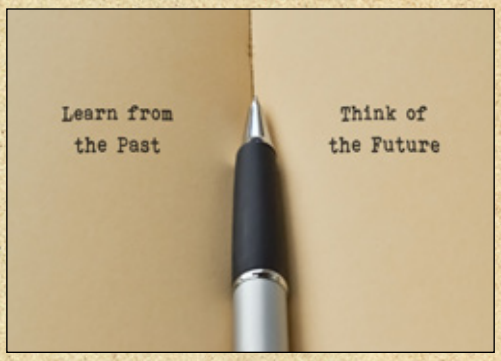
domestic preparedness .com

DomPrep Journal

Subscribe Volume 13, Issue 12, December 2017

Emerging Threats to Rail Infrastructure: Part I, Freight
By Joseph Trindal



ARTful Leadership & Disaster Management
By Eric J. McNulty

The Presidency & Control of Nuclear Weapons
By Jerome H. Kahan

Mass Fatality Research – New York & Beyond
By Katie Joel & Terry Hastings

Indiana's Emergency Response Guidelines for School Safety
By Robert Quinn

Maryland's Approach for Raising the Resilience Index
By Charissa Cooper & Jessica Nusbaum

10 Questions for Selecting Business Continuity Software
By Erin Valentine

Excess Equipment Sales & Potential National Security Threats
By James M. Rush

EMERGENCY SERVICES WEBINAR SERIES 2017

KNOWLEDGE WHEN YOU NEED TO RESPOND

In the world of emergency operations, conditions change. So does the knowledge needed to respond effectively. American Military University (AMU) is proud to host a series of free, 1-hour webinars for responders and emergency managers, covering these and other essential topics:

- Violent Incident Consequence Management, the Emergency Manager's Role
- Principal Investigator for the Firefighter Injury Research and Safety Trends (FIRST)
- Drafting and Implementing Effective Fire Department Policies and Procedures
- Financial Systems Management for Fire and EMS Agencies
- Organized Response to Mass Casualty
- Firefighter Health: Heart Healthy Solutions

Webinar attendees may receive a 5% tuition grant for degree and certificate courses at AMU.

REGISTER FOR THE WEBINAR SERIES TODAY AT
PUBLICSAFETYATAMU.COM/ DPJ

FOR MORE INFORMATION ABOUT CUSTOMIZED TRAINING TO MEET YOUR NEEDS, CONTACT ANTHONY MANGERI AT
AMANGERI@APUS.EDU.

AMU American Military University
Learn from the leader.™

AMU is part of the accredited American Public University System and certified to operate by SCHEV.

Business Office
P.O. Box 810
Severna Park, MD 21146 USA
www.DomesticPreparedness.com
(410) 518-6900

Staff
Martin Masiuk
Founder & Publisher
mmasiuk@domprep.com

Catherine Feinman
Editor-in-Chief
cfeinman@domprep.com

Carole Parker
Manager, Integrated Media
cparker@domprep.com

Advertisers in This Issue:

American Military University

BioFire Defense

Federal Resources

FLIR Systems Inc.

PROENGIN Inc.

DomPrep Journal is electronically delivered by the IMR Group Inc., P.O. Box 810, Severna Park, MD 21146, USA; phone: 410-518-6900; email: subscriber@domprep.com; also available at www.DomPrep.com

Articles are written by professional practitioners in homeland security, domestic preparedness, and related fields. Manuscripts are original work, previously unpublished, and not simultaneously submitted to another publisher. Text is the opinion of the author; publisher holds no liability for their use or interpretation.

Featured in This Issue

Pictured on the Cover: (top row) Trindal, Source: ©iStock.com/af_istocker; McNulty, Source: ©iStock.com/benjaminec; (second row) Kahan, Source: U.S. Army; Joel & Hastings, Source: ©iStock.com/adrianocastelli; (third row) Quinn, Source: ©iStock.com/csfotoimages; Cooper & Nusbaum, Source: MEMA, 2017; (bottom row) Valentine, Source: ©iStock.com/TECHDESIGNWORK; Rush, Source: ©iStock.com/bashta

Invisible Threats Exposed

AP4C

Portable Chemical Detection System
Protects First Responders, Military & Infrastructure

- Fast, Reliable Analysis of Invisible Hazards Saves Time & Lives
- Unlimited Simultaneous Detection Exposes Unknown Agents
- Low Maintenance & Operation Costs Save Money
- Rugged Handheld Design is Easy-To-Use With Minimal Training
- Complete System Includes Accessories & Case for Easy Transport

Learn More Online

PROENGIN

Chemical and Biological Detection Systems

Preparedness & Resilience Without the Hype

By Catherine L. Feinman

As another calendar year comes to a close, agencies and organizations are reflecting on the events of 2017: hurricanes, mass shootings, wildfires, critical infrastructure failures, disease outbreaks, cyberattacks, and other incidents that have strained local resources. DomPrep's readers are continually challenged to be prepared for, respond to, and mitigate the consequence of disasters. When a crisis occurs, the gaps in planning and response are forced into the spotlight. However, when disasters are diverted, the success often goes unseen. This edition of the *DomPrep Journal* recognizes and thanks all those who work behind on the firing line and behind the scenes everyday to make their communities safer and more resilient through their activities, informational resources, and recommendations.

Those tasked with preparedness and resilience roles participate in numerous activities, including tabletop and full-scale exercises, conferences, and discussions with other local, regional, and national stakeholders. DomPrep roundtables, for example, bring together diverse groups of professionals to identify a problem and find possible solutions. Others hone their leadership skills and build relationships to better prepare for the next disaster. Of course, leadership comes with great responsibility to do the most good for the most people, which includes all levels of leaders from the local fire chief to the president of the United States.

The driving forces behind many preparedness and resilience efforts begin with informational resources and tools. Tools created for one jurisdiction are often applicable to others. However, they are only beneficial if they are shared. This includes research on low-frequency, high-consequence events – such as mass fatalities – to help build resilience in areas that have yet to experienced them. It also includes response guidelines created for one jurisdiction being used as a building block for others.

In addition to research, guidelines, and other informational tools, recommendations based on lessons learned and best practices are critical for building community resilience. Partnerships and information sharing play key roles when the goal is to increase resilience within and between communities. Asking the right questions and making the best purchases in advance help to ensure continuity of operations and continuity of government when disasters do occur. Potential security threats must be considered at every stage of the planning process – from evaluation to resource management, including disposal of equipment. This is just a fragment of what has been and continues to be done – often without accolades – to keep communities safe, secure, and resilient.

Best wishes for a safe and resilient New Year!

Emerging Threats to Rail Infrastructure: Part I, Freight

By Joseph Trindal

There is a desire for some bad actors to target rail systems, especially the hazardous materials freight rail network. This threat underscores the need for the rail transportation industry to maintain and strengthen partnerships with federal, state, and local authorities. With over 140,000 miles of infrastructure, there are difficult security challenges. For example, the U.S. rail system moves over 1.8 billion tons originated/year of freight, petroleum, chemicals, and military assets, making it a vital lifeline. A recent roundtable examined current issues and progress regarding this important topic from government and private sector experts.

Analysis of terrorist attack and plot trends targeting transportation infrastructure in developed countries demonstrates a growing interest in rail systems. Over the past 13 years, European rail systems infrastructure have been the increased focus of successful terrorist attacks, failed attempts, and disrupted plots. Examples include:

- The March 2016 suicide bombing on board a metro train at a station in the center of Brussels, Belgium, part of a coordinated operation that targeted the city's international airport, killed 32 people and wounded more than 300 others;
- The March 2010 coordinated suicide bombings in Moscow, Russia, subway killed 40 and injured more than 100;
- The July 2005 coordinated suicide bombings on three underground trains and a double decker bus in London, UK, public transport killed 52 people and injured over 700 more;
- The March 2004 coordinated bombings over a period of about four minutes on four commuter trains operating on the same line in Madrid, Spain, killed 192 people and injured over 1,800 others.

Noteworthy terrorist failures include the September 2017 attempt to detonate an improvised explosive device on board a London Underground train at Parsons Green station and the attempt to execute a mass shooting on board a high-speed train operating in northeastern France in August 2015. In the United States, numerous plots envisioning attacks on domestic rail systems have been disrupted, the most advanced being a plan to detonate suicide explosives on board New York City subway trains foiled in September 2009. More recently, a plot to target a VIA Rail passenger train in the Toronto, Canada, area during the September 2012 to April 2013 period was disrupted by the combined efforts of a joint investigation. The Royal Canadian Mounted Police and the Federal Bureau of Investigation (FBI) monitored the two main plotters and the timely reporting of pre-attack surveillance observed by a conductor on a passing train operating on the targeted rail line.

Certainly, the interest of terrorist groups in targeting rail systems has persisted. In August 2017, al-Qaida published issue 17 of its Inspire online publication that focused on inciting attacks against both passenger and freight rail systems in the United States and Europe. On 10 October 2017, Domestic Preparedness moderated a roundtable discussion entitled "Emerging Threats to Freight Rail Infrastructure." The panel was comprised of distinguished speakers representing a board range of stakeholders in the freight rail transportation sector. Representatives from the following agencies and organizations contributed to this discussion on emerging threats and mitigation strategies in the freight rail transportation sector: Transportation Security Administration (TSA), Threat Analysis Division; TSA, Office of Security Policy and Industry Engagement; the FBI's Rail Security Program; the U.S. Department of Defense (DoD) TRANSCOM; National Protection and Preparedness Directorate (NPPD), Protective Security Coordination Division; Amtrak Police, Criminal Intelligence Unit; the Association of American Railroads (AAR); and the Secure Technology Alliance. Many interesting and relevant points were discussed during this important roundtable event.

Holistic Perspectives on Threat Mitigation

The panel acknowledged that, although the trends in terrorists' actions and priorities continuously evolve, so too are integrated measures to disrupt, detect, and mitigate threats to the freight rail industry. Recent events indicate a terrorist focus on the rail sector, but predominately target passenger and commuter rail systems. Attacks such as 2017 Parsons Green bombing in London and the 2016 Brussels bombings targeted urban commuter rail infrastructure during peak hours. TSA's officials made clear that the risks of attack on the freight rail sector are low. The FBI pointed out that their investigative activities still include cargo thefts by criminal actors and gangs, as well as disruptive activities targeting freight rail by environmental activists. The panel identified cyberthreats as an emerging challenge, a common public and private sector threat across customer facing, business, and operational systems.

