Fall 2010

Explosives recognition and awareness training: a psychological approach to pre-blast mitigation

James Wade Hawkins

EXPLOSIVES RECOGNITION AND AWARENESS TRAINING:

A PSYCHOLOGICAL APPROACH

TO PRE-BLAST MITIGATION

by

JAMES WADE HAWKINS

A THESIS

Presented to the Faculty of the Graduate School of the

MISSOURI UNIVERSITY OF SCIENCE AND TECHNOLOGY

In Partial Fulfillment of the Requirements for the Degree

MASTER OF SCIENCE IN EXPLOSIVES ENGINEERING

2010

Approved by

Dr. Jason Baird, Advisor
Dr. Paul Worsey
Dr. Francis Montgomery

ABSTRACT

The nation's security strategy tends to be reactionary to a specific event. It is rare when established policies have proven successful, even though there is substantial financial and resource investment. The payoff is measured by analyzing the desired minimal effect rather than prevention of the event altogether. Such is the case in combating explosives-related threats.

Today, research and development, science and technology, are plugged as the saviors of a post-blast event. Synthetic and composite materials are used to strengthen barriers and cutting-edge technology is utilized to refine the latest in standoff detection. These legitimate measures provide a sense of security for those who are "protected." By establishing acceptance that the blast will occur, a facility's infrastructure and occupants fall into a specific category where minimizing is the accepted goal, rather than blast prevention being the ultimate objective. Although massive walls can act as a deterrent to terrorist attacks, evil doers are capable of breaching those barriers both from the exterior and interior. Therefore, a more logical goal of preventing the blast must be emplaced.

Like safety, where the aim is to prevent injury, explosives training must be implemented to enhance a site's capabilities to deter possible attacks. This paper investigates the current practices in explosives recognition and awareness (ERA) training, the availability of such training to pertinent security personnel and first responders, the tactics utilized to mitigate explosives events and develops a comprehensive psychological training mechanism, site awareness of firing and explosives devices (SAFE-D), on which both the private and public sector can build an authentic explosives site security plan.

ACKNOWLEDGMENTS

This composition is a result of much needed assistance throughout an extensive academic career. First, if not for Arlene Chafe, with the International Society of Explosives Engineers (ISEE), pursuing an explosives degree would have never come to fruition. Also, this author is grateful to the instructors, staff and professors in Missouri S&T's Mining Department for their patience and instilling an atmosphere of making things happen. Thanks to Missouri S&T as well for writing the checks during this research and to all the students who helped with projects.

Coming into the program, there was some skepticism as to the extensiveness of the advanced explosives training offered in Rolla. Thanks to the diligence, and sometimes maniacal work of Dr. Paul Worsey, explosives education at Missouri S&T has become a global standard. Across academia, Paul's efforts will be duplicated and mimicked, however; it is his vision, persistence and ability to push other's buttons that will remain truly inimitable. Special gratitude must be extended to the rest of the committee. Thanks to Dr. Francis "Dee" Montgomery, for her patience and enthusiasm in participating in this explosives adventure. Dee's expertise has guided this research on a unique level typically uncharted for many engineers.

Throughout one's career, there are few advisors, counselors, associates, friends and teachers that can genuinely be drawn upon. However, at Missouri S&T there exists the refreshing common sense of Dr. Jason Baird. A fellow serviceman, Jason has afforded countless opportunities for students to think for themselves and delve into legitimate research without the militaristic intimidation. He is a great friend and mentor and provides a realistic learning environment for those armed with little more than reason and logic. Thanks Jason for all your guidance.

Lastly, I must thank my best friend, the mother of our wonderful children and my wife, Amy. Without complaint, Amy has encouraged and supported me throughout my ridiculously lengthy college career. She has dealt with a deployment, relocations and many long nights studying. She has done so graciously, and while pursuing her own degree and career. Amy, there has never been a better battle buddy than you.

TABLE OF CONTENTS

LIST OF ILLUSTRATIONS

Page

LIST OF TABLES

Page

ACRONYMS

AAR	After Action Review
ALERT	Awareness and localization of Explosives-Related Threats
ANFO	Ammonium Nitrate/Fuel Oil
ATF	Bureau of Alcohol, Tobacco, Firearms and Explosives
BATS	Bomb Arson Tracking System
CES	Certified Explosives Specialist
CFATS	Chemical Facility Anti-Terrorism Standards
CIED	Counter Improvised Explosive Device
CIKR	Critical Infrastructure and Key Resources
COE	Center of Excellence
CRM	Composite Risk Management
CSETAT	Chemical Sector Explosive Threat Awareness Training
DHS	Department of Homeland Security
DOJ	Department of Justice
ERA	Explosive Recognition and Awareness
EU	Explosives Unit
FBI	Federal Bureau of Investigation
FLW	Fort Leonard Wood
FM	Field Manual (U.S. Army)
GSA	General Services Administration
HR	Human Resources
HSC	Homeland Security Council
HSPD	Homeland Security Presidential Directive
ICMI	International Cyanide Management Institute
IED	Improvised Explosive Device
IME	Institute of Makers of Explosives
IP	Office of Infrastructure Protection
ISEE	International Society of Explosives Engineers
ISO	International Organization for Standardization

IST	Infrastructure Survey Tool
JTTF	Joint Terrorism Task Force
LERP	Local Emergency Response Plan
MJIEDSP	Multi-Jurisdictional IED Site Plan
NCTC	National Counterterrorism Center
NIPP	National Infrastructure Protection Plan
OIG	Office of the Inspector General
OPD	Officer Professional Development
PMI	Protective Measure Index
PSA	Protective Security Advisor
RBPM	Risk-Based Performance Measure
RICC	Research and Industrial Collaboration Conference
SAFE-D	Site Awareness of Firing and Explosives Devices
S&T	Science and Technology
SAV	Site Assistance Visit
SEA	Safe Explosives Act
SEMA	State Emergency Management Agency
SOP(s)	Standard Operating Procedure(s)
SSC	Sector Security Council
SWAT	Special Weapons and Tactics
TSA	Transportation Security Administration
TTPs	Tactics, Techniques, and Procedures
USAES	United States Army Engineer School
VBIED	Vehicle-Borne IED

1. INTRODUCTION

During the past decade, billions of American dollars have been spent to combat explosives-related threats. The focus of this investment has been, and continues to be, the funding for better explosives detection technologies and improved barrier systems. Just in 2010 alone an abundance of the nation's treasure has gone to fund extraordinary sensor technology in hopes of easing citizens' safety concerns. These investments include $215 million allocated for the 2011 budget for the purchase of body scanners to be utilized at airports. This initiative was sparked by the alleged high-explosive detonation attempt by Umar Farouk Abdulmutallab aboard an aircraft on Christmas 2009 in which some officials believe the X-ray device would have revealed the explosive (HSNW, 2010). Interestingly, this funding is earmarked despite privacy concerns that may eventually reach the United State Supreme Court. The attempt was foiled by courageous passengers and poor execution on Abdulmutallab's part.

Other recent funding includes over $1 billion for explosives detection systems allocated from the Transportation Security Administration's (TSA) share of the 2009 American Recovery and Reinvestment Act and a 2010 budget of over an additional $1.5 billion for purchase and installation of explosive detection systems (HSNW, 2010). These are substantial investments for equipment that may give false positives or negatives or simply may not work at all, especially at safe standoff distances. Further, there may be legitimate concerns other than privacy and cost. Some technologies may use radiation, may be incompatible with existing screening techniques or may be limited as to what type of explosive or explosive residue it can detect. Therefore, it is essential that site security professionals, facility managers and owners and operators consider low-cost, effective approaches to raise explosives-related threat awareness, and equip their employees with the knowledge of how to recognize those threats. It is the goal of this research to investigate current practices of human perception and to develop a foundational training program on which companies can build a practical and testable site security plan that addresses explosives-related threats and aids to alleviate complacency.

1.1. PROBLEM STATEMENT

The concentration on bulk and trace detection sensors and systems at standoff is a legitimate research venture for mitigating the risk of an explosives event, as is the manufacturing of superb barrier systems. Like detection systems, many companies, and vast amounts of financial support, are directed to the development, testing and improvement of blast resistant barriers. Schools such as Missouri University of Science and Technology (Missouri S&T), an engineering university located in Rolla, Missouri, continue to create and test astonishing blast resistant materials. Again, millions of dollars are invested to perfect the physical protection against substantial improvised explosives devices (IEDs).

Alternatively, a mindset accepting of the premise that explosives events will occur must also be subjected to scrutiny. Neither this author, nor any reasonable person, will logically argue that all events, such as crime, can be prevented. However, the ultimate goal must be just that. This same philosophy applies to any safety program. For occupational safety purposes an employer encourages a zero-accident policy although the occasional smashed finger will occur. The realistic and achievable end state must be that of risk acceptance and mitigation as discussed in Section 3. But facility managers must set their aim to the pinnacle of safety and not toward the inevitability of the event. They must act in the interest of protecting their employees, contractors, visitors and infrastructure and continue to implement economically viable and practiced procedures to ensure site safety. The federal government's explosives-related threat focus, albeit noble, should not be the sole protection on which a company relies. Although federal agencies have enjoyed many successes stopping potential terrorist attacks, they have received their share of criticism as well. Considering that the United States alone uses billions of pounds of explosives annually, and in some cases, as discussed in Section 2, those explosives are accessible to egregious employees, facility managers must develop a hybrid approach to mitigate the threat. This concentration should not only involve the best available proven technology, but also a component of explosives education and training. Throughout this composition, clear parallels will liken ongoing procedures in varying industrial practices to the creation of SAFE-D.

Certainly, the focus of this composition is not to discourage the continued development of bulk and trace detection sensors and systems and blast resistant barriers, but rather the aim is to investigate the lack of genuine psychological explosives-related threat training for security forces, first responders, employees, researchers and contractors. The initial focus for site security, especially at structures like hospitals and schools, must address the attitude and behavior of those charged with protecting others and establishing a climate in which explosives and explosives components can be recognized, an explosives event can be avoided and those assigned with site security are continuously alert to the explosives-related threat.

