, Environmental & Occupational Health, Institute for Biosecurity, Saint Louis University

APPENDIX D
Demographics of DomPrep Respondents

In what sector are you employed?	
	Percentage of Responses
Fire Service	9.7%
Law Enforcement	8.7%
EMS	3.8%
Emergency Management	14.6%
Public Health	14.8%
Hospital (including VA)	9.3%
Federal Government	7.5%
Military	2.6%
State/Local Government	5.5%
Non-Government Organizations (NGOs)	3.0%
Privately Owned Company	8.3%
Publicly Traded Company	4.7%
Self Employed	2.0%
Not Employed	0.6%
Academic Institution	4.3%
Student	0.6%

What type of position do you hold?	
	Percentage of Responses
Upper Management	26.6%
Middle Management	28.4%
Operations	18.1%
Technical	6.8%
Training	5.4%
Administration	6.2%
Other	8.5%

"Today we were unlucky, but remember we only have to be lucky once. You will have to be lucky always."

–The Irish Republican Army, after narrowly missing
British Prime Minister Margaret Thatcher
During the 1984 Brighton Hotel Bombing in England

Underwriters

BIOFIRE
DEFENSE

QuickSilver
ANALYTICS, INC.

FLIR

Thermo
SCIENTIFIC

protected by emergent
biosolutions