The panelists agreed that defeating every threat is practically unattainable. However, disrupting plots and creating difficult environments that thwart attacks are key elements of a shared strategy for narrowing risks. It was pointed out during the discussion that, if some of the early indicators of the Parsons Green and Brussels attacks as well as other successful terrorist operations against passenger trains and stations had been recognized, reported, and acted upon, these plots may have been disrupted before the attacks were launched. According to a 16 September 2017 BBC news report, London's Metropolitan Police commissioner, Cressida Dick, stated that police had interdicted six "significant plots" in the months leading up to the Parsons Green attack. A shared challenge across the rail sector is recognition and early identification of threat indicators.

The TSA and FBI both noted that public and private stakeholders in the rail industry work closely together in developing broad understandings of threat indicators. TSA's Threat Analysis Division assesses data collected from a wide array of sources, domestically and abroad, to produce threat analysis products that are disseminated to stakeholders in both the public sector and throughout the rail industry in the United States and Canada. Although the discussion panel included representation from many organizations, the panelists knew one another well. Many panelists stated that they talk with one another on a daily basis.

Strength in Partnerships

Developing and maintaining a holistic threat understanding requires constant coordination among the stakeholders, both internal within government and external with the private sector. Thriving partnerships share certain common goals and understandings that weather the test of time. The 9/11 attacks caused significant economic impact across several levels of the aviation industry as well as disrupting many nation-state economies. For both public and private sectors, a unifying common thread is the shared understanding of economic consequences of terrorist plots that target critical infrastructure.

In the rail sector, the railroad police agencies have a long history of working with local public sector police agencies in investigating cargo thefts and rail asset vandalism. Today there is close interaction among federal, local, and railroad agencies, with the FBI's Rail Security Program and their local field offices taking a proactive role. The FBI frequently supports local law enforcement and railroad police agencies in nonterrorist criminal matters with intelligence and investigative support.

State, local, federal, and railroad partnerships are strengthened through a national network of local-based task forces, such as the FBI-led Joint Terrorism Task Forces (JTTFs). Numbering over 80 JTTFs nationwide, law enforcement representation includes railroad police in many locations.

The American Association of Railroads (AAR) is a nonprofit industry group representing the Class I freight railroads, Amtrak, and some regional railroads. The AAR expressed the strength by which the railroads collaborate with the federal and local government partners. The AAR member railroads have a long history of working with state and local first responders on both safety and security matters. Within the freight railroad industry, AAR leads its members in developing and maintaining unified security plans that are current and inclusive. The AAR unified security plan model focuses on five key areas: (1) train operations, (2) critical infrastructure, (3) hazardous materials, (4) military transport, and (5) cyber and communications. In implementing the plan, the AAR serves as the security information center for the railroad industry and facilitates preparedness exercises jointly, involving railroads and government officials across the United States and Canada. These regular, recurrent, structured exercises are designed to place plans and procedures under stress in realistic terrorism and cyberthreat incident scenarios, develop lessons learned in areas for improvement, and apply those lessons to strengthen future capacities for all participating organizations.

Relationships among federal, state, local, and tribal government agencies are stronger through the establishment of intergovernmental points of contact across jurisdictions. The growth of state and locally operated fusion centers has generated a network of intergovernmental collaboration. Operating under a National Network of Fusion Centers with unifying guidelines, intelligence, advisories, and lessons learned are rapidly and securely communicated. Private sector representatives with proper clearances and bone fide "need to know" are integrated into the National Network of Fusion Centers.

The Rail Sector Coordinating Council, stemming from the National Infrastructure Protection Plan, is the rail industry principal liaison forum of coordination between the railroads, stakeholder organizations, and the government. An important coordination strategy for AAR members is to achieve the goals of the National Infrastructure Protection Plan and sector-specific plans by proactively and collaboratively planning, training, exercising, sharing information, and assessing capacities against risks. The railroad industry supports the threat awareness of fusion centers through sharing of advisories on matters pertaining to terrorism, cyberthreats, and measures to mitigate risk.

U.S. Department of Homeland Security's (DHS) Protective Security Coordination Division fields Protective Security Advisors (PSAs) across the country to engage the 16 critical infrastructure sectors, which include the Freight Rail sub-sector. The PSAs' primary mission is to protect critical infrastructure. The five mission areas are: (1) plan, coordinate, and conduct security surveys and assessments; (2) plan and conduct outreach activities; (3) support National Special Security Events and Special Event Activity Rating Level I and II events; (4) respond to incidents; and (5) coordinate and support improvised explosive device awareness and risk mitigation training. PSAs are security subject matter experts who engage with state, local, tribal, and territorial government mission partners and members of the private sector stakeholder community to protect the nation's critical infrastructure. PSAs serve as regional DHS critical infrastructure security specialists, providing a local perspective to and supporting the development of the national risk picture by identifying, assessing, monitoring, and minimizing risk to critical infrastructure at the regional, state, and local levels.

In August 2017, al-Qaida published an online magazine that focused on inciting attacks against both passenger and freight rail systems in the United States and Europe.

In addition, there is a network of railway enthusiasts, called "rail buffs," who make a recreational hobby out of observing and noting railroad activity. Many rail buffs are well known to railway engineers and workers; some even on a first name basis. These rail buffs tend to be very familiar with their railway areas of interest and can easily spot suspicious behavior or activity. The rail buff network is loosely connected through the Railfan Network. Local railroad and law enforcement collaboration with rail buffs is an example of grassroots connectivity.

A collaboration challenge from some organizations is continuity of principal points of contact. For some agencies and organizations, personnel assigned to key collaborative positions change every few years. Relationships are built over time and, when personnel change with promotions or reassignments, it can be disruptive. At the very least, a degree of institutional knowledge and expertise needs to be re-learned. This matter tends to be more of an issue with some of the federal agencies than local and railroad organizations.

Through the network of government, private, and citizen collaboration around the freight rail industry, terrorists' ability to prepare an attack is made more difficult, takes longer and provides much greater risk of detection and interdiction. Collaborative success is demonstrated in the high volume of thwarted terrorist plots in recent years.

State of Rail Sector Information Sharing

Networks of collaboration are only useful and sustainable if they provide value to the network stakeholders. Meaningful information sharing – distilled from data and intelligence analysis – is critical to keeping ahead of evolving terrorist threats. Within the federal agencies, there are verticals of information sharing between agency headquarters and the agency's field personnel. More important is the information flow that spans across agencies and includes private sector stakeholders.

The federal agencies with responsibilities for freight rail security today are closely integrated in sharing information across common networks and direct collaborative relationships. For example, the FBI information-sharing network goes beyond headquarters to the field, as the FBI oversees 84 JTTFs with representation across numerous federal, state, and local agencies. The FBI's Rail Security Program engages with railroads and other federal agencies at various levels, with multilateral information sharing. The FBI and TSA also collaborate with trusted international partner countries drawing on intelligence, incident analysis, and lessons learned. Collectively, the network of public and private information analysis, intelligence development, and sharing improves stakeholder threat awareness.

Agencies and private sector information sharing takes many forms. The joint government-industry coordinated Rail Intelligence Working Group (RIWG), is an example of public and private sector collaboration in action for information sharing. The group is comprised of representatives from the FBI, TSA, Amtrak, the American Public Transportation Association, and AAR – a partnership that remains unique across critical infrastructure sectors. Recently, the RIWG analyzed the video and the August 2017 Inspire edition. These materials urged supporters to target trains, particularly emphasizing so-called "Train Derail Operation" with lengthy instructions on building a "homemade derail device" for this purpose. The RIWG developed and disseminated informational awareness advisories through various rail industry and public sector networks, including the AAR's Railway Alert Network. These materials highlighted both the complexities of the actions advocated and the lack of understanding reflected in the magazine articles of the rail transportation system and its safety and security capacities. This cooperative effort reflects a joint commitment to sharing timely and useful security information across government and industry for security enhancement.

Complementing this work, the AAR publishes the Rail Awareness Daily Analytic Report (RADAR) as well as focused awareness advisories through the Railway Alert Network, keeping railroad and government stakeholders continuously informed on matters of relevance to rail security. Similarly, both TSA and the U.S. Department of Transportation produce and disseminate informational, intelligence, and alert products. Recipients of the governmental and Railway Alert Network products include officials with numerous federal agencies in the United States and Canada, state and regional fusion centers in the United States, and law enforcement and physical and cybersecurity leads for freight and passenger railroads in the United States and Canada.

The FBI's Tripwire Program has proven highly effective as a means for actionable information sharing. Described as "See Something, Say Something with focus," the Tripwire Program educates industry stakeholders on key trends and potential indicators of criminal terrorist preparation. Stakeholders are encouraged to report any suspicious activity with relevant details to local law enforcement or the FBI Field Office. The FBI conducts a structured assessment of Tripwire reports, some of which have led to preliminary investigations with a few resulting in criminal investigations and prosecution before planned attacks materialized.

Effective rail industry-centric information management ensures that priorities are aligned, and timely action is taken, in a concerted effort to create conditions to prevent bad outcomes. AAR pointed out three elements of the railroad industry's security strategy. First, understand that prevention is attainable. Second, worry less about what is not known and learn what can be known as thoroughly as possible. Third, avoid self-inflicted wounds through actions that ease adversaries' ability to achieve their disruptive, destructive, and event lethal purposes. Gaining continuous situational awareness from reporting by railroad operators while providing these operators with relevant threat intelligence and related security information is advantageous for developing a results-oriented preventive posture.

Through effective information sharing that creates a climate of relevant awareness and response, threats can be either blunted or significantly mitigated in potential effects. AAR also stressed the need to ensure that information-sharing structures avoid inadvertently facilitating the preparation of criminals and terrorists. Rail operations and security information must be shared only with those who have a valid need to know. Government information-sharing networks are only accessible by credentialed personnel who have been vetted and meet agency standards for physical and logical access to systems and information. Similarly, railroads control access to security information received from all sources.