1.2. INFORMATION SHARING

In order to properly address the pertinence of explosives-related threat training to a facility, there first must be an investigation into the current state of information gathering and sharing. Explosives recognition and awareness (ERA) training, specifically being able to identify basic components of explosives material and possible detonators, as well as understanding the common characteristics of high explosives and the result of a significant blast, must address typical concerns of site managers. The training must:

- Establish a common explosives vocabulary
- Be continuously improved and tested
- Address site specifics and professional roles
- Cover the risk management process
- Create a basic knowledge of explosives components
- Be available and cost effective to obtain
- Be incentive-based rather than punitive
- Receive participant feedback regarding attitude and behavior.

These criteria are analyzed further in this work.

Historically, training that targets ERA both in the public and private domains has been protected, expensive or non-existent. Despite the concentration for development of explosives detection, especially since the September 11th attacks on the United States, sharing information regarding explosives and explosives-related threats has been a contested issue. As discussed in Section 2.2, even federal agencies tasked with such

training tend to draw fire for jurisdictional issues and poor tactics and implementation of policy when working with other entities. What's more, the attacks in 2001, and not so much the 1993 bombing of the World Trade Center and 1995 Oklahoma City attack have created an international stigma regarding explosives. Drastic and immediate measures such as the Safe Explosives Act (SEA) of 2002 were common results of 9-11 and the push for better explosives detection technology has been reinforced publically by the 2001 and 2009 attempted attacks by shoe bomber Richard Reid and the aforementioned Abdulmutallab, respectively. While the attack on the A.P. Murrah Federal Building in Oklahoma City didn't seem to spawn sudden panic regarding explosives detection, it did change the way in which the federal government evaluated its own vulnerabilities.

Within two months of the Oklahoma City attack, the Department of Justice (DOJ), along with several other federal agencies, released its "Vulnerability Assessment of Federal Facilities." The report was the initial effort to be undertaken by the General Services Administration (GSA) to outline physical security measures and construction regulations of government structures. While its primary focus was that of physical security, it did spawn several subsequent standards that strengthened total security measures. The DOJ report also created an awareness that security training must be taken into consideration as well, although explosives-related training was not specifically offered as a performance-based measure. In his paper, "Anti-Terrorism: Criteria, Tools & Technology," Joseph Smith of Applied Research Associates, Inc. points out that "it is important to remember that security protection issues must be examined as a whole" (Smith, 2003). Smith also acknowledges that "The best defense against death and injury from bombing attacks is to prevent the attack from occurring (Smith, 2003)."

Understandably, preventing every attack should be the goal, but as history has shown, it may not be possible. Nonetheless, making the training and information sharing a priority can significantly reduce the risk of an attack.

As explosives threats continue to be classified as terrorism and occasional acts of war employed by states, it is prudent to mention that numerous terroristic activities are simply criminal acts committed by the unlawful. Even during combat operations in Iraq and Afghanistan troops find themselves policing up the undesirables of the population. Notably, within this population there is an abundance of lawlessness as well as available

explosives material to carry out attacks. Therefore, it is crucial that both public, specifically law enforcement, and private sectors meld together not only the training needed to mitigate the risk of explosives-related threats, but also the intelligence required to direct the effort toward pre-blast mitigation rather than post-blast response. Many professionals, both in academia and industry, insist that this approach in enabling response and security officials with knowledge will pay dividends in stopping attacks altogether. Kathleen Kiernan, who participated in a committee workshop sponsored by the National Research Council, shares this perspective. Kiernan points out by stating that more involvement in information sharing can lead to a definition of what right looks like. It's this philosophy, also exhibited by the military and law enforcement, which could give those responsible for site security the necessary gut instincts which "would be helpful in detecting IED-related anomalies (National Research Council, 2008)."

John Groves, a retired Army Lieutenant Colonel and professor at Drury University at Fort Leonard Wood, Missouri, agrees with Kiernan's assessment. Groves, which has over 40 years of law enforcement experience, states that one of the most significant flaws in addressing such threats is a lack of information sharing between competing agencies (Groves, 2010). The nation's own Department of Homeland Security (DHS) has specifically addressed this need in its 2010 budget; allocating $260 million of its $42.7 billion to "fortify our intelligence system by improving information sharing and analysis by potentially adding thousands more state and local level intelligence analysts" (U.S. Government (OMB), 2010).

The philosophy and the investment coincides with the federal government's intent on providing a more solid information framework in which all pertinent entities can establish an intelligence and training dialogue for the good of preventing an explosives attack. The Homeland Security Act of 2002 created a federal mandate for agencies to share certain information (U.S. Department of Justice, Office of the Inspector General, Audit Division, 2009). Subsequent efforts would further hone that concentration toward explosives. In 2007, Homeland Security Presidential Directive 19 (HSPD 19) outlined the national policy "to counter the threat of explosive attacks aggressively by coordinating Federal, State, local, territorial, and tribal government efforts and collaborating with the owners and operators of critical infrastructure and key resources to deter, prevent, detect,

protect against, and respond to explosive attacks" (Department of Homeland Security, 2009). Sectors involved with operating critical infrastructure and key resources (CIKR) have developed a unique response to this collaboration under this and other directives, which is discussed in Section 2.1.

Although this is the obvious position of the United States, it seems that the implementation of the directive along with the availability of realistic and effective explosives training is much more complicated. However, there has been some movement on the directive which is revisited in Section 2.1. Still, the horror exists that the nation will suffer once again an unimaginable attack, with the use of explosives, such as the Beslan, Russia school tragedy in September 2004. In this vicious attack, over 300 innocent victims, more than half of which were children, were massacred in a three-day standoff in which several dozen terrorists used firearms and IEDs. In his book, *Terror at Beslan*, author and special operations instructor for an antiterrorism advisory group, John Giduck, argues that the attack may be an indication of what is to come in America. Giduck also claims to have attempted to offer his expert analysis of Beslan to officials at the DHS; although this offer was never entertained (Giduck, 2005). Retired Army Lieutenant Colonel Dave Grossman wrote the foreword for Giduck's book. In his words, Grossman, who is a former West Point psychology professor and expert witness in the government's case against Oklahoma City bomber Timothy McVeigh, projects that the lessons learned at Beslan must be applied to protect America's children from a similar attack. The true enemy in Beslan, just three short years after 9-11, was the complacency established in an already volatile state. Grossman further echoes Giduck's analysis that those lessons include the implementation of comprehensive site security married with a coordinated response. He states that children are the nation's most important resource and that the most crucial task for America is "to protect our young" (Giduck, 2005). This coincides with the DHS objective if America's young is considered a key resource and America's schools are valuable infrastructure.

In the summer of 2010, the DHS moved again to improve the crosstalk between agencies on all government levels. As part of its Counter Improvised Explosive Device (CIED) Risk Communications initiative, the Human Factors Division of the DHS Science and Technology component is funding a phased project to improve information sharing

about IED events (Department of Homeland Security, 2010). Again, this is a technologically-driven project that aspires to provide computer-based training scenarios to all civil authorities and not an ERA initiative. As discussed in Section 2.1, CIED also fulfills requirements outlined in HSPD 19. The DHS has other projects that address ERA in some capacity; those are specifically detailed in Section 2.1 as well.

2. BACKGROUND

2.1. DEPARTMENT OF HOMELAND SECURITY

Since it was created in 2001 by President George W. Bush, the DHS has played a major role in protecting the nation. The department is tasked with numerous aspects of national security, including border and transportation security, law enforcement and emergency response. In more recent times, the DHS has been active in defining and regulating specific industries that hold vital interests for the nation's operational capabilities. It is certainly pertinent to investigate that role when considering explosives-related threats in the country as the DHS is a major hub in dealing with mitigating risk from those threats. The DHS risk assessment model is reviewed in Section 3.1.

Although substantial effort to create the office was in place prior to the September 11th attacks, it wasn't until shortly after the attacks that the Office of Homeland Security was activated. The office, headed by former Pennsylvania governor Tom Ridge, was tasked to "oversee and coordinate a comprehensive national strategy to safeguard the country against terrorism, and respond to any future attacks" (Borja, 2008). That fall, President Bush issued the first HSPD, which created the Homeland Security Council (HSC) and further defined the agency's role (U.S. Department of Homeland Security, 2008). The following year, the organization was propped up as a department of the federal government and since then there has been 25 HSPDs issued.

Perhaps the best known directive is HSPD 3 which established the Homeland Security Advisory System. Enacted in March of 2002, the system uses a five-tier, color-coded classification to determine the nation's threat level and the protective measures associated with each. According to the DHS website, where a more comprehensive explanation of each level can be found, the goal is "to inform all levels of government and local authority, as well as the public, to the current risk of terrorist acts." Figure 2.1 is an example of the warning system with each tier (U.S. Department of Homeland Security, 2010). At the time of this publication, the threat level was yellow.

Figure 2.1. The Homeland Security Advisory System

Since the threat level advisory system has been implemented, the system has peaked at the orange level several times, typically due to intelligence gathered from suspected terrorists. The aviation threat level has peaked at red and normally remains at a higher level for the transportation-specific sector. The chronology and recent status of the Homeland Security Advisory System is a useful tool for facility managers to gain a general awareness of the nation's threat status, but operators must establish their own means of adjusting a facility's alert system. This can be accomplished simply by audible, multi-media-based systems. The system can be updated to address a variety of situations such as pending severe weather, public unrest and demonstrations, disgruntled employees or financial breakdown. These threat levels should be part of the local emergency response plan (LERP) and coincide with law enforcement's ability to respond to a potential event.

The DHS has several components, many of which are law enforcement. Like most governmental agencies, there is vast bureaucracy involved in determining jurisdictional control. Table 2.1 shows the Department components and brief description of their particular function (Department of Homeland Security, 2010).

Table 2.1. DHS components

Components	Principle Duties
Directorate for National Protection and Programs	Risk-reduction
Directorate for Science and Technology	Research and development
Directorate of Management	Budget and expenditures, HR
Office of Policy	Coordination and planning
Office of Health Affairs	Medical activities
Office of Intelligence and Analysis	Information and intelligence
Office of Operations Coordination and Planning	Monitoring federal security
Federal Law Enforcement Training Center	Law enforcement training
Domestic Nuclear Detection Office	Multi-level nuclear detection
Transportation Security Administration	Transportation systems protection
United States Customs and Border Protection	Protecting the country's borders
United States Citizenship and Immigration Services	Immigration policies
United States Immigration and Customs Enforcement	Border and infrastructure security
United States Coast Guard	Ports and waterways security
Federal Emergency Management Agency	Hazard preparedness
United States Secret Service	Government official protection

Under Science and Technology resides the Directorate's Explosives Division. Not surprisingly, the division's main focus is directed around technological advancement and not centered on developing ERA. According to the Explosives Division website, the unit is seeking "effective techniques to protect our citizens and our country's infrastructure

against the devastating effects of explosives by seeking innovative approaches in detection, and in countermeasures" (Department of Homeland Security, 2009). Under the objectives of the division is a training initiative for canines, an applicable approach for facility managers as well and a discussion topic in Section 5.

As one can see, the main branches of the DHS are extensive and redundant in regards to expertise. A brief overview of this particular agency serves to highlight the DHS's functionality and set the foundation for historic and future goals as pertained to fundamental explosives training in both the public and private realm.

2.1.1. HSPDs 19 and 7: the National Infrastructure Protection Plan.

Authored in early 2007, the intent for HSPD 19 was to further define the nation's policy in combating terroristic explosive threats. The government names the following concentrations in achieving this goal:

- applying techniques of psychological and behavioral sciences in the analysis of potential threats of explosive attack;
- using the most effective technologies, capabilities, and explosives search procedures, and applications thereof, to detect, locate, and render safe explosives before they detonate or function as part of an explosive attack, including detection of explosive materials and precursor chemicals used to make improvised explosive or incendiary mixtures;
- applying all appropriate resources to pre-blast or pre-functioning search and explosives render-safe procedures, and to post-blast or post-functioning investigatory and search activities, in order to detect secondary and tertiary explosives and for the purposes of attribution;
- employing effective capabilities, technologies, and methodologies, including blast mitigation techniques, to mitigate or neutralize the physical effects of an explosive attack on human life, critical infrastructure, and key resources; and
- clarifying specific roles and responsibilities of agencies and heads of agencies through all phases of incident management from prevention and protection through response and recovery (Department of Homeland Security, 2009).

The first goal is perhaps the most revealing aspect of this strategy, and likely the least acted upon at the local level. Modern potential threat includes a variety of assailants and not just radical terrorists as defined by the public's perception. Militia groups, disgruntled employees, teenaged delinquents, activists, previously convicted criminals and religious fanatics all can be terrorists. The psychological and behavioral approach, however, takes a commonality among potential threats and concentrates the security response toward actions rather than appearance and association. The DHS, as mentioned in previous sections, has taken policy measures to ensure a broad approach is considered when combating explosives-related threats.

Another interesting area is the final goal. When it comes to an explosives event, the federal government continues to struggle with not only the proper response, but also the ensuing investigation as well. To date, both the Federal Bureau of Investigation (FBI) and Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) have struggled to work within a clearly defined capacity when responding to explosives attacks and have toiled over the implementation of the government's policies. Each also has had astounding victories in stopping potential terror attacks. It is worthy to note that there exists other directives and policies that relate to this subject, however, a comprehensive investigation of these would deviate from the focus of this composition.

While policy implementation is an obvious problem not all of the federal initiatives have been rejected from the cause nor have they stemmed ambiguity in determining clear objectives The National Infrastructure Protection Plan (NIPP) has developed a model for site security that could be manipulated to fit any facility's needs.

Responding to HSPD 7, the purpose of the 2009 NIPP is to appoint the DHS the leading governmental entity in defining CIKRs and working with private sectors to ensure those assets are protected for the good of the nation. More specifically, the NIPP's goal is to:

" Build a safer, more secure, and more resilient America by preventing, deterring, neutralizing, or mitigating the effects of deliberate efforts by terrorists to destroy, incapacitate, or exploit elements of our Nation's CIKR and to strengthen national preparedness, timely response, and rapid recovery of CIKR in the event of an attack, natural disaster, or other emergency" (Department of Homeland Security, 2009).

The NIPP, developed under former DHS Secretary Michael Chertoff, outlines a comprehensive collaboration between a federal Sector-Specific Agency (SSA) and its CIKR sector. Appendix A is a table from the NIPP that shows the agencies and sectors. The NIPP further highlights utilization of risk management, as discussed in Section 3, and continues to establish a working rapport between the private and public sectors through the implementation of site security plans to protect the country's critical resources. The plan is quite extensive, covering the scope of 18 identified CIKRs, assigning areas of responsibility for specific agencies and revisiting HSPD 19. In the plan, the Secretary of Homeland Security identifies the Office of Infrastructure Protection (IP) as the coordinating group for explosives-related events. The IP is tasked specifically with improving the effort to address IED-specific threats by "coordinating national and intergovernmental IED security efforts; conducting requirements, capabilities, and gap analyses; and promoting information-sharing and IED security awareness" (Department of Homeland Security, 2009); all of which are reoccurring themes on the national level.

The NIPP also revisits several aspects of the DHS's role by stressing many points of HSPD 19 and how the departmental crosstalk should coincide with the private sectors obligated to protect resources and infrastructure. It also describes the need for better information sharing, as stated in Section 1. The NIPP addresses this need by tasking the DHS, stating it "will establish and maintain secure information-sharing systems to provide law enforcement agencies and other first-responders with access to detailed information that enhances the preparedness of Federal, State, local, tribal, and territorial government personnel to deter, prevent, detect, protect against, and respond to explosive attacks in the United States" (Department of Homeland Security, 2009). The aforementioned CIED Risk Communications initiative is a step in the right direction for crucial information sharing. The NIPP also creates a working relationship to allow CIKR sectors to develop site security plans, which are evaluated by the DHS on risk-based performance measures (RBPMs). This approach allows a facility to develop its unique plan, rather than having the execution of that plan dictated exclusively by the government.

As part of its CIKR learning series, the DHS sponsors ongoing training events and webinars to assist private sector facility operators to hone their site security to an

acceptable level. In November 2009, Michael Norman, the IP Field Operations Branch Chief and manager of the Protective Security Advisor (PSA) program presented a web-based training session explaining the branch and departmental role in providing site assistance visits (SAVs). The purpose of SAVs is to assist a facility in the assessment of its comprehensive security plan. The SAV concentrates on three aspects: physical security, security management and the security force. The visit, part of a vulnerability assessment, is guided under the PSA assigned to that region or state. Without having taken part in such an assessment, this author is unaware of the weight explosives training contributes to the security force.

The methodology of the survey is rather complex and involves hundreds of variables with respect to the three security areas. The entire process is extensive, but the gist is "to provide a valuable tool back to the owner/operator" in order to appropriately assess the security risks (Norman, 2009). The assessment is designed to allow facility managers to direct security efforts under DHS recommendations, conveyed to the facility as a protective measure index (PMI). The feedback assigns a numerical ranking to each area of security and allows the operator to manipulate data to adjust security efforts to the need of the facility. This tool, also known as the Infrastructure Survey Tool (IST), is the premise of site awareness and training and should be coupled with the site's comprehensive risk management process. In fact, this approach can be accomplished on a local level with many security upgrade solutions developed as no-cost alternatives by the facility's own employees. This empowerment seems to be the standard for at least one sector working to improve infrastructure protection against terrorists.

2.1.2. Chemical Facility Anti-Terrorism Standards Case Study. As discussed in the previous section, there are 18 different sectors for which the DHS provides SSAs. Perhaps the most impressive effort to date in fulfilling security requirements is the Chemical Sector's approach to facilities security as outlined by the DHS. The program, established in 2007, is known as the Chemical Facility Anti-Terrorism Standard (CFATS). The CFATS regulation is quite extensive, and given its current implementation, is not completely understood by industry. The methodology of CFATS, however, is the primary focus for relating chemical facility TTPs to other facilities

seeking to combat explosives-related threats. Nonetheless, a brief history regarding the participants and creation of CFATS is pertinent. As with any new regulation, there are numerous consultants in line to assist each company in achieving the standard. Like risk management though, many of these facilities may have the expertise they need to not only meet the goals of CFATS, but also to develop their own standards that exceed the federal regulation.

In 2004, a conglomerate of chemical sector professionals formed the industry's Sector Security Council (SSC). This council, now comprised of 15 organizations and corporations, including the Institute of Makers of Explosives (IME), partners directly with the DHS in forming a union that addresses concerns within the industry and national security. The SSC is also aiding the industry by "developing new initiatives to share information and best practice; and enacting the regulations under CFATS" (Summit Gazette, 2010). The council also works with the DHS in organizing an annual meeting of professionals known as the Chemical Sector Security Summit. In 2010, the fourth annual summit convened in Baltimore, Maryland, for two days of discussion, training, business interaction and information sessions. The summit, designed to enhance the communication of CFATS inquiries from the industry to DHS, succeeded in clearing the goals of the standard creating a venue for professionals to discuss concerns in applying CFATS to their facility. The DHS acknowledges this success as well.

The SSC, as well as the industry, receives tremendous praise from the DHS for its continuing efforts to bring security of CIKR to the forefront. In his remarks to summit participants, DHS IP Assistant Secretary Todd Keil states the "conference is a model for the type and level of engagement we need if we are going to safeguard the Nation's critical infrastructure" (Chemical Sector Security Summit Remarks, 2010). Homeland Security Secretary Janet Napolitano attended the event as well, praising the NIPP, SSC and CFATS as "Flexible, practical, and collaborative programs" that "play a key role in enhancing the security and resiliency of our nation's chemical facilities and other critical infrastructure" (Department of Homeland Security, 2010). Through the chemical SSA, the industry also focuses somewhat on ERA.

Throughout the first of half of 2010, the chemical sector SSA sponsored several Chemical Sector Explosive Threat Awareness Training (CSETAT) programs. The course

is a six-module, one-day event geared to offer chemical facility security personnel a closer look at IEDs and to enhance the "chemical sector's ability to deter, prevent, detect, protect against, and respond to attacks that use IEDs" (Department of Homeland Security, 2010). This training is unique to the chemical sector and provides facility managers a psychological edge in ERA by incorporating a legitimate threat to crucial infrastructure, a focus again echoed in Section 5. The training revisits the NIPP and applicable HSPDs, as well as trends in terrorism, IED and VBIED (vehicle-borne IED) design, incidents and explosive effects, IED trends, indicators and detection, and surveillance detection (Miller, 2010)**.** This approach psychologically prepares the security officials within the industry with a foundation of IED knowledge that can be married with a basic understanding of explosives components. The program also updates CFATS as well. Appendix B shows the CSETAT information flyer for 2010. The program is slated to continue again in 2011. Besides, the aforementioned program, the DHS has other explosive initiatives as well.