Cyberthreats, vulnerabilities, and attacks are increasing. Threats and attacks are focusing on public facing, business, and operational enterprise systems and devices, including person and nonperson tractions, personal and support staff, and third-party vendors and service providers. The continued expansion of the internet of things and smart connected transactions are creating new and ever-increasing exploitation opportunities. These threats have implications for the freight rail infrastructure, especially given the evolution and integration between rail operation and business enterprise systems, in addition to known ICS/SCADA weaknesses and vulnerabilities.

Public and private sector leaders are working together to address this threat. Cybersecurity is the fastest growing focus of railroads, government agencies, and DoD. DoD's reliance on commercial rail infrastructure has been long established. Today, DoD TRANSCOM's surface deployment mission is supported in large part by commercial railroads. DoD's rail deployments are closely synchronized with mission commands and the railroad industry, where movement information must be secure. Currently, DoD is working with the Critical Infrastructure Resilience Institute, a DHS Science and Technology center of excellence operated by the University of Illinois at Urbana-Champaign, to develop a refined cyberrisk scoring metric.

Similarly, AAR member railroads have elevated cybersecurity at the top of their priority lists. As freight rail systems become more automated and integrated, railroad investment in securing information technology networks – including those in development for the Positive Train Control system, which includes design to mitigate the risk of exploitation by cyberthreats. Amtrak pointed out that they have invested and continue to invest in securing their cyber systems. Nearly 85% of Amtrak's ticket sales take place on the internet. Amtrak police vigorously investigate growing volume of cyber and financial crimes involving their ticketing system.

A major challenge in top-down information sharing is the security classification of the information. The federal government Code of Federal Regulations (CFR) establishes requirements for managing unclassified but sensitive information. The term "Sensitive Security Information" (Title 49, CFR, Part 1520) is applied to information that falls short of meeting the National Security Classification regulations, but if disseminated it would be detrimental to the transportation security. TSA's sharing of Sensitive Security Information provides an important intermediate level for broader dissemination with regulatory safeguards and information security standards.

Freight Rail Security Regulatory Influence

Both DHS and U.S. Department of Transportation provide federal regulatory oversight of freight rail security matters. Additionally, some states apply regulations that impact freight rail security. The TSA Rail Transportation Security Rule (Title 49, CFR, Parts 1520 and 1580), promulgated in 2006, is among the federal regulations designed to strengthen rail industry security and reduce risk associated with the transport of security-sensitive materials. The Rail Security Rule developed into regulatory requirements practices that most railroads had already implemented. For example, the rule requires secure chain of custody of security-sensitive materials, which most railroads had already performed pursuant to agreed, voluntary security actions with TSA as a prudent business practice. The rule further requires regulated railroads to designate a rail security coordinator and mandates security concern reporting to TSA. The rail security coordinator requirement does enhance consistency in public and private sector coordination with the regulated railroads.

Regulations, at both state and federal levels, have generated linear reporting mandates and prescribed standards. However, regulatory reporting standards tend to be reactive and cannot replace stakeholder driven initiatives to build strong, functional relationships. As one TSA official stated, "Our success has been built on collaboration, not regulation."

Many on the panel pointed out that regulation alone does little to enhance rail security and may, in some instances, produce the self-inflicted damage that should be avoided. The U.S. Department of Transportation requirement for railroads to report to states detailed information on the routes used, and frequencies of operations on those routes each week, by trains transporting high volumes of crude oil and other flammable liquids has resulted in publication of those schedules. Open-source publication of the operations of hazardous shipments unnecessarily releases security and safety information outside the first responder and community emergency planning agencies – and needlessly exacerbates risk.

Regulatory oversight by government inspectors and reporting regimes strain the railroads' personnel resources. In some situations, rail security coordinators and other railroad personnel are drawn away from performance based rail security matters to address report legibility or formatting. Security regulatory development and implementation should be collaborative between public and private sectors – as the private sector best practices often exceed regulatory standards.

Key Takeaways

The current and future state of freight rail security continues to change. The panel addressed a number of key strengths and some challenges for securing the nation's freight rail infrastructure. Some of the salient points from the Emerging Threats to Freight Rail Infrastructure roundtable discussion include:

- Threats are dynamic – There is significant evidence that threat trends involving the freight rail transportation infrastructure are changing. Intelligence assessments and extremists' propaganda and threats reflect a continuing interest of terrorists in targeting rail systems. Cyberthreats are increasing as well, which has implications for business and operations networks of railroads. Generally, the threat to rail systems is low but, as one participants stated, "Low does not mean 'no'."
- Cyberthreats are increasing – This includes attacks on public facing, business, and operational enterprise systems, including person and nonperson tractions, personal and support staff, and third -party vendors and service providers. The continued expansion of the internet of things and smart connected transactions are creating new and ever-increasing exploitation opportunities. This has implications for the freight rail infrastructure, especially given the evolution and integration between rail operation and business enterprise systems.
- Criminal activities overshadow terrorist threat – The federal, state, local, and railroad police agencies investigate far more cargo theft, vandalism, and disruptive criminal activity, including trespass and blockades by protesters, than terrorist plots involving the freight rail sector.
- Stakeholder partnerships are strong – The coordinated effort among federal, state, local, and private sector agencies and organizations is stronger than ever before. Through rail sector focused task forces, fusion centers, working groups

and interagency networks, collaboration for planning, information sharing, training, outreach, response, and recovery are based on common goals of enhancing security.

- Public and private partnerships are collaborative – Stakeholder organizations in the public and private sectors have designated points of contact and established functional structures to promote collaboration and coordination around rail system security. Effective practices for elevating prevention and response capacities are widely shared among the railroads and with public sector agencies.
- Information sharing is multi-lateral and relevant – Intelligence and security information sharing occurs continuously among freight and passenger railroads, federal government agencies, state and regional fusion centers, and law enforcement agencies through a variety of networks. This extensive effort develops and sustains a current and relevant understanding of threat indicators and informs reporting capacities among stakeholders in industry and government. Enhancing security through constant emphasis on effective information sharing remains a common focus with public and private sector organizations. All involved apply appropriate protections based on need-to-know and access controls.
- Freight railroad security focus and capacities are strong – The Class I railroads, as well as most others, maintain strong security capabilities. AAR provides uniform and consistent guidance and support for its railroad members. The railroad industry's unified security plan in use by all Class I railroads and many others is an industry standard. AAR supports security awareness training through products disseminated to freight and passenger railroads via the Railway Alert Network and facilitates preparedness exercises for the railroad industry, which includes public sector agencies in the United States and Canada. The railroads actively engage with federal, state, and local investigative and intelligence agencies to ensure continued access to relevant information and analysis.
- Information security challenges remain – Some information and intelligence obtained by federal agencies is highly classified and has limited distribution in its raw form. Agencies have developed standards for redacting or recasting classified information into unclassified intelligence products while still maintaining security protocols. TSA's Sensitive Security Information is an example of unclassified but sensitive information, which can be shared and managed in accordance with federal regulations. Representatives of state and local agencies as well as designated private sector employees, with bone fide need-to-know, may be sponsored for security clearance to receive classified briefings and intelligence products.

- There are three key risk mitigation points – (1) Understand that prevention is attainable; (2) learn as much as possible about what can be known; and (3) avoid self-inflicted wounds. Many potential threats and security risks can be avoided or substantially mitigated by acting on timely and actionable information. Develop thorough practical understanding of security threats at the right levels and align resources and capabilities accordingly. Recognize that resources are finite; partnerships based on common priorities and practical information can be effective in actionably preventing most risks. Avoid inadvertently making the terrorists' or criminals' planning and preparedness easier to put into action. Maintain informational and operational security over sensitive information that could be useful to terrorists and criminals.
- Railroads are prioritizing cybersecurity – As the industry moves toward greater reliance on integrated cyber systems, railroads recognize the economic returns for investing in secure system designs. Cybersecurity is a high priority throughout the railroad industry.
- Railroad regulations have limitations – Regulations levied on the freight rail industry have increased over the years. Many of the regulatory requirements codify and establish government oversight over best practices that had already been established by freight and passenger railroads. Some regulations between jurisdictions undermine strong security measures. Regulations alone do not create collaboration. Greater alignment between regulatory rule making and the railroads would go a long way to harmonizing best practices and achieving the shared goals between the public and private sector.

Conclusion

Western railroad system infrastructure continues to be an evolving terrorist target of interest. Expressed terrorist organizations' desires to sow economic harm through attacks involving critical infrastructures – for example, passenger and freight rail systems – is publicized in their global outreach to affiliated and non-affiliated groups as well as lone actors seeking recognition. Although the proliferation of global, web-based outreach by certain terrorist groups to unaffiliated groups and lone actors may indicate the effectiveness of multinational counterterrorist operations, it also creates new challenges for pre-attack detection and interdiction.

In the United States, the continued strengthening of public and private partnerships in the freight rail sector creates extreme difficulties for terrorists and criminals to succeed in executing attack plots. Intergovernmental cooperation and information sharing continue to improve with actionable lessons learned and pre-attack indicators shared bilaterally between local personnel and national agencies. Similarly, the daily interaction between the rail industry and government officials, at all levels, enhances situational awareness such that terrorist pre-attack and plot indications are more likely detected and proactively thwarted.

Joint federal, state, and local interdiction and prosecution of terrorist plotters are indications of the successes stemming from public and private partnerships.

Challenges remain for private sector and government agencies in the freight rail sector. As demonstrated by the security and safety initiatives implemented by railroad companies and standardized by private industry organizations like the AAR, the private sector's economic interests drive innovation that stay ahead of government regulations. Many of the railroad companies' security procedures exceed regulatory minimum requirements, whereas some regulations even divert private sector resource priorities in counterproductive ways. Intergovernmental regulations and policies need greater alignment in developing cohesion between federal, state, and private sector shared objectives for freight rail security and safety. With emerging cyberrisks and the growing need for information security in the global digital age, all stakeholders in the rail transportation sector need to examine ways to deny terrorist plotters and attackers access to open source information and resources. Creating greater difficulties for terrorists and criminals is a universally shared public and private sector sustainable goal.