2.1.3. Awareness and Localization of Explosives-Related Threats. Additional programs under the office include the Office of Bomb Prevention's "Tripwire," which is an information and IED communication medium; the multi-jurisdictional IED site plan (MJIEDSP), which allows communities to share and respond to events; and perhaps the department's most legitimate effort to enhance ERA, the Center of Excellence (COE) for the Awareness and Localization of Explosives-Related Threats or ALERT.

Originating in 2008, ALERT is a multi-agency effort that includes not only governmental involvement, but also academia and industrial participation. Some of the nation's most renowned research facilities, along with successful research corporations and esteemed S&T institutions, have combined to form a comprehensive educational approach to explosives threats. Albeit a concerted technological venture, ALERT is a copacetic opportunity to establish a joint concentration aimed at bringing ERA to the forefront of technology, in both detection and blast mitigation. The program also focuses on developing future experts in the explosives field by developing recruiting plans to entice potential law enforcement professionals into the realm of advanced explosives training.

Northeastern University in Boston and the University of Rhode Island are leading the COE's effort to bring to the table all entities with a legitimate interest in explosives detection and characterization and blast mitigation. ALERT specifically is geared to "conduct transformational research, technology and educational development for effective characterization, detection, mitigation and response to the explosives-related threats facing the country and the world" (Northeastern University, 2010). As mentioned, ALERT has an impressive core partnership as well. The Northeastern University website lists all the affiliates as of 2010. Those participants are listed in Table 2.2.

Table 2.2. ALERT partners

Academic
Boston University, California Institute of Technology, Hebrew University of Jerusalem, Missouri University of Science & Technology, New Mexico State University, Rensselaer Polytechnic Institute, Soreq Nuclear Research Center, Texas Tech University, University of Puerto Rico at Mayagüez, Washington State University
Strategic
Idaho National Laboratory, Lawrence Livermore National Laboratory, Los Alamos National Laboratory, Sandia National Laboratory, Massachusetts General Hospital, Tufts University, Woods Hole Oceanographic Institution
Industrial/Governmental
Analogic Corporation, American Science & Engineering, John Adams Innovation Institute, Lockheed Martin Corporation, Raytheon Company, Siemens Corporate Research, Textron Systems Corporation

There are several other underlying participants in the program as well. As mentioned previously, ALERT comprises a multi-focused effort to not only explore a partnership with the nation's explosives experts, but it also defines each highly-technological research effort.

ALERT has four main research initiatives: explosives characterization, explosives sensors, explosives sensor systems and post-blast mitigation. Each program, recognized as F1, F2, F3 and F4, respectively, are strictly technology-based plans to improve detection and barrier systems. However, these core initiatives are married with an educational initiative led by the University of Rhode Island. The aim is to "establish a conduit that includes precollege, undergraduate, graduate and career professional components" and train those future leaders "who will be important contributors to DHS and to the success of its critical mission" (Northeastern University, 2010). That "critical mission" is to further develop a defense against terrorist threats using explosives and enhance the security for CIKR on which the nation depends. As part of this research, a comprehensive short-course was developed to address local security threats and is discussed in greater detail in Section 4.

The education phase of ALERT is a genuine route for law enforcement seeking to specialize in advance explosives training. Outside of a few universities, though, first responders must network on all governmental levels to gain that knowledge, unless a private company is compensated to provide the ERA training. Even rarer is the offer of a formal explosives degree or authentic certification in academia. But under the ALERT initiative, high-school and community college students, undergraduates and graduates can obtain the advanced training and education from universities such as Missouri S&T which offer several levels of explosives education. In fact, Missouri S&T seems ideal for obtaining ALERT's goals due to its variety in explosives education where "students have the exclusive opportunity to safely handle and employ explosives in various disciplines while pursuing either an explosives engineering emphasis or certificate, explosives engineering minor and an Explosives Engineering Master of Science" (Hawkins, 2010). Facility managers must also find ways for their security professionals to gain ERA training as well. As stated in the previous section, the chemical sector has made available such training through the DHS.

Obviously there is a distinctive technological concentration to mitigate explosives-related threats. What's more, there are even specialized training sessions available if companies know where to seek the information. But where the initiative falls short is on the implementation of ERA for site security and the psychological

attentiveness, or rather the presence of complacency and obliviousness, to the dangers facing communities daily. Protecting the country, and making known these threats, is a primary role of the federal government.

2.2. FEDERAL EXPLOSIVES INVESTIGATORS

Outside of the military, there are two primary investigating agencies when explosives-related threats surface on a national level. Both the FBI and ATF have distinct jurisdiction in intelligence gathering and post-blast investigation. The FBI has its Explosives Unit (EU) which is tasked with conducting "examinations of evidence associated with bombing matters" (Federal Bureau of Investigation, 2010). According to the agency, the EU is involved with bombing scenes and IED component identification. The FBI also has 15 explosives detection canines in its police force. These dogs are a viable component to a site's explosives security plan and, as discussed Section 5, can be trained exclusively on a reward system, which is difficult to execute with humans. Implemented over the last decade, FBI dogs are trained to detect over 19,000 explosives compounds (Federal Bureau of Investigation, 2010).

The FBI has the primary obligation to investigate terrorism in the United States. This authority has been granted throughout the last three decades, primarily through Presidential Directives (U.S. Department of Justice, Office of the Inspector General, Audit Division, 2009). Considering IEDs are a growing weapon of choice by terrorists, it stands to reason that the agency must arm itself with explosives-related knowledge and capabilities in order to effectively respond to possible terrorist attacks which involve explosives. The National Counterterrorism Center (NCTC) reports that in 2009, there were nearly 11,000 terror attacks worldwide (U.S. State Department, 2010). This alarming increase must signal to federal agencies that developing and implementing a sound education and response plan must be in the forefront of the national strategy.

From the National Consortium for the Study of Terrorism and Responses to Terrorism, a DHS COE at the University of Maryland, Figure 2.2 shows the exponential increase in the usage of IEDs as terrorists' weapons of choice (University of Maryland, 2010).

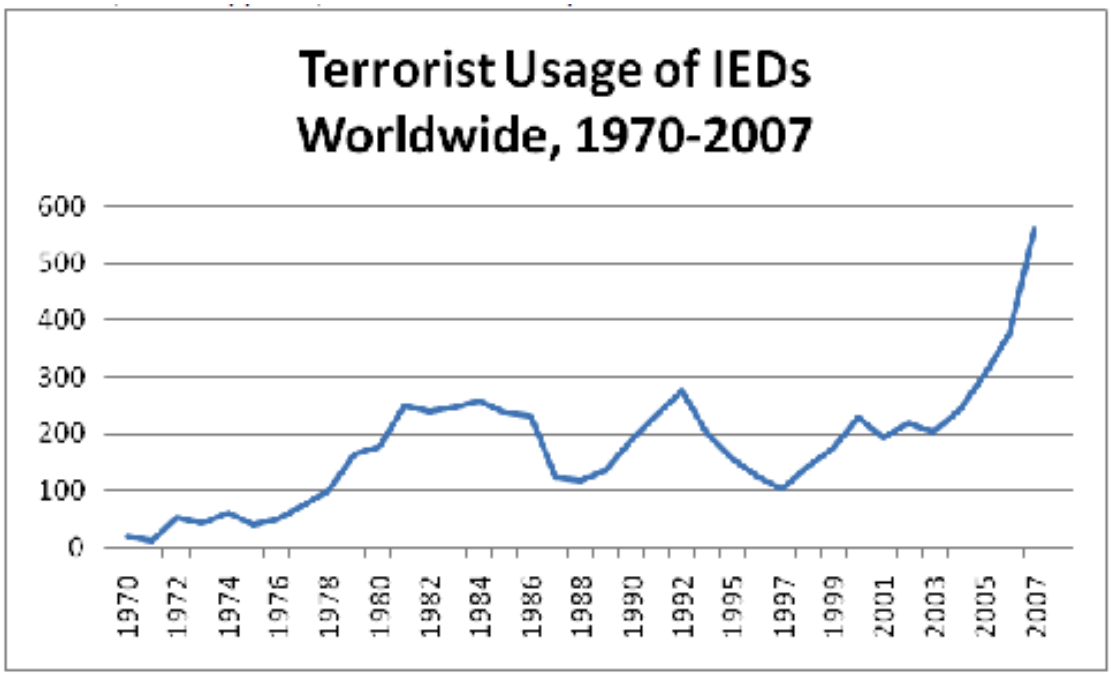


Figure 2.2. Terrorist usage of IEDs worldwide, 1970-2007

When it comes to explosives regulations, the ATF has the lead. Reassigned to the DOJ in early 2003 under the Homeland Security Act of 2002, the ATF has been primarily responsible for the explosives industry. The agency's most legitimate explosives effort to date is ensuring proper storage and licenses of explosives and enforcement of the SEA of 2002. More details about the SEA are discussed in the following section.

Like the FBI, the ATF has an explosives detection canine program as well. To date, the agency has deployed over 300 canines worldwide trained to detect similar compounds as the FBI trained force (Bureau of Alcohol, Tobacco, Firearms and Explosives, 2010). As with the FBI's EU, the ATF employs its own explosives experts. A Certified Explosives Specialist (CES) is tasked with conducting investigations regarding explosives and explosives regulations. The CES is a special agent with the ATF required to acquire two years of training (Bureau of Alcohol, Tobacco, Firearms and Explosives, 2010). The ATF also trains Explosives Enforcement Officers (EEOs). These experts have more extensive duties than the CES and offer a wide range of services. From the ATF website, an EEO is trained in:

- Providing technical advice/assistance on Federal storage regulations and the handling or disposing of explosives;
- Threat and infrastructure vulnerability assessments both domestically and abroad;
- Constructing facsimiles of explosive devices;
- Preparing determinations on explosive, incendiary, and destructive devices for court proceedings;
- Providing expert witness testimony;
- Conducting render safe/disassembly procedures on explosive and incendiary devices and materiel;
- Conducting large scale explosive destruction operations;
- Operational & training support to state/local, national and international agencies and interests;
- Underwater explosives dive and recovery operations;
- Research studies and analyses of explosives-related equipment and materiel;
- Supporting National Special Security Events and other major events (Bureau of Alcohol, Tobacco, Firearms and Explosives, 2010).