DomPrep would like to thank all those who participated in the 10 October 2017 discussion, upon which this white paper is based. The participants who contributed to this important discussion include but are not limited to the following:

Zamawang Almemar, *Chair of ZAMA and Associates LLC*
Jason Carnes, *Chief, Modal Analysis–Intel Analyst, DHS/TSA/Threat Analysis Division/Strategic Analysis Branch*
Wayne "Jake" Carson, *Chief, Mission Assurance Branch/TRANSCOM, DOD - SDDC/JDPAC/TRANSCOM/ Mission Assurance Division*
James A. Cook, *Inspector, Amtrak Police Department*
Thomas Farmer, *Assistant Vice President Security, Association of American Railroads*
James Finney, *Protective Security Advisor – National Capital Region, Department of Homeland Security*
Scott Gorton, *Manager, DHS/TSA/Office of Security Policy & Industry Engagement/Surface Division/ Freight Rail Industry Engagement*
Albert J. Guarnieri, *Supervisory Special Agent, Federal Bureau of Investigation*
Thomas J. Lockwood, *Board Member, Secure Technology Alliance*

Joseph W. Trindal, PPS, is a career homeland security professional with over 40 years of experience in both public and private sector. He has been a contributing writer to DomPrep for over 10 years. Having served for two decades with the U.S. Marshals Service, attaining the position of chief deputy U.S. marshal, he answered an invitation to contribute in creating the U.S. Department of Homeland Security (DHS) as regional director of the Federal Protective Service for the National Capital Region. During his service as an executive at DHS, he led a select team developing the Chemical Facility Anti-Terrorism Standards regulations, DHS's first legislated regulatory authority. Since his retirement, with over 30 years of government service, he continues executive service, now in the private sector security industries. A past president of the FBI's InfraGard, he led the transformation of the National Capital Region Chapter into a leader in public-private partnership initiatives. Currently, he is president and chief operating officer with the Akal Group of Companies, leading over 2,000 employees serving in 22 countries with a $250M portfolio of U.S. government and private sector contracts. Living in Virginia, and a veteran of the U.S. Marine Corps, he holds degrees in police science and criminal justice.

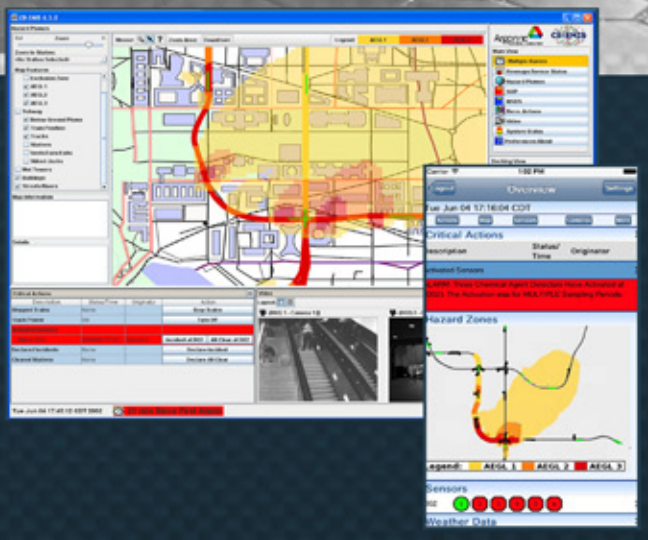
PROTECT™

A systems approach to **SAVING LIVES.**

Real-time CBRNE detection, surveillance and crisis management application.

DETECT
IDENTIFY
ANALYZE

COMMUNICATE
RESPOND
ISOLATE



High threat, high visibility installations such as subways, mass transit terminals, and airports, require rapid detection and verification of chemical agent attacks. **PROTECT**™ delivers and **SAVES LIVES**.

FEDERAL RESOURCES®

800.892.1099
federalresources.com

ARTful Leadership & Disaster Management

By Eric J. McNulty

Disaster preparedness and response professionals had a front-row seat for the turbulence in 2017. A historic hurricane season left first responders and the communities they serve struggling to keep up. Fires continue to ravage the west. Active shooter and terrorism incidents keep everyone on edge. Infectious disease outbreaks remain a constant worry. Cyberattacks open a new threat vector. Prolonged preparation, response, and recovery put stress on physical, emotional, financial, and infrastructure systems. Leaders must adapt to changing circumstances and needs.

The term VUCA is familiar to many in the preparedness and response communities. It stands for volatile, uncertain, complex, and ambiguous. Military officials coined the acronym to describe the emerging threat matrix defined more by disaggregated actors such as al-Qaida and, more recently, the Islamic State group (IS) and lone-wolf attackers than by monolithic threats such as the Soviet Union. Today, the VUCA is used to describe everything from business conditions to weather in addition to its military applications. It calls for more nimble thinking and action. In the context of VUCA:

- *Volatility* is the real and perceived increase in the pace of change.
- *Uncertainty* reflects a decline in predictability – surprises are to be expected.
- *Complexity* refers to the myriad interdependencies that connect organizations across geographic, sector, and social boundaries. In complex adaptive systems, similar inputs may yield wildly different outputs.
- *Ambiguous* refers to certain fuzziness in the present and the future, "Who exactly is the enemy – and how best are they countered?"

The Context Now: From VUCA to VUCAST

Through personal research, two more letters have been added to the acronym: System-scale change (S) and Transparency (T). *System-scale change* marks the current age. There have always been wars, financial volatility, pandemics, and other disruptions. However, the simultaneous remaking of multiple industries – from banking to publishing to retail and more – has been leading to uncertainty about jobs and financial well-being. Along with this, there are significant shifts in the natural world on which societies depend for food, water, and other resources. For example, severe weather events are reported to be increasing in frequency and intensity.

Four mega-trends stand out where the long-term trend line is clear, even though there remains great variability over the short-term. These trends have global effects and the potential to be fundamentally transformational:

- *Climate change* – Hurricanes Harvey, Irma, and Maria are just the latest examples of the consequences of a climate in flux. Dramatic wildfires flare.

Seas are rising and warming. Wet places are getting wetter. Drier areas are becoming drier. Crop yields are less predictable. Food and water insecurity are on the rise.

- *Global urbanization* – More than half of the human population now resides in urban areas and will rise to 75% by 2030. Most of this growth will be in the developing world without robust governance structures or public health infrastructure. For example, Ebola became a global threat in 2014-2015, not because it was a new virus but rather because it emerged in a densely populated area where rapid spread was inevitable – and almost unstoppable.
- *The aging of the developed world* – The global north is aging because of greater longevity. Europe is aging fastest followed by North America. Vulnerable elderly populations present distinct challenges for first responders, the health care system, and other preparedness, response, and recovery professionals.
- *The continued exponential growth of computing power and, with it, interconnectedness* – Technology will continually evolve rapidly, making investment decisions more challenging than ever. Collective knowledge will surge, and an unprecedented number of people will have access to it.

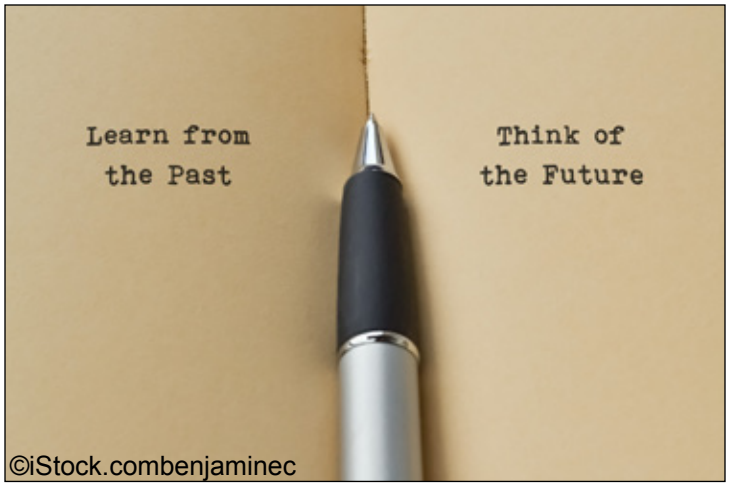
The T is for ubiquitous *Transparency*. In the new reality, almost everyone can see almost everything in almost real time thanks to innovations such as smartphones, pervasive communications networks, and even low-level commercial satellites. The power to upload live video is in the hands of the average person. For example, on social media, citizen journalists streamed live, raw, unfiltered reports of the August 2017 protests in Charlottesville, Virginia. In another case, a video of an airline passenger dragged from his seat by security personnel became an instant viral sensation. On a daily basis, body-camera footage documents the actions of law enforcement.

In a VUCAST world, there are three defining characteristics of organizations that thrive, be it a government agency, nongovernmental organization, or a private sector corporation: *Adaptive* capacity, *Resilience*, and high levels of *Trust* (ART). Building this capacity is at the heart of ARTful leadership.

Making the Shift to ARTful Leadership

Despite living in the digital age, many organizations remain rooted in an analog, industrial mindset based on linear thinking that optimizes for control. A thicket of regulations and rules governs who does what. It takes years to learn how to work in the system. In such an environment, individuals play defense – protecting turf, jockeying for position, and waging petty political battles. Success is measured in control-centric tangible terms such as title, jurisdiction, budget size, and number of direct reports. Stagnation and rigidity often set in.

ARTful leaders instead optimize their organizations' flow of information, resources, energy, and initiative. This is how upstarts such as Airbnb, Uber, and Amazon.com have upended their industries. For example, if Amazon.com ran a disaster response operation, automation and artificial intelligence would help improve logistics. Constant experiments would be run to improve the ease and efficiency with which survivors receive information



and assistance. Big data analytics would optimize matching resources with needs and measuring impact. Continuous improvement would be daily practice.

More important than any technology is the ARTful mindset. With confidence in an abundance of situational understanding, expertise, and judgment throughout the enterprise, decisions are pushed downward. Frontline responders are given both the freedom and expectation that they will act with agility and intelligence. Industrial-age leaders were commanders. ARTful leaders are catalysts for collaborative problem solving.

Adaptive Capacity

Adaptive capacity is the ability to embrace and thrive amid change, to be nimble and proactive through periods of rapid shifts, technology advances, and other variables both natural and manmade. The constants are mission focus, values, positive behaviors, and continuous learning.

In some ways, the nonresponse world can learn much from disaster managers about adaptability. For example, at the National Preparedness Leadership Initiative, high degrees of adaptive capacity were observed in the response to superstorm Sandy in 2012 and in the aftermath of the Boston Marathon bombings in 2013. More recently, in 2017, the fluid coordination between officials and the "Cajun Navy" after Hurricane Harvey in 2017 saved lives.

However, there is still much to be done as policymakers and legislators focus on rigid rules based on prior events rather than forward-looking principles. In major disasters, the myriad agencies and organizations involved must function at a level of complexity beyond the ability to design the system – and they must do so swiftly and in synchrony. Order is more important than control.

Leaders foster order and adaptive capacity by continually asking questions that probe the system to discover what is likely to happen next: "What am I missing?" "Do we think – or do we know?" "What do you see?"

Resilience

The turbulence of VUCAST makes resilience imperative. There are frequent bumps, shocks, and jolts. Many people think of resilience as the ability to bounce back. However, every disaster leaves its mark. ARTful leaders define resilience as the ability to bounce forward. Such resilience has three equally important yet often disconnected components: psychological, organizational, and structural.

The psychological component is about one's mental state. After an adverse event, resilience is seen at the first moment people feel hope for the future. It is about cultivating the feeling, "We can do it!"

The organizational aspect involves creating some coherence amid chaos. Here, the National Incident Management System (NIMS) and other incident management systems are invaluable because they delineate structures, roles, and responsibilities for responders. There is confidence in the system.

This endorsement includes an important caveat: Attention must be paid to behaviors within the system (see "The Human Factors in Leadership Decision Making"). A robust structure alone is not sufficient.

The structural component involves the manmade components of the system such as water, food, waste, transportation, etc. Here, ARTful leaders acknowledge that critical components of response and recovery exist outside of NIMS. Community groups and self-deployed specialists involve themselves in these efforts. Leaders should work with, not against, these stakeholders with the goal of order beyond control. To foster greater resilience, make it an articulated criteria in policy development and decision making from preparation through recovery.

Trust

The third component of ARTful leadership is trust as the foundation of a values-based culture. Uncertainty (the U in VUCAST) can take a psychological toll. People naturally want to hold onto something solid. They look to their leaders to make sense of the situation, find direction, and get assurance that someone "has their backs." The team may not like every decision, but will be more accepting of them when their leaders are trustworthy and the culture values trust. ARTful leaders ask how they and their teams can be fully trustworthy partners for each stakeholder. The answers then guide both thinking and action.

Transparency, the "T" in VUCAST, looms large. Leaders and their organizations are under constant inspection. Today, the impact of every remark and each choice can spread and be amplified at blazing speed. And those impressions endure. Living and leading as a trusted individual has never been more important – or required more discipline and commitment.

The true north of an ARTful leader is clarity and coherence: of the larger purpose and the current tasks, of the enduring values that will guide the organization, and of the measures for success. With this, an organization can develop the adaptive capacity, resilience, and level of trust that serve as a powerful counter to the roiling forces of VUCAST. The opportunities will also be vast for the leaders who are smart, facile, and ARTful enough to navigate them.

Eric J. McNulty, M.A., is the director of research at the National Preparedness Initiative, a joint program of the Harvard T.H. Chan School of Public Health and the Center for Public Leadership at Harvard's Kennedy School of Government. He is also an instructor at the Harvard Chan School. He has engaged in field research in numerous crisis responses and teaches on leadership in numerous graduate and executive programs. He is a frequent speaker at conferences and other events.

The Presidency & Control of Nuclear Weapons

By Jerome H. Kahan

"The whole point of U.S. nuclear weapons control is to make sure that the president – and only the president – can use them if and whenever he decides to do so," said Alex Wellerstein, a historian of nuclear weapons at the Stevens Institute of Technology, in an article published on 1 December 2016. As presidents and circumstances change, it is important to understand presidential authority and legislation as they relate to nuclear weapons. DomPrep Welcomes Your Feedback To This Flash Poll, Preparedness and Resilience For A Nuclear Incident

On 6 August 2016, during the presidential campaign, some 50 national security officials who had served in former republican administrations signed an open letter declaring that Donald Trump has "dangerous qualities" for someone in command of the U.S. nuclear arsenal. Expressing similar concern, in late January 2017, the staff of the *Bulletin of the Atomic Scientists* moved the so-called "Doomsday Clock" forward 30 seconds to two-and-a-half minutes to midnight. A primary reason for the decision to move the clock was Trump's "disturbing comments about the use and proliferation of nuclear weapons." This change signals that the global risk of a nuclear catastrophe is greater now than it has been since 1953, when the United States and the Union of Soviet Socialist Republics (USSR) began testing hydrogen bombs.

Presidential Authority

Several key steps are required in order to launch a nuclear strike. The nuclear "Football" – resembling a large, black, leather briefcase – contains the launch codes for nuclear weapons and must remain close to the commander in chief, with his authentication codes (known as the "Biscuit"), wherever he goes. Once the president's identity is confirmed, the Football enables him to communicate with the Pentagon's National Military Command Center, which is responsible for generating Emergency Action Messages to nuclear launch control centers, nuclear submarines, reconnaissance aircraft, and battlefield commanders worldwide.

Under the War Powers Act of 1973, presidents have been given expanded power and authority to trigger a nuclear attack – even without a declaration of war or congressional authorization. The Act recognizes that, in the nuclear age, the president is not required to consult Congress before responding to an attack on the United States, or its territories, possessions, or armed forces; nor is he required to do so when considering the possibility of initiating a nuclear strike against a nuclear-armed adversary perhaps to pre-empt an imminent nuclear attack.

Restricting Nuclear Use

Senator Ed Markey (D-MA) has expressed concern that inflammatory rhetoric heightens the risk of war, "No human being should have sole authority to initiate unprovoked nuclear war." In an attempt to address this problem, the senator joined U.S. Representative Ted Lieu (D-CA) in introducing the *Restricting First Use of Nuclear Weapons Act of 2017* (S.200 and H.R. 669) on 24 January 2017. This would prevent a president from conducting a nuclear

weapons attack before determining that the enemy has first launched a nuclear strike against the United States or one if its allies.


Source: U.S. Army

Similarly, Senator Bob Corker (R-TN), chairman of the Senate Foreign Relations Committee, said in November 2017 he wants to have hearings to explore the "realities of this system" that grants a president sole authority to launch nuclear weapons, whether responding to a nuclear attack or not, with no way to revoke it. Previously, at a 30 October 2017 hearing of the Senate Foreign Relations Committee, he asked Defense Secretary James Mattis whether the president should be able to launch a first strike against another nuclear-armed country about to attack the United States without consulting Congress. Mattis stated that a pre-emptive strike ordered by the president would be essential in this case because there would be no time to get Congress into the operational loop. But other members of Congress argued that key Congressional leaders should be given a chance to advise the president in situations where he is considering the option of ordering a U.S. retaliatory nuclear strike.

John Mecklin, editor-in-chief of the *Bulletin of the Atomic Scientists*, warned in a commentary on 30 November 2017, "The Constitution does grant to Congress the power to declare war, but it is unclear whether a law that significantly constrained the president's nuclear command authority . . . would be constitutional." Moreover, legislation to change the nuclear chain of command could result in dangerous consequences, such as causing U.S. allies and adversaries to question whether the United States would be able to respond rapidly with its nuclear forces during a nuclear crisis.

The Status of Nuclear Decisions

Nearly a year after his inauguration, Trump has earned the trust of some former critics by not mishandling his nuclear launch responsibilities and not triggering an unwanted nuclear exchange. However, his behavior, actions, and statements remain unpredictable. Although this is not the best way to exercise the solid and stable leadership required to properly handle the highly classified contents hidden in the Football, Trump has admitted that "decisions are much different when you sit behind the desk in the Oval Office." It is now more important to consider the policies and procedures needed to make critical decisions like nuclear launch orders rather than focus on off-the-cuff remarks under pre-election circumstances.

DomPrep Welcomes Your Feedback To This Flash Poll, Preparedness and Resilience For A Nuclear Incident

Jerome H. Kahan is an independent analyst with over 40 years of experience in national and homeland security, having held senior positions in the State Department, including the Policy Planning Staff and Counselor at the U.S. Embassy in Turkey. He has also worked with various research organizations, including senior fellow with the Brookings Institution. He has written or contributed to books and articles, taught as an adjunct professor at Georgetown University, and been a member of the Council on Foreign Relations, and the International Institute of Strategic Studies. He has a master's degree from Columbia University in electrical engineering.

Mass Fatality Research – New York & Beyond

By Katie Joel & Terry Hastings

Low-probability, high-consequence situations, such as mass fatality events, often stress or overwhelm local response capabilities within a very short timeframe. The ability to handle these situations differs greatly depending on the size of the jurisdiction affected and its readily available resources. New York State Division of Homeland Security and Emergency Services Research conducted research to address this issue.

Mass fatalities are of great interest to New York given the ongoing threats of mass violence, as evidenced by the recent shootings in Las Vegas and Texas. In addition, research has confirmed that New York State leads the nation in the total number of mass fatality events, with more than 500 incidents to date. As evidenced by recent terrorist plots in New York City, the next mass fatality event could potentially be around the corner.

A Multifaceted Research Effort

To better understand the ways in which past mass fatality events have been handled as well as best practices that have been learned, the New York State Division of Homeland Security and Emergency Services (DHSES) undertook in 2016 a multifaceted research effort, in conjunction with the New York State Department of Health, to examine past events more closely. The research included an initial literature review, followed by analysis of after-action reports from identified critical incidents. Interviews with seven key response personnel were conducted, and a national survey of 191 responders was administered. The target audience for this research is the emergency response community, to include public safety and public health personnel. The research included qualitative interviews and quantitative data captured through a nationwide survey as part of a comprehensive research initiative.