Besides providing explosives experts, the ATF is charged with maintaining the Bomb Arson Tracking System (BATS). This is a web-based database which provides all levels of law enforcement "access to national arson and explosives incident information" (Bureau of Alcohol, Tobacco, Firearms and Explosives, 2010). While BATS seems like an extraordinary tool for explosives investigators across the nation, it has some issues with information sharing. These problems, as well as other investigative barriers between the ATF and FBI, are discussed in Section 2.2.2. As mentioned in previous sections, there is little doubt that the U.S. policy regarding explosives-related threats is firm in intention. However, like previously noted, the problem is not the strategy, but rather the implementation of regulations such as the SEA, an effort with which the ATF continues to struggle.

2.2.1. The Safe Explosives Act of 2002. The ATF's 2007 edition of Federal Explosives Law and Regulations incorporates extensive revisions from the SEA. According to then director, Michael Sullivan, the SEA was developed to ensure that explosives materials were protected from use in IEDs. Sullivan states in the law that "Security of all explosives materials is an essential tool in the war against terrorism" (Bureau of Alcohol, Tobacco, Firearms and Explosives, 2007). The former director reverts to the importance of implementing the SEA stating that the ATF takes the role in ensuring proper implementation of the SEA for securing explosives, but he also acknowledges that "internal controls and industry-created publications also support the secure and safe storage of explosives materials" (Bureau of Alcohol, Tobacco, Firearms and Explosives, 2007).

This philosophy coincides with the overall premise; which is more specifically outlined in Section 3.2, that companies are well served to exceed standards through self-regulating standard operating procedures (SOPs). These SOPs should be comprehensive, applied, practical and dynamic with continuous improvements. Methods for achieving this goal are outlined in Section 3.2 as well.

The SEA's main purpose is to define persons who are prohibited from receiving or handling explosives. Effective January 2003, the prohibited persons category was expanded and the ATF became more involved in guaranteeing that proper background checks were conducted to ensure safe explosives handling. Besides industry, this standard applies to academic institutions and businesses outside of military occupational specialties which require explosives handling. Missouri S&T's explosives engineering program conducts background checks of all students enrolled in an explosives course. Although the ATF has received criticism in implementing the SEA, facilities must ensure these checks are conducted for the safety of their employees, contractors and visitors. Table 2.3 has the complete list of prohibited persons (Bureau of Alcohol, Tobacco, Firearms and Explosives, 2002).

Table 2.3. ATF's list of prohibited persons

Prohibited Persons
Aliens (with some exceptions)*
Persons dishonorably discharged from the military*
U.S. citizens who have renounced their citizenship*
Convicted felons
Users and addicts of controlled substances
Fugitives
Mental defectives or persons committed to mental institutions

* These categories were added to the SEA 2002

All categories of prohibited persons may apply for relief from explosives disabilities by filing with the ATF. However, each company employing potential explosives handlers must take measures that protect the public and limit access to materials that can be used in an attack. Additionally, those tasked with security of a facility that utilizes explosives must become familiar with the regulation. This provides a secondary system of checks for site security, and if a company's security component is aware of those people who are permitted to handle explosives on site, then the likelihood that prohibited persons come in contact with explosives is reduced.

While the introduction of the SEA seems a worthy undertaking, the ATF has received severe criticism with regards to its implementation. Again, the reoccurring theme is not the problem with policy, as there seems to be more than an adequate compilation of regulations on the federal level, but rather the process of implementing that policy.

2.2.2. Office of the Inspector General Reports. As part of the process to ensure the policies of the government are properly employed; a system of studies is emplaced. Often times, these investigations stem from anonymous information obtained from the applicable industry, or the tragic consequence of a catastrophic event, such as the 9-11 Commission. In either case, the process involves official probes into the execution of

lawmakers' intent. That jurisdiction on the national level, as it pertains to the health and welfare of citizens, lies with the Office of the Inspector General (OIG).

In March 2005, the OIG published a report regarding the ATF's implementation of the SEA. The "Review of the Bureau of Alcohol, Tobacco, Firearms and Explosives' Implementation of the Safe Explosives Act" is highly critical of the ATF's initial efforts in completing appropriate background checks for possessors of explosives and identifying those who may have been prohibited persons. The report, which exceeds 100 pages, states that there are "critical deficiencies in the ATF's implementation of the background check and clearance process that prevented the agency from ensuring that prohibited persons are denied access to explosives" (Office of the Inspector General, 2005). In short, there are already citizens within the community handling explosives that should not be. For those within the industry, this is probably not a surprise. The report's conclusions, which many have been disputed by the ATF, reinforce the idea that policy makers once again created a realistic avenue to combat explosives-related threats just to fall short in implementing the standards. In just two years since the SEA went into effect, the agency charged with upholding explosives regulations was bombarded with questions of competency.

Notwithstanding the intentions of the investigation, is it a fair assessment to not only create a system of licensing and handling with federal oversight, but also to encourage the lowest level of scrutiny possible. Considering the horrific consequences if nefarious possessors of explosives are not identified, each entity concerned with site security, especially vulnerable sites as hospitals and schools, must then become more vigilant in understanding what explosives can do and what components of IEDs may look like.

The findings by the OIG are more profound than just background checks. The report criticizes other aspects of the SEA's implementation. These conclusions range from delayed investigations of explosives licensees, the ATF's knowledge and tracking of prohibited persons, failure to properly train inspectors on the SEA and coordination of investigations with the FBI. The OIG cites that "comparison of ATF and FBI data found no record that the ATF requested FBI background checks on 59 of 683 employees of explosive licensees (9 percent) whose ATF records we examined" and it was also found

"that the ATF had failed to complete the background check process for over half (655 of 1,157) of the individuals identified by the FBI as possible prohibited persons" (Office of the Inspector General, 2005). From the findings, it appears the FBI and ATF have done little to help one another, even when national security is on the line. Not surprisingly, the relationship between the ATF and FBI has soured the intent of the SEA as well. This is more evident in another OIG report.

In October 2009, the OIG released its "Explosives Investigation Coordination Between the Federal Bureau of Investigation and the Bureau of Alcohol, Tobacco, Firearms and Explosives." Leading up to the report, the DOJ took several measures in clearing the explosives investigation boundaries between the ATF and FBI. As discussed in the 2005 report, the animosity between the two agencies might have well been created when the decision was made to include the ATF into the DOJ ranks, historically the FBI's turf. While the 2005 publication found fault mainly with the ATF though, in this more recent probe both agencies receive harsh criticism.

After the merger into the DOJ, the ATF was required to work together with the FBI under the stipulations discussed in Section 2.2. Nonetheless, a series of memorandums and directives from the Homeland Security Act to this latest report was unable to create a lucid guideline in which all involved would play nice. One of the primary points of contention is the authority over an explosives investigation, in which the OIG describes both agencies at fault. The report points out that if terror or suspected terror is involved, then the FBI and Joint Terrorism Task Force (JTTF) have jurisdiction. The OIG backed its disputed findings with surveys conducted with agents of both components, a methodology used with local laws enforcement in this composition to analyze the effectiveness of ERA training. Even employees of the ATF and FBI agreed that jurisdictional disputes disrupted timely and precise investigations, with upwards of 90-percent stating that conflict existed over which agency should lead the investigation (U.S. Department of Justice, Office of the Inspector General, Audit Division, 2009). This sentiment has trickled down to state and local responders as well with nearly all of the respondents agreeing that the federal response is nothing more than an ambulance chase for accolades. This perception not only denies the national agencies respect, but also draws incongruent focus intended by the SEA. With response to explosives events being

the most contested issue in federal reaction, the OIG report actually contains 15 recommendations for improving working relations between the FBI and ATF. These include consistencies in explosives training, the use of canines, improving BATS and requiring the FBI to provide information to the ATF's tracking database and explosives handling procedures (U.S. Department of Justice, Office of the Inspector General, Audit Division, 2009).

The OIG reports should not be used as stand-alone documents to discredit the national effort. Rather, facilities across the country must recognize that with significant flaws in protection against explosives-related threats comes the opportunity to develop a unique and comprehensive approach to site security. This system, coupled with the continued effort of the federal authority, must entail a focus on education and training and not just reliance that the federal government, or private security companies for that matter, will foil every attack; especially when there seems to be numerous flaws in information sharing and implementation. Facilities have an obligation to protect, and sometimes that protection comes at a cost. Owners and operators must make every reasonable attempt to create an authentic protection plan that includes information sharing and addresses the specific needs to the company. This effort expands well beyond technology.

2.3. PRIVATE SECURITY COMPANIES

The United States has a robust private security industry. Many companies offer various training and services from which facilities managers may opt for a specialization, like that of the chemical sector. The availability of these products is much too vast to cover within this analysis. Likewise, this author has no intent of offering free advertising for the numerous companies offering explosives classes and training in the thousands of dollars. Although it is necessary to acknowledge that for a price specific explosives training is available. Not only will companies offer expertise in ERA, providing that the investment is made to obtain their product, but these same companies will also fulfill the risk management need. These professionals, most of which are credible and qualified, make substantial profit providing a company a product which is simply arranged.

Nonetheless, many within the industry lobby for more training and exposure to realistic threats in order to better protect the facility where they work and themselves.

In a free market society, a climate exists where those with knowledge can provide services for those who are willing to pay for it. Companies peddle their expertise to the tune of $500-$1,000 a day for explosives training. Training kits, such as IED packages that include simulated explosives devices, can cost in the thousands and even tens of thousands. There is no question that many of these resources are applicable to site security, however, unlike the nation's budget for detection systems and barriers, the goal of ERA training must be achieved at much lesser cost. Many local and state budgets simply cannot absorb the expenditure of this expensive training. But, with the proper network and attitude, low-cost, effective ERA training can be co-sponsored among first response agencies and a collaborative effort can be made to co-host either private companies or academic professionals to offer the applicable classes. The goal is to get those tasked with security a basic knowledge of explosives, not to make them experts.

A common question in the ERA training discussed in Section 4 is "What does an IED look like?" Instructors with even the basic knowledge of IEDs know that the mechanism can take on the appearance of countless devices, limited only to the manufacturers' imagination. Therefore, rather than spending thousands of dollars for a training kit, site security forces can devise their own with common items found in retail stores or strewn about the property. A reasonable approach to spotting out-of-the-ordinary components is the key to ERA and not necessarily the ability to identify the explosives itself. Couple that focus with the use of canines and simple standoff, a foundation of site security has been laid at a relatively low expense. Some of these basic concepts and recommended solutions are outlined in Section 5.

In the meantime, facilities can establish communication with all levels of government support and begin their site assessments. They can take advantage of low-cost approaches, like that of chemical sector's CSETAT, or continue to seek high-paid consultancy for ERA, site surveys and risk management. Until each sector defined in the NIPP undertakes a strict approach that encompasses diligent protection of CIKR, to include vulnerable humans, each facility must establish a process that prepares its employees.

3. RISK MANAGEMENT

3.1. EFFECTIVE RISK MANAGEMENT MODELS

Inherent in every successful operation is a comprehensive and continuous risk management process. Facility managers must understand the incessant nature of risk and how it applies to their procedures and infrastructure. Much of what is discussed about implementing risk management and how it pertains to every legitimate business is derived from the author's nearly two decades of military service and advanced knowledge of composite risk management (CRM). As with other sections of this composition, risk management is a crucial component of ERA and basic security needs. Therefore, a military model, as well as other examples, will be utilized to convey the importance of CRM within any environment. Additionally, owners and operators concerned with explosives threats will be given insight on how a distinctive change in attitude and behavior will pay dividends in morale, prestige and even profit. The most impressive aspect of CRM is the fact that it is extremely cost effective and can be implemented by the facility's own employees. The subsequent text details other advantages that better prepare a facility's security force on a psychological level.

3.1.1. United States Army. There are two basic approaches to risk; acceptance and mitigation. Militarily, leaders are trained to recognize a variety of hazards that may alter a mission or harm troops. The U.S. Army instills risk mitigation at the earliest level of soldier development. As with government regulations, such as the CFATS example in Section 2, there are countless private companies ready to offer costly consultancy to aid in developing a risk model for a particular entity. However, the military approach is to inculcate a behavior change that gives a psychological advantage to its own personnel. Facility operators, using this same philosophy coupled with appropriate ERA training, will have a tremendous psychological edge as well. As cited in the Army's own Composite Risk Management field manual, FM 5-19, CRM is an amalgamation of past experience and decision making that results in "teaching Soldiers [sic] 'how to think' rather than telling them 'what to think' " (Department of the Army, HQ, 2006). The

subsequent text briefly outlines the military CRM model and further relates the model to the NIPP's approach as outlined by the DHS strategy on risk mitigation.

The Army CRM FM 5-19 is an extremely helpful tool for leaders at all levels. It implements an approach of reason and proven TTPs rather than a complex computer-based application that possesses no ability to think. As well, the FM 5-19 further relates this suggested common-sense approach as a substitute to those believing that risk can be adequately wrapped into software. It states that "Technical competency, operational experience, and lessons-learned weigh higher than any set of alpha-numeric codes. Mathematics and matrixes are not a substitute for sound judgment" (Department of the Army, HQ, 2006). This point, not only valid, but also pertinent to any operation, is objectively made despite the Army's own use of a matrix-based assessment. The fact is that algorithms should be tools to aid in the CRM process and not as substitutes to logical thinking freely exercised by the personnel on site. Again, today there seems to be a strict focus on technology, like the billions of dollars spent on detection equipment and complex barriers, rather than a low-cost, common-sense approach. When considering the intrinsically catastrophic effects of an explosives event, it is unwise to trust a machine to dictate crisis management. The Army's use of CRM is a reasonable approach which incorporates all aspects of the process into a quick reference. As well, it assigns responsibility to the appropriate level of the decision-making process rather than allowing inexperienced leaders to accept unnecessary risk.

The model consists of a five-step process. This method begins by identifying the hazards, assessing the hazards, developing controls and making decisions, implementing the controls and supervising the process and evaluating the outcome. As discussed later, there are other models available which use similar guidelines in evaluating and managing risk. Figure 3.1 shows the cyclic and continuous process of the Army CRM process as shown in the FM 5-19.

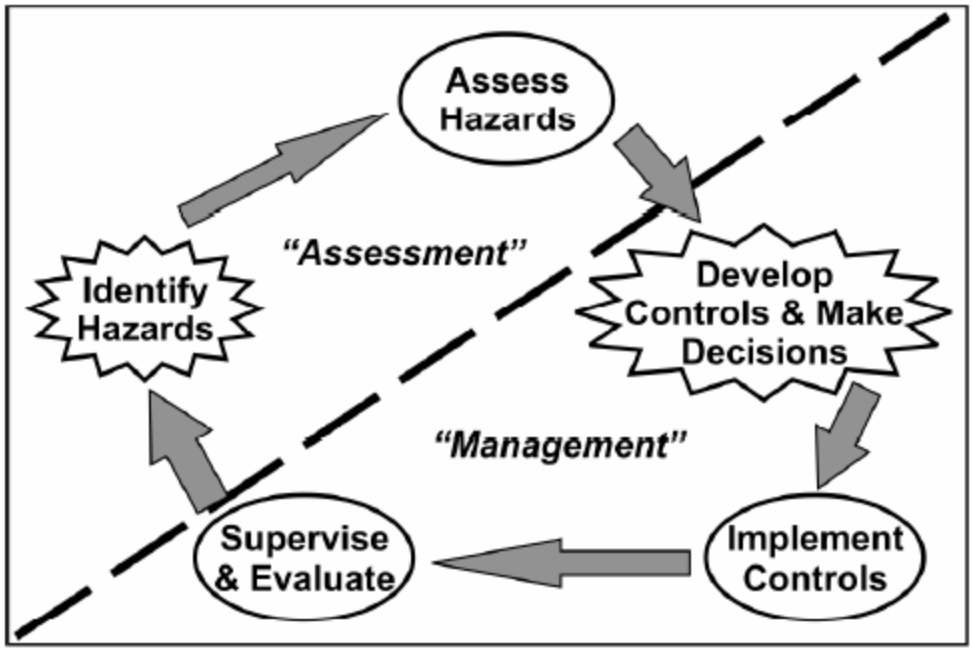


Figure 3.1. The Army risk management model

The CRM model is designed to apply to any mission or operation at any level. In the military, a CRM worksheet is completed prior to convoys, physical fitness training, range qualification and any other training event.

Perhaps the most important part of the process is assessing the appropriate hazards. Like most risk management models, the Army uses two main variables as functions of risk to identify and attempt to quantify the hazards that may affect an operation. These components of risk address the likelihood the event will occur and the effects on personnel and equipment if it does transpire. The FM 5-19 contains specific definitions for each and categorizes the two criteria as probability and severity. Most models of risk management use some form of each category. Figure 3.2 shows the Army's risk management matrix.

RISK ASSESSMENT MATRIX						
		Probability				
Severity		Frequent A	Likely B	Occasional C	Seldom D	Unlikely E
Catastrophic	I	E	E	H	H	M
Critical	II	E	H	H	M	L
Marginal	III	H	M	M	L	L
Negligible	IV	M	L	L	L	L
E – Extremely High		H – High		M – Moderate		L – Low

Figure 3.2. The Army risk management matrix

The probability section has five categories: frequent, likely, occasional, seldom and unlikely. The FM 5-19 provides leaders specific definitions for each to allow more objectivity in assessing the hazard (Department of the Army, HQ, 2006).

- Frequent – Occurs very often, known to happen regularly.
- Likely – Occurs several times, a common occurrence.
- Occasional – Occurs sporadically, but is not uncommon.
- Seldom – Remotely possible, could occur at some time.
- Unlikely – Can assume will not occur, but not impossible.

Once the probability of the hazard is defined, leaders look into the severity of the event if it was to occur. Severity has four categories: catastrophic, critical, marginal and negligible. Definitions for the categories of severity are much more conducive to mission. However, a brief range from the FM 5-19 spans from “catastrophic” as total operational failure and death to “negligible” being little or no impact on the operation. After probability and severity are determined, the matrix allows leaders to join the two to determine an overall risk level for the mission. The risk levels are: extremely high, high, moderate and low.

The next step in the CRM is to mitigate hazards by developing and implementing controls to reduce the overall risk level. The highest risk hazard is the level accepted for

the mission. Once the risk level has been established, responsibility is assigned as to whether to conduct the operation or attempt to further mitigate unacceptable hazards. This entire process is completed on a "Risk Management Worksheet." Appendix C is an example of a completed worksheet on which hazards and controls are identified for a company's rifle qualification range. The residual risk becomes the conscientious focus for the appropriate authority. For the military, this risk decision is based on the risk level and may span from a company commander for low risk training to a division commander for extremely high risk missions. A civilian facility or operation can mirror this process by allowing qualified personnel to make the appropriate decision on the low end of the assessment to as high as owners for the more risky decisions. For instance, an ammunition manufacturer may routinely assign a moderate risk to facility operations. However, with intelligence geared toward attacks on the facility coupled with an elevation in the Homeland Security Advisory System, plant managers may opt for an extremely high risk level. In correlation, a gate guard at the same facility may point out to her supervisor that visibility is obscured due to weather conditions for the day. The facility, not needing a plant manager to adjust the risk level, may empower that security supervisor to raise the risk from low to moderate.

The Army's risk management model is simplistic and easy to use. It's also a readily available tool that can be completed on all levels at any site. It is important to note that it is impossible to mitigate all risks and there will always be hazards present, identifiable or not. The purpose of assigning responsibility for the varying risk levels is to make the final risk acceptance authority accountable. This procedure is utilized somewhat by other governmental agencies as well.

3.1.2. DHS Risk Management in the NIPP. The DHS model for risk management is similar to that of the Army's and other genuine professions. This section contains a brief summary of the DHS risk management process and draws comparisons and contrasts to the military model. The procedures for mitigating risk are commonplace among public organizations and can easily be applied to most entities. In the NIPP, the risk management process is regarded as "the cornerstone" of the plan (Department of Homeland Security, 2009). It is this philosophy, that incorporating realistic risk

management is actually cost saving in both resources and expenditures, which generates a psychological advantage of prevention rather than reaction. Also like the military, the DHS version is a cyclic model that requires continuous assessment in order to protect CIKR. Figure 3.3 shows the NIPP risk management framework (Department of Homeland Security, 2009).

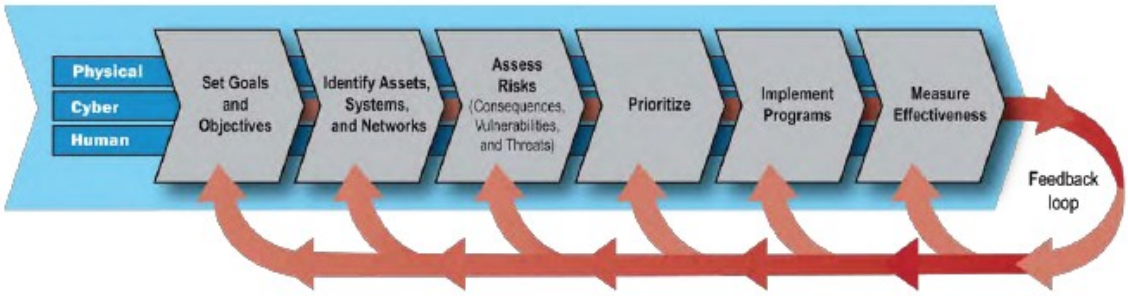


Figure 3.3. NIPP risk management framework

The first step to the NIPP's risk management model is to set goals and objectives considering the physical, cyber and human elements with regards to CIKR protection. This approach, unlike the Army model in which encompasses all justifiable risks without being categorized, provides a risk management focus for facility managers. The "human" aspect provides a psychological legitimacy of which there is an acknowledgment that attitude and behavior, complacency and resiliency are indeed credible functions of the risk management process. The goals and objectives are specific to the cause of the company and should be direct and well-defined.

Once a site properly identifies the goals, it must continue with identifying the resources in which a developed plan can become reality. In identifying these assets, or systems and networks that exist to aid the facility, a consideration must be given to the availability of the asset. For example, although federal explosives databases are an asset, specifically the BATS system discussed in Section 2.2, the usability and timely update of the system may not be an asset, but rather a hindrance. Nonetheless, site operators must take advantage of all available resources with the understanding that any one of those can

be made unavailable during an emergency. The more a company can put into place its own systems, like those discussed in the following section, the more it can rely on the data.

The next step to the NIPP framework is assessing the risk. As shown in the previous figure, risk is defined as a function of consequence, vulnerability and threat. This coincides with most basic models which consider the likelihood and severity of the event. As stated in the NIPP, "it is important to think of risk as influenced by the nature and magnitude of a threat, the vulnerabilities to that threat, and the consequences that could result" (Department of Homeland Security, 2009). The following of each definition comes from the NIPP text and gives clear and concise structure with regards to risk assessment:

- **Consequence**: The effect of an event, incident, or occurrence; reflects the level, duration, and nature of the loss resulting from the incident. For the purposes of the NIPP, consequences are divided into four main categories: public health and safety (i.e., loss of life and illness); economic (direct and indirect); psychological; and governance/mission impacts.
- **Vulnerability**: Physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard. In calculating the risk of an intentional hazard, a common measure of vulnerability is the likelihood that an attack is successful, given that it is attempted.
- **Threat**: Natural or manmade occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property. For the purpose of calculating risk, the threat of an intentional hazard is generally estimated as the likelihood of an attack being attempted by an adversary; for other hazards, threat is generally estimated as the likelihood that a hazard will manifest itself. In the case of terrorist attacks, the threat likelihood is estimated based on the intent and capability of the adversary.

Once again, the model contains significant similarities to the Army's approach and provides a method for calculating the risk as it applies to the facility. Even more crucial than assessing all possible threats is deciding which ones to mitigate in great

detail and which ones must be realistically accepted. This is covered in the next step of the framework.

After the risks are identified and assessed, prioritizing the most substantial and applicable must take place. This stage, as it pertains to CIKR covered in the NIPP, is a sector-specific approach on a broad level, but must take an intimate focus for a single site. Owners must take into account the cost effectiveness of mitigating the risk and which hazard should receive not only the money, but also the attention. In the Army, a traditional phrase of such prioritization focuses that attention as it relays time management to a rifle qualification. For pop-up silhouettes on the rifle range, the closer targets tend to stay exposed for the shorter amount of time. The farther a target, the longer it stays exposed. Therefore, soldiers are encouraged to engage the closest target first. The same applies to a company attempting to prioritize its risks. If the site is planning a long-term event that exposes its infrastructure or employees, proper consideration must spotlight the timeframe as well as the functions of risk. Put more simply, security officials must engage more pressing threats rather than spending time planning for possible future threats. This does not mean that those risks are not assessed, but rather that crucial resources be allocated to mitigate the immediate problem. Long-term threats also may change in time or prove false altogether.

Subsequent to prioritization is implementing the plan. This is a time where the best possible solution has been devised to "prevent, deter, and mitigate the threat; reduce vulnerability to an attack or other disaster; minimize consequences; and enable timely, efficient response and restoration in a post-event situation, whether a terrorist attack, natural disaster, or other incident" (Department of Homeland Security, 2009). Like identification of pertinent resources and assets, putting into action a risk management plan is subject to variables in the system. A major component of this is the cost effectiveness of the solution. Often times an episode could have been prevented if enough money was thrown at the problem. But if a company is bankrupt, the risk management process is moot. Therefore, cooperative training programs, employee feedback, psychological tools and common-sense solutions must be entertained to offset extreme costs. Most industries are succumbing to best-available technology to alleviate systematic issues, but that technology, as noted in the previous sections, can be costly and difficult to

utilize. The NIPP continues to extensively cover plan implementation and provides numerous programs on which sectors can rely.

Perhaps the most critical component of the DHS risk management model is measuring the effectiveness of the plan. This step can be achieved in many ways but must coincide with the intent of the goal and objective. Like the after action review (AAR) in the Army, timely feedback must be obtained in order to improve or abandon processes not accomplishing the standard. This feedback can be ascertained at any stage of the cycle and should come in the form of legitimate improvement to the plan rather than pure criticism without solution. A suggested method in quantitatively gauging the security effort is the test of a practical pilot. This method, as discussed in Section 5, tests security TTPs prior to and after ERA. Its intent is to improve procedures through statistical analysis of a cost-effective training program. For facilities and sectors using RBPMs, it is also a method of checking the success or failure of the standard. Most importantly, it gives owners a baseline as to whether a new plan needs to be created and implemented or if a proven tactic can be improved upon.

The risk management system is just one component, albeit a critical one, of ERA and how it applies to overall site security from explosives-related threats. As the need for training comes to light, facility managers have been given so far basic tools and considerations for protection against explosives events. It is up to them to establish a standard operating procedure.

3.2 DEVELOPING A STANDARD OPERATING PROCEDURE

The goal of an SOP is to establish protocol within a unit. It must exceed every regulatory expectation. Additionally, it must be exposed to third party review. This review can be from partners in the industry or even government employees. Regardless of the design of an SOP, it must be living proof of the procedures in which a facility incorporates under certain tests. Site security is just that, an essential daily test of the ability of the owners and operators to provide a safe environment for protection of their people, products and infrastructure; especially when dealing with explosives-related threats. This section provides examples of successfully implemented “self-regulation.” It also discusses monetary benefits as well as the safety measures that lead to efficiency in

production and public relations. In order to develop a process in which SOPs for ERA and site security are legitimate and detailed, companies must assume an appropriate risk management method and incorporate routinely a basis for review. The mining industry is particularly scrutinized publicly for not practicing established SOP or for blatantly violating federal regulations. Yet the industry has taken great strides to enhance public opinion of the necessary trade. The environmental impact of mining, and how the industry has approached criticism, acts as a superb example of how facilities can take government regulation, like CFATS practices, and incorporate a program under their own volition that exceeds the standards. Environmental disaster and the mitigation thereof, is also perfect illustration as to the cost and consequence of letting safety and risk management falter. Disasters of significant consequences, such as oil spills, are perfect examples.

At the time of this publication, British Petroleum has spent over $11 billion following the April 2010 oil rig explosion. The company has set aside a trust for another $20 billion to settle future claims. Coincidently, the company released a report in the fall of 2010 announcing a new Safety and Risk Operation promising "sweeping changes" in the company's risk and safety approach (British Petroleum, 2010). Lost in the monetary obligation of BP is the fact that 11 employees were killed in the explosion that spilled oil throughout the Gulf Coast. The following initiatives will guide facility managers through a psychological approach to safety rather than just a "check the box" mentality. Furthermore, it develops an understanding that self-regulating procedures outweigh the potential effects of disaster.

3.2.1. International Organization for Standardization; ISO 14001.

Non-governmental organizations can act as proponents of both industry and government. The intent of the International Organization for Standardization (ISO) is to serve as an institute that "enables a consensus to be reached on solutions that meet both the requirements of business and the broader needs of society" (International Organization for Standardization, 2010). The ISO, while mandated by some governmental agencies for particular industries under specific conditions, allows for businesses in most countries to understand community impact and develop procedures to continually evaluate and

improve operations to benefit the society in which it is located and the bottom line for the company. While the ISO has its own recently published, broad guideline for risk management, ISO 31000, a non-certification standard released in 2009, it is another standard on which this analysis will center. In mining, the standard that exercises the aforementioned principles is ISO 14001, "Specification of Environmental Management Systems."

Part of the ISO 14000 series, the most recent edition of the 2004 standard is geared toward a company's environmental management system which enables participants to freely incorporate the standard's principles and develop solutions to potential impacts to the environment. These developed systems will vary greatly with industry. Often, this conformity is subject to a third party check that is not only familiar with the industry, but also the standard. More briefly, it permits companies to develop measures to an improving system that allows for review and maneuver, this is a reasonable approach to developing an SOP against explosives-related threats as well. While the requirements are numerable, the gist of the program is to give a site the freedom to initiate its own measures, but it allows for a system of checks and balances by subjecting the program to continuous improvement and review by qualified professionals. Most participants in ISO 14001 cite tremendous advantages in implementing the standard.

A system that creates more work and uses additional resources but lowers cost seems counter intuitive. However, many companies participating in ISO 14001 have cited significant results in their investment, not to mention the benefits received once the public acknowledges that a strict standard has been successfully implemented under self-regulation, all the while exceeding legislative requirements. It only makes sense, as discussed in Section 5, to appropriately inform the community about the company's safeguards. As noted, "the benefits…are greatly diminished if customers and the general public are not made aware of this achievement" (Morris, 2004). Research has shown that most companies agree with this opportunity to self-regulate, although many, like the chemical sector working under CFATS, still have questions about implementation.

A study published in 2003 by the University of North Carolina at Chapel Hill, investigated the tradeoff of participating in environmental management systems. Included

in the findings was “positive observed impacts on the economic performance of these participating facilities” and more than half expressed a reduction in liability (UNC Department of Public Policy, 2003). These investments go further if a facility recognizes that the prevention of a BP-type disaster will pay even more. Other organizations use this same technique of self-compliance and goal-setting as a means of rendering safe inherently dangerous procedures. These comparisons suitably fit the mitigation of explosives-related threats in that the consequences, as stated earlier in the risk management models, are worth an authentic training mechanism that implements a change in human behavior and attitude.

3.2.2. International Cyanide Management Code. In keeping with the environmental theme, there are other organizations that rely on self-regulation. Like ISO 14001, the International Cyanide Management Institute (ICMI) outlines a voluntary program that maintains the safe manufacturing, transportation and use of cyanide for gold producers. Cyanide is a vital chemical used in the extraction of gold ore. The institute acknowledges the necessity of the chemical, like the necessity of explosives consumption in the U.S., and provides guidelines for users of the deadly chemical to improve the safety and health of workers and the environment. Again, the purpose of this comparison is to note consistencies and benefits in programs where there is a concentration of self-regulation with the consideration that a significant event can be devastating for the company. By drawing these comparisons, it is the intent of the author to bring to light that a facility can incorporate in its own SOP the same approach at a relatively low cost. This also makes a determination that if the facility fails to implement sensible ERA along with other countermeasures, the catastrophic outcome may be insurmountable.

The ICMI code is strikingly similar to the ISO 14001 standard. It urges participants to be “audited by an independent third party to determine the status of Code [sic] implementation. Those operations that meet the Code [sic] requirements can be certified. A unique trademark symbol can then be utilized by the certified operation. Audit results are made public to inform stakeholders of the status of cyanide management practices at the certified operation” (International Cyanide Management Institute, 2010). As with the ISO 14001 standard, this composition will not investigate fully the intricate

details of the code or any other standard, but will emphasize to facility managers the advantages of a similar approach. Obviously, there are the quantifiable benefits as well.

In a 2009 report, the ICMI code was evaluated by Dawn Garcia of SRK Consulting, who noted that "Benefits include lower risk operations, easier financial funding, and better community relations" (Garcia, 2009). Like the ISO 14001, it is commonly recognized that this level of transparency produces measureable advantages. However, to participate in the cyanide code, signatories must pay fees. Cyanide producers and users must conduct a cost-benefit analysis to justify participation in the program. Unlike BP, where billions of dollars barely dent the annual profit, this risk management technique must be put in the perspective of environmental damage or danger to human life; quite obviously the same focus for explosives attacks or incidences.

In 2009, an overflow from a solution pond containing sodium cyanide caused environmental and biological damage near a Ghana-based gold mine. In early 2010, the Environmental News Agency reported that the Newmont Mining would pay $5 million in compensation (Environmental News Agency, 2010). While there were no human deaths at Ahafo gold mine, the blemish on Newmont's reputation and perhaps the perception of the industry as a whole most likely will hurt worse than the slight cut from Newmont's more than a half a billion dollars first quarter earnings. This goes for BP and the oil industry as well. Coincidently, Newmont Mining Corporation is an ICMI code signatory receiving its Ahafo certification more than a year prior to the spill (Golder Associates Pty Ltd, 2008). According to the company, it was a technological failure, a malfunction in pond-level instrumentation, which led to the spill.

But what happens when a company has everything to lose? When compared to the loss of life and infrastructure from the 1995 Oklahoma City bombing, dead fish and plants have little clout. As stated in Section 1, a facility must maintain a diligent stance on site protection and utilize all reasonable means to protect its interests. When telecasted images of the bodies of small children, courageous first responders and other innocent civilians reach every American home, the dust will barely settle before investigations are launched and methods are questioned. There is a simple, low-cost approach to combat these devastating effects. And while owners and operators cannot guarantee the protection of all CIKRs, they can effectively harden the target to deterrence, and within a

reasonable budget, make ERA training applicable to their facility. This training must focus on altering the mindset of facility managers and first responders. It must allow flexibility in SOP development and empower security personnel to create realistic risk management models. Most importantly, ERA training must provide a clear foundation of recognizing explosives components and an understanding of the catastrophic effects of blasts.

4. EXPLOSIVES RECOGNITION AND AWARENESS TRAINING

Sparked by a combination of ideas, offering low-cost, comprehensive ERA training to law enforcement was the culmination of two experiences by the author. After discussing several events in which local law enforcement was exposed to potentially deadly explosives threats, an offer was made to organize and provide no-cost ERA training for police officers in the Rolla, Missouri area. Additionally, with the introduction of a new program at Missouri S&T, a Master of Science in Explosives Engineering, an effort was also undertaken to provide professional development to interested officers and non-commissioned officers (NCOs) from the United States Army Engineer School (USAES) located at Fort Leonard Wood (FLW), Missouri. These two endeavors are the origination of the methodology used to develop and communicate the need for ERA for first responders and military professionals who typically take roles in explosives-related threat response, mitigation or policy. This training is a fundamental contributor to eliminate complacency, develop the understanding of explosives threats through advanced education and create awareness of explosives that has normally eluded technological researchers.

In the fall of 2010, this researcher participated in an event sponsored by Northeastern University in Boston, Massachusetts, the home of the DHS COE for explosives-related threats, dubbed the Research and Industrial Collaboration Conference (RICC). The annual event is geared to bring together those in industry and academia to establish a better transition of technologies, most used in explosives detection, from college and national labs to the personnel in the field. Again, while this is a noble effort, the discouraging discovery made by this author is that most of the researchers have never witnessed a high-explosive detonation nor did they understand the concept of adequate standoff. A suicide bomber is capable of carrying explosives to cause death at hundreds of meters; explosives detection technology presented at the RICC touted standoff distances 50 meters or less. These researchers, like law enforcement, are in need of pertinent ERA training as to better develop the technology used by security professionals.

With the cooperation of Dr. Jason Baird, an explosives expert from Missouri S&T, ERA training at Missouri S&T was first introduced in the fall of 2009. Initially,

members of the Phelps County Sheriff's Department participated. The goal was to introduce basic knowledge of explosives and explosives devices to first responders operating in close proximity to the storage and usage of explosives. The topics include explosives regulations and guidelines, safety and handling, demonstrations of high and low explosives, initiators and initiation systems, special detonators, and hazards associated with explosives.

The ERA training quickly gained the interest of other departments and within the next year 30 officers participated from not only the sheriff's office, but also Rolla Police Department, Rolla Special Weapons and Tactics (SWAT), Missouri S&T Police (University Police), reserve training officers and two special agents from the FBI. There are ongoing efforts to bring agents from the ATF and employees from the Missouri State Emergency Management Agency (SEMA) as well as private industry professionals.

A survey was created in order to tailor the ongoing training to fit the needs of the participants. An example of the survey is shown in Appendix D. Survey analysis and results are discussed in the subsequent text in this section.

Each ERA participant was asked to complete a survey that required five quantitative responses and three qualitative answers. For the quantitative responses, a range from one to five was used to score the familiarity and interest of the participant, and the significance and effectiveness of the training. The applicability rating, ranging from one to five, is as follows:

1-not at all, 2-slightly, 3-somewhat, 4-very, 5-extremely.

For instance, if an officer is asked how familiar she is with explosives, circling the numeral one would indicate no familiarity and five would indicate expert familiarity. The following by-question analysis gives insight as to the pertinence of ERA to law enforcement officers who completed the survey.

Question 1: How effective was this training in reinforcing your knowledge of explosives?

Out of 29 responses the mean answer was 4.55. This indicates that training provided was between “very” and “extremely” effective. This shows that officers felt more educated and informed about explosives after completing the training. This awareness equates to a psychological advantage when responding to an explosives-related threat especially to those operating within close proximity to explosives storage and transportation

Question 2: How effective was the instructor(s) at presenting the material?

All participants with the exception of two indicated that the instructors were extremely effective in conveying the training topics. The average was 4.93, which shows that the trainers at Missouri S&T utilized proven teaching techniques and generated sufficient interest through demonstrations, discussion and visual aids. Current information, such as recent failed IED attempts within the U.S., was used to reinforce learning and make it applicable to the profession.

Question 3: At your present level, how significant are explosives-related threats?

Two-thirds of the participants scored a four or five, indicating that they believed within their current role, they will encounter an IED. The response average was a 3.93, showing that most respondents felt that there is a “very” significant threat of an explosives event occurring within their community. A reality confirmed by Question 8. Only one participant indicated a score lower than three.

Question 4: How interested are you in participating in more advanced explosives training?

The mean for interest in future training was 4.28. These results indicate that future advanced ERA training would be of significant interest to most trainees. One participant answered that there was no interest in more advanced explosives training.

Question 5: Prior to taking this training, how familiar were you with explosives and explosives-related threats?

Out of 29 responses, nearly all were scored a three or less. The average familiarity score was 2.1, indicating that this training increased the ERA for most of the attendees as this was their first significant explosives training session in which they felt more aware of the potential threats. Couple this with the results of Question 1, there is no doubt that emergency response professionals need and welcome the training.

The survey's three quantitative questions 6-8 were collected and categorized into major responses. This portion of the survey acts as a written AAR in which participants can provide written feedback to improve the