Overall, the research led to key findings, which include the identification of eight major challenges commonly associated with the management of mass fatality events. According to the national survey, less than half (35%) of the participants had high or very high confidence in their jurisdictions' ability to handle major mass fatality events. The major challenges include the following:

- Emergency communication and information sharing
- Assistance for victims' families
- Response coordination
- Inadequate resources
- Ways to address responders' posttraumatic stress
- Inadequate training and exercises
- Victim identification (and associated cultural issues)
- Collaboration with media

Communication and information sharing gaps can easily develop due to the sheer number and diversity of individuals, as well as organizations that respond to a large-scale event. This challenge is often compounded when dealing with worst-case scenarios – such as mass fatalities – because the responders and stakeholders may not have worked together on a routine basis. Relationships are at the forefront of preparedness. When an event becomes "all hands on deck," being familiar with other response agencies and the way in which they typically operate are at the epicenter of a coordinated response. These relationships can be formed before mass deployment via training or exercises, including: full-scale drills, disaster-specific run-throughs, and tabletop exercises. Cross training and collaboration among various disciplines has been seen as an implemented best practice with the goal of integrating emergency response functions on a different level.

Although the number of victims varies for large-scale events, it is important to remember that, for each victim, there are concerned family members and loved ones they are leaving behind. The recovery process becomes just as much about helping the families of the victims to cope and receive some sort of closure as it does managing the emergency response. Family Assistance Centers and Disaster Missing Persons Call Centers can aid in this effort. It is also important for a jurisdiction to be able to manage issues such as post-disaster ceremonies and dignitary visits because they typically help bring closure to the families of the victims.

Only 35% of the participants in a national survey had high or very high confidence in their jurisdictions' ability to handle major mass fatality events.

Through the national survey, it was reported that only 27.2% of respondents believe that their jurisdictions have the resources to successfully manage a mass fatality event, and 71.3% of respondents believed that more effort and resources should be dedicated to preparing for mass fatality events. Resource gaps can exist in a multitude of areas, including limited morgue space. Relationships with funeral homes can assist in the establishment of temporary morgue space. Also, in some situations, regional or state-owned refrigerated trailers may be available for use; however, these are less common.

If the event is large enough to warrant a federal disaster declaration, Disaster Mortuary Operational Response Team (DMORT) assistance is typically provided. DMORT was formed under Emergency Support Function #8 (ESF #8) with the objective of providing victim identification and mortuary services in times of extreme need. Although it can be a great resource of help in terms of large-scale disasters, in many cases, events will not meet the threshold required to be eligible for DMORT assistance. Coroners and medical examiners take on a key diverse role following mass fatality events – one that is crucial in not only effectively and efficiently handling the aftermath, but one that also greatly affects the healing and recovery process of families of victims and the community alike.

The physical and mental health of responders cannot be ignored, both during a response as well as after. During a response, there is the potential for prolonged operational periods. Without being able to rest, responders will not be able to do the quality of work they are

capable of doing. Incident commanders and safety officers must ensure appropriate operational periods and responder downtime, but this is sometimes easier said than done. Following a major disaster, peer-to-peer support is beneficial, as it allows responders to "debrief" with others who have been in similar situations.

Media Concerns

In today's environment of social media and 24-hour news cycles, working with the media is another important consideration. Worst-case scenarios are typically accompanied by chaotic circumstances. The competition among news agencies adds to the disorder. Some media will go to drastic measures to get a "good story," including impersonating family members when calling the hospital in the hopes of learning new information, as noted during the interviews with responders. In some of the circumstances analyzed, the rush for information led the media to publish false reports and fed rumors that, in turn, caused more chaos and panic. No one can fully anticipate how the media is going to react or the moves they will make. Having a plan in place for handling the media is essential, particularly because, depending on the size, scope, and scale of the incident, both national and international media could be drawn to the event. The media should be viewed as a key partner in helping to get the message out to the public, but that partnership requires ongoing collaboration and trust.

Learning from the ways in which past large-scale incidents have been handled is crucial in understanding the best way to approach future events. In a November 2008 interview, Rahm Emanuel, then chief of staff for president-elect Barack Obama, stated, "You never want a serious crisis to go to waste." Jerome Kahan explained in an August 2017 article how this thinking allows "decision-makers to be proactive rather than reactive in their thinking" and could potentially streamline the way in which worst-case scenarios are managed in the future.

Having plans and being able to implement them in times of chaos are two very different matters. Plans are of value when they have been continually exercised and updated. Without ongoing attention, plans will not possess any operational value, particularly in the instance of mass fatality events. Although various unpredictable factors accompany an unforeseen situation, it is possible to have a framework and partnerships in place that make the handling of large-scale events considerably more manageable.

Since society is continually expanding and changing, preparedness requires repeated assessment and planning. Without continual attention, planning, and practical application, a community will not be able to keep up with changing times and technology. With threats such as terrorism, increased population demands, and other factors on the rise, the risk associated with the occurrence of a worst-case scenario is also increasing. Disasters test the preparedness of an entire community, not just its emergency functions. Preparation for events of any magnitude, let alone one of increased scale, is vital in keeping the population protected from harm.

Katie Joel (pictured above) is currently an analyst with the New York State Division of Homeland Security and Emergency Services. She has done research surrounding preparedness capabilities associated with mass fatality incidents.

Terry Hastings is currently the senior policy advisor for the New York State Division of Homeland Security and Emergency Services, and an adjunct instructor for the College of Emergency Preparedness, Homeland Security and Cybersecurity at the State University of New York at Albany.


WE STEPPED UP
SO YOU CAN
STEP BACK.
The new FLIR identiFINDER® R440 lets you scan for radiological threats from farther away to keep you and your community safe.
The new R440 is a lightweight, sourceless RIID that can be operated with one hand and is IP67-rated to survive tough missions. Not only does the 2x2 NaI detector deliver sensitive and fast detection, but it also provides accurate identification during secondary screening. The new 360° EasyFinder™ Mode expedites decision-making to keep you safe.
Learn more at flir.com/R440
FLIR identiFINDER R440
Highly Sensitive, Sourceless Handheld RIID
FLIR

Indiana's Emergency Response Guidelines for School Safety

By Robert Quinn

The 2016 Legislative Session of the Indiana General Assembly passed Senate Enrolled Act 147 requiring the Indiana Department of Homeland Security (IDHS) to establish minimum standards and approve best practices no later than 1 July 2017 for a school emergency response system. The new guidelines are helping to improve school safety and security across the state and offer a template for other states to consider when reviewing and updating their emergency response systems.

Senate Bill 147 defines the term "emergency response system" and requires the department to establish emergency response system guidelines with input from the Division of School Building Safety within the Indiana Department of Education (IDOE). Emergency response systems were given the following definition:

Systems designed to improve technology and infrastructure on school property that may be used to prevent, prepare for, respond to, and recover from a manmade or natural disaster or emergency occurring on school property.

These guidelines address an all-hazards approach to school safety, which more effectively addresses a well-rounded emergency response system.

The legislation was written in such a way that provided IDHS flexibility to develop a product that best addressed the legislative requirement. As mentioned in the definition above, it was important that the product addressed an all-hazards approach to school safety, which would more effectively address a well-rounded emergency response system. The legislation required IDHS to simply develop guidelines, rather than requirements for schools to follow. This has allowed Indiana schools to be flexible with their implementation of the guidelines.

Collaborative Effort

It was essential for state government to include external stakeholders in both the public and private sectors to ensure that the developed guidelines included the most appropriate information and was developed with input from around the state. The product working group involved nine Indiana professional associations related to public safety and

education, federal professional associations, and state government agencies that brought important perspectives into the decision-making process (all partners are listed on page 1 of the document).

This group brought together approximately 20 individuals who met four times throughout 2016 and the first half of 2017 to implement a strategy, discuss and debate product content, and ensure that a well-rounded safety and security document was developed.

The Product

The final product, titled Indiana School Safety Guidelines for Emergency Response Systems, identified 17 school emergency response components as decided by the project working group. The components address the necessary pieces of an emergency response system that are encouraged to be included in every school. The guidelines focus on the following recommendations:

©iStock.com/csfotoimages

- Access Control & Visitor Management
- Training & Exercise Opportunities
- Planning, Procedure, and Policy
- Facility Safety Leadership and Direction
- Importance of Building Relationships with and Involving Local First Responders

These five topics are expanded upon within each of the 17 components.

One of the consistent themes of the product is "people over products." The group acknowledges the importance of physical tools for safety and security (e.g., doors, locks, windows), but without training these tools are less effective. Putting the focus on the people involved in school safety emphasizes building relationships with first responders, preparing uncommon stakeholders (e.g., facilities staff, parents, bus staff) for emergency situations, and identifying methods of utilizing the large student population as a trained safety and security mitigation tool.

On 1 July 2017, the project working group successfully developed a product that has been disseminated around Indiana. To share this information, professional associations, local emergency management agencies, and IDOE were utilized, and a copy was posted for the public on the IDHS website.

Moving Forward

The legislation not only required IDHS to develop guidelines, but also maintain them. No specific maintenance schedule was provided, but IDHS determined that an annual review of the product was appropriate and would disseminate an updated product on 1 July 2018.

With the 2017 product released, it is important that IDHS request feedback from individuals who work in and around schools on a daily basis. To do that, the IDHS needed to get into the communities and talk with its partners. This socialization initiative is helping to gain statewide agreement and support for the included content, to guide content, and to direct the future of this product.

IDHS identified County School Safety Committee Meetings, held in each Indiana County, as the best method for receiving product feedback. Meetings occur at the discretion of the committee, some on a monthly basis, whereas others occur once per year. County commission meetings bring together representatives from the schools, first responders, local government, state government, and relevant private industry.

Through the end of 2017 and into early 2018, IDHS intends to attend county commission meetings around the state to elicit input. Through December 2017, IDHS has already attended 10 county meetings in various parts of the state. The important feedback received has seen information added to the National Incident Management Systems trainings that is specific to school employees and addresses the importance of providing safety training to part-time or contract staff.

The project working group will continue to play a critical role in the development and revision of this document. The working group will review any information included in this document to maintain transparency and collaborative input.

Robert Quinn currently serves as the Indiana State continuity director for the Indiana Department of Homeland Security. In this position, he leads the IDHS school safety projects. Working with school safety specialists from around the state, he has been able to facilitate the coordinated efforts to create school safety guidelines assigned by the Indiana Senate Bill 147 (2016). He has been involved in addressing school safety topics such as architectural design and renovation of schools within Indiana, providing additional hazmat and radiological awareness information, improving both higher education and K-12 event management preparation, and assisting in the development and implementation of a statewide higher education/emergency management consortium.

Maryland's Approach for Raising the Resilience Index

By Charissa Cooper & Jessica Nusbaum

Threats, whether natural or manmade, have the ability to negatively impact communities. Although government agencies serve communities before, during, and after disasters, emergency management officials understand the realities of gaps that exist in disaster management systems exclusively managed by government. There is a mounting cognizance of the need for effective communication and coordination from a broad range of stakeholders to reduce the negative effects of a given disaster.

Emergency management officials recognize the importance of diversity in disaster management. Often, the unsung heroes of disaster response and recovery are the voluntary organizations in the community. They frequently begin their work alongside the first responders and are the last ones out after the long process of recovery has been completed. In addition, engagement between the private and public sectors is a component of increasing community resilience. This is not simply a matter of the private sector retaining the capabilities to support communities, but also the ability of government agencies to provide support to businesses. When surveyed, partners in Maryland's Private Sector Integration Program often highlight the need to receive timely and vetted information from their government partners. It is important to emphasize that partnerships between the public, private, and voluntary sectors can help to elevate a community's resilience index.

Getting the Team Together

A whole community approach to disaster management requires an investment from public, private, and voluntary organizations. The utility of this investment allows for a collective response because no one organization can fully address all the complexities of disaster management. Emergency exercises present the opportunity to practice coordination between stakeholders ahead of an event. On 16 November 2017, the Maryland Emergency Management Agency (MEMA) convened over 100 representatives from various levels of government, the private sector, and voluntary organizations to share the challenges, lessons learned, and best practices from disaster events. Although not akin to the traditional structure of an emergency exercise, the theme of that one-day summit, "Piecing It Together: Building Resilience Through Partnerships," was birthed out of the concept that each organizational component has a "piece" or role in emergency management.

The challenge in bringing together a broad range of stakeholders is building group consensus. In an effort to develop sessions that identified and removed potential roadblocks to gaining buy-in, a pre-event survey was developed. The survey, sent to the private and voluntary sectors, allowed participants to provide feedback on logistical aspects such as location and topic areas, and gave them an opportunity to become members of the planning team. The survey results highlighted the need to address lessons learned from recent incidents. An interdisciplinary planning team with representation from state, local, private,

and voluntary organizations converged to guide the development of the overall summit. The depth of subject matter expertise on the planning team allowed for the following targeted goals to be developed:

- Determine the best way to maintain partnerships between the public, private, and voluntary sectors;
- Determine if current plans and protocols sufficiently support resumption of operations and continuity following disaster situations;
- Examine key issues, challenges, and resolutions that exist in response to managing interruptions to business operations, such as complex coordinated terrorist attacks, civil unrest, and other no-notice disaster events;
- Examine the effectiveness of maintaining the flow of critical information among and between the public, private, and voluntary sectors;
- Identify strengths, gaps, and areas for improvement in regard to information sharing networks before, during, and after no-notice disaster situations; and
- Identify ways to improve coordination among and between the public, private, and voluntary sectors before, during, and after disaster situations.

Collaborative Conversations

The summit captured the essence of the interdependencies that exist in the disaster management process. Throughout the day, the summit showcased initiatives being developed and occurring regionally and nationally – including work being done by the National Voluntary Organizations Active in Disaster (NVOAD), Region 3 of the Federal Emergency Management Agency (FEMA), and the West Virginia Voluntary Organizations Active in Disaster (WVVOAD). Jenny Gannaway, executive director of WVVOAD, and Lorra Michelle Breeland, the voluntary agency liaison for FEMA Region 3, presented on the work that is being done in West Virginia to assist residents who lost private access bridges to their homes as a result of flooding events in 2015, 2016, and 2017. To date, 44 bridges have been repaired or replaced and over 100 are on a list for future work. The WVVOAD member organizations continue to help drive the project forward through various avenues, including fundraising and labor.

Partnerships between government, private sector, and voluntary organizations can help to elevate a community's resilience index.

Greg Forrester, president and chief executive officer of NVOAD, explained that a challenge encountered by the voluntary sector during the 2017 response to Hurricane Maria in Puerto Rico was determining how to provide wrap-around services to individuals and families relocating from Puerto Rico to the U.S. mainland. Issues including sheltering, feeding, schooling, and translation services needed to be taken into consideration for these evacuees, and the communities turned to nonprofit and voluntary agencies to fill the gaps that existed. The impact of the stories and lessons learned will hopefully strengthen recovery and response by the voluntary community in Maryland.

Throughout the summit, conversations with the private sector explored avenues for risk reduction and addressed the challenges businesses experience while managing disaster situations. The opportunity to share best practices across disciplines and sectors created an atmosphere for organizations to examine and identify ways to improve their preparedness efforts. These connections afforded the unique opportunity for pre-event collaboration and communication between the public and private sectors. The return on investment is seeded in an integrated network of two-way information exchange with the aptitude to influence operational decisions.

Outcome & Recommendations

Although the task of building partnerships may be arduous, the true feat is sustaining them. Recognizing that the effort of all sectors is required to create resilient, prepared communities is a starting point for this process. The synergy generated at this summit is a part of the linkage needed to support the relationship between governmental and nongovernmental organizations. At the end of the summit, participants were encouraged to consider the next steps. This includes keeping the connections established and continuing the conversations. The result, based on the results of the participant feedback, is that events like this are valuable. Over 90% of participants who responded to the post-event survey conveyed they were pleased with the overall event. In addition, participants found the opportunities to network with others among the leading outcomes of the event. This network can be translated into the mobilization of preparedness, response, and recovery actions throughout Maryland.

Attendees left with a greater idea of the capabilities that exist throughout the state and contacts for various types of emergency events. As each sector works to solve the problems sustained by disaster situations it is helpful to know that a support network of expertise with a communal goal of increasing resilience exists. The challenge still exists in identifying which, if any, participants are missing from these dialogues and the work needed to engage them. Raising the resilience index requires all community members to recognize their roles in preparing for, responding to, and recovering from disaster situations.

Charissa Cooper (pictured above) is currently the private sector liaison and a National Capital Region planner for the Maryland Emergency Management Agency. In this role, she manages the Private Sector Integration Program and performs outreach to the business community in Maryland. Prior to this position, she led efforts regarding plan development for Ebola virus disease and other emerging infectious diseases at the Georgia Department of Public Health. She has experience developing and maintaining emergency response and all-hazard preparedness plans at the federal, state, and local level. She received her Masters of Public Health specializing in Environmental and Occupational Health from Florida International University.

Jessica Nusbaum is the Maryland State individual assistance officer and community preparedness coordinator with the Maryland Emergency Management Agency (MEMA). She works closely with voluntary agencies and other community partners, using an all-hazards approach to preparedness, to ensure that the citizens of Maryland are ready when disaster strikes. Prior to starting her career in emergency management, she spent 13 years working in the nonprofit sector, providing various case management services to individuals and households with barriers such as mental illness, homelessness, and substance abuse. She holds a bachelor's degree in business from Mount Saint Mary's University.

10 Questions for Selecting Business Continuity Software

By Erin Valentine

Being resilient when faced with an emergency or catastrophic event requires preplanning to ensure that operations can continue with minimal interruption throughout the event or restart soon after the event. Business continuity software can help bridge the continuity gap during these times. Answering these 10 questions before purchasing will help ensure a good match between the software and the user.

Choosing a business continuity software tool can be like choosing a new car. There is an overwhelming abundance of possibilities available in every model, size, and price range. The buyer narrows down the selection by asking themselves questions about functionality, capacity, affordability, and maintenance costs. An organization in the market for a business continuity software package should begin by asking themselves the same type of questions.

Question 1: Does This Organization Really Need Business Continuity Software?

Before shopping for a car, for example, buyers should consider whether they actually need a car at all. Maybe they could get by with a bicycle. Business continuity software is essentially the same at the core: a database capable of aggregating data and producing reports. User must then determine other criteria, for example: whether they need the system to do more than simply store information; and whether they have few enough plans that they can update and maintain the documents manually. If so, a database management system merged with a word processor may suffice.

Business continuity management can present a huge administrative burden. However, business continuity software allows the operator to input data once and have it cascade across multiple plans and reports. One alternative to expensive software is the Department of Homeland Security's (DHS) Ready.gov website, which offers a free Business Continuity Planning Suite with a training module, automated plan generators, and a self-directed exercise for testing the completed plans.

Question 2: What Does the Organization Need the Software to Do?

In the car scenario, the buyer considers the intended uses – for example, just to go back and forth to work every day, or to haul a trailer. If the user needs business continuity software to perform more complex functions, it helps to identify those needs before purchasing a product. Some features and functions to consider include, but are not limited to: Business Impact Analysis (BIA) tools; risk assessments; incident management capabilities; emergency notifications; tests and exercises; and mobile device applications. Some systems allow users to

choose these options individually. The most important factor is that the user interface is simple and easy to use.


©iStock.com/TECHDESIGNWORK

An integrated BIA tool can be particularly valuable in determining critical business functions and recovery times, as well as identifying assets and dependencies. The findings can then be integrated into business continuity plans. Many programs offer an incident management tool that can turn response and recovery plans into systematic actionable tasks with timed reminders and an event log. However, be sure the program can accept and store supporting files such as PDFs or Word documents.

Question 3: How Much Can the Organization Afford?

Pricing for business continuity software varies greatly depending on factors such as integrated capabilities, number of users, level of technical support, and hosting options. At some point, car buyers have to determine whether they can afford an initial deposit and monthly payments. Similarly, an organization considering business continuity software should prepare for an up-front implementation fee and annual licensing fees, in addition to potential charges for user training and technological support. Many programs base costs on the number of users. As the organization grows, the software needs to grow with it, which often requires additional user licenses.

Question 4: Who Hosts the Software and How Safe Is the Data?

The car shopper may consider vehicle security: street or garage parking at night; garage locks and security; and car alarm systems. Most business continuity software offered today is hosted in a cloud-based environment, but there are a few self-hosted solutions. For those interested in Software as a Service (SaaS), make sure to look into the security of the hosting data center. Federal government organizations require offsite data centers be certified by the Federal Risk and Authorization Management Program (FedRAMP). If the organization collects personally identifiable information as part of the business continuity cycle, that data should not only be encrypted, but also backed up regularly and quickly recoverable.

Question 5: Will the New Software Integrate With Current Software?

For a car, this may include determining whether a bike rack from the old car will fit onto the new one. For business continuity, whether the existing technology works with the new

technology may be a concern. Some business continuity software is designed to integrate with third-party applications, such as human resources databases. This type of functionality saves a great deal of time, especially when personal contact information has to be updated across multiple databases and plans.

Other business continuity software is designed to integrate with emergency notification services like Everbridge. The user can activate the notification feature using personnel contact information inside the business continuity software. Other useful features include integration with existing Geographic Information Systems (GIS) and Active Directory services.

Question 6: How Easily Can the Software Be Implemented?

How the organization has been managing its business continuity to date, how is has been storing its data, and how it has structured its plans help answer this question. The organization should make sure that existing data could easily be imported. Most business continuity software allows for the upload of spreadsheets. When it comes to formatting plans, however, most software is less flexible. If the organization currently creates plans in a word processing program, the new software may not be able to recreate that format exactly. In car terminology, the person buying a new car should not expect the gas tank to be on the same side of the car as the old one.

Like buying a car, many questions need to be asked before purchasing business continuity software. These 10 questions can help with the process.

Other issues may arise for organizations whose business continuity programs are less mature. In the past, the business continuity coordinator may have been doing all the heavy lifting. Once a software program is implemented, individual plan owners may be asked to complete an online BIA or input plan data themselves. If the organization's business continuity program is not fully mature, it may be difficult for employees to understand and adapt to the demands of the software.

Question 7: How Should the Software's Output Look?

Car buyers have an idea of what they want the new car to look like – for example, sleek and shiny, or tough and functional. Similarly, business continuity applications produce output differently. Some software create plans as Word documents, but most produce PDF documents, making them more difficult for plan owners to add comments or changes. Many software packages offer custom reports, although some are easier to create than others. Some reports are as easy as drag-and-drop; others require the user to master programs like Crystal Reports. Some software does not allow the user to create custom reports at all; instead, the user must ask the software provider to create the reports for them.

Warning: if the organization depends on call trees for employee notification, make sure the new software will support them – many vendors consider call trees outdated and no longer offer this feature.

Question 8: What Training Will Users Need?

Moving a business continuity program from a word processing document and a spreadsheet to a fully integrated software program can be like going from an automatic to a manual transmission: all of the sudden, there are multiple moving parts and the driver needs to learn coordination to avoid stalling. New software can present a steep learning curve. Not only is there the challenge of learning to operate the programs, there is also the challenge of teaching plan owners to assess and prioritize their business functions. If individual plan owners are responsible for conducting their own BIAs, a significant amount of training may be required. Software owners can either conduct the training themselves, or pay the vendors to do so.

Question 9: How Much Technological Support Will Be Required?

While a car buyer determines the value in purchasing a roadside assistance plan, the business continuity professional determines how much technological support users of the business continuity software will require, as well as when and how the support will be provided. Business continuity software varies in terms of technological support, so several needs must be assessed: time (24/7 support or only during business hours); availability (business's hours compared to vendor's hours); accessibility (live support or online portal); and cost.

Question 10: Where Is the Best Place to Start?

Just like car dealerships, there are a multitude of software vendors. The findings of an independent research organization, such as the Gartner Magic Quadrant for Business Continuity Management Program Solutions are a good place to start. Recommendations from peers and professional organizations are also valuable. Vendors will gladly demonstrate their software via webinar; and some even offer a free trial period.

As with any purchase, thorough research and comparison are key. Keep in mind, though, that the organization may be using this software for years to come. It is important to choose a package that is best for the business right now as well as flexible enough to grow along with it.

Erin Valentine, CBCP, MBCI, is the business continuity/disaster recovery coordinator at General Dynamics Information Technology (GDIT). She spent the first decade of her career as an exercise and training administrator at the Maryland Emergency Management Agency (MEMA). Prior to GDIT, she supported the Social Security Administration's Office of Security and Emergency Preparedness as a disaster preparedness specialist. She holds a bachelor's degree from Towson University and is certified by FEMA as a Master Exercise Practitioner and Professional Continuity Practitioner. She is a Certified Business Continuity Professional (CBCP) and a Member of the Business Continuity Institute (MBCI). She currently serves as the program director of the Central Maryland Chapter of the Association of Continuity Professionals.

Excess Equipment Sales & Potential National Security Threats

By James M. Rush

Recent terror attacks have demonstrated that the modus operandi for terrorists to attack innocent people is to use whatever tools can easily be obtained. Some agencies and companies may inadvertently sell or donate the very equipment terrorists may use to kill people and endanger national security. This proposal offers a barrier to terrorists wishing to exploit the healthcare, public health, chemical, and pharmaceutical industries in the area of excess equipment.

A possible threat to national security involves the normal sales or donations of excess or outdated medical, laboratory, or research equipment in both the private and public sectors. These sales and donations may constitute a source of supply for terrorists or their suppliers to build improvised weapons of mass destruction in the United States or overseas. Items such as incubators, X-ray radiation sources, mixer-investors, centrifuges, and other pharmaceutical, hospital, or public health laboratory equipment could equip terrorists with tools to inflict harm.

Biomedical Equipment (Medical, Pharmacy, Laboratory & Imaging) Excess Equipment Programs

The Armed Services dispose of excess equipment through the Defense Logistics Agency (DLA) Disposition Services. The DLA Disposition Services typically attempts to redistribute excess materials to Defense Department organizations, as well as to state and local government organizations and certain nongovernmental organizations with requirements for excess property. When equipment exceeds DLA's needs, the DLA Disposition Services conducts "public sales" to organizations wishing to bid on "lots" of equipment – for example, a "lot" may consist of a pallet of computers. The specific screening or vetting process currently being conducted on persons or organizations placing bids on government property is unclear.

The private sector also must manage its excess medical equipment. Most civilian hospitals utilize medical equipment such as X-ray and laboratory equipment as financial assets on financial management records. This means that, once a piece of equipment has been fully amortized, it loses much of its identity and tracking by hospital management officials. As new equipment is purchased, plant engineers or purchasing personnel often sell the equipment being replaced with little or no scrutiny of which organizations are purchasing the equipment. In many cases, resellers purporting to be Third World relief organizations or religious/charity organizations procure excess equipment for a small fraction of the original acquisition cost. Persons or organizations with nefarious intentions could easily disguise themselves.

Recommended Solutions

To mitigate potential threats, the government should establish a government property pre-sales vetting system, under the management of the Federal Bureau of Investigation (FBI) counterterrorism function.

Government-owned equipment – All federal and other agencies that are required to submit excess equipment to the DLA Disposition Services would continue submitting the actual excess equipment and required turn-in documentation to their local DLA Disposition

Services field office. Prior to sale or donation of any government-owned equipment to a private entity, the DLA would submit the potential buyer to the FBI government property pre-sales vetting system. Once the FBI sends an approval document, the sale would proceed as normal.

It is important to note some governmental agencies or jurisdictions may not be required to dispose of excess medical equipment through DLA Disposition Services. One solution to close this gap would be for these agencies or jurisdictions to voluntarily submit excess medical equipment and potential buyers through the private sector screening process listed below.

Private sector excess equipment, voluntary participation – Before selling or donating excess equipment to external entities, nongovernmental organizations and state and local entities including universities, research laboratories, state reference laboratories, etc., would voluntarily electronically submit the name of any entity wishing to purchase excess equipment to the FBI for vetting before selling or donating the equipment. The vetting request would also include the equipment description/nomenclature, model number, and manufacturer of any biomedical equipment requiring screening prior to sale to the community or gifting to humanitarian groups or other nongovernmental organizations.

Similarly, manufacturers of chemical, radiological, biological, and pharmaceutical equipment may already have programs similar to this already in place. If not, these entities could voluntarily participate in the FBI pre-sale screening process. Examples of potential equipment requiring pre-sales FBI screening may include:

- Portable and installed X-ray or CT-scan apparatus/equipment and any equipment containing a radiological source deemed traceable (subject to a determination of source strength to be tracked by radiological specialists or health physicists);
- Laboratory diagnostic and biological classification equipment including incubators, centrifuges, dryers, and mixer/investors;
- Pharmaceutical/chemical manufacturing and automated mixing equipment;
- Biomedical equipment repair, diagnostic, and calibration equipment; and

Other equipment determined by U.S. federal agencies, including Department of Homeland Security, Department of Health and Human Services, FBI, Drug Enforcement Administration, Food and Drug Administration, Occupational Safety and Health Administration, and National Institute for Occupational Safety and Health.

The United States is in a generational struggle against terrorists who wish to disrupt and destroy the current way of life. Terrorists have shown an ability to think out-of-the box by using airplanes, pressure cookers, automobiles, trucks, and other everyday objects as instruments of destruction. Even more creativity is needed to stay a couple steps ahead of adversaries. The idea put forth in this paper serves as a reminder to always look for ways to close gaps and defeat threats before they can become attacks.

James M. Rush has over 36 years of healthcare administration and community emergency-management experience in the U.S. armed forces, the U.S. public-health community, and the nation's civilian healthcare industry. He recently served as the Region III project officer for the National Bioterrorism Hospital Preparedness Program, which is dedicated to assisting healthcare organizations prepare for "all hazards" events and incidents. He is author of, among other published works, the "Disaster Preparedness Manual for Healthcare Materials Management Professionals."

Our commitment to BioDefense

has allowed us to be ready

for the Ebola outbreak

in West Africa.

Now, with the FilmArray system

and our reliable BioThreat Panel,

we are able to test for 16

of the worlds deadly

biothreat pathogens

all in an hour.

Now That's Innovation!

BIOFIRE®

DEFENSE

Learn more at www.BioFireDefense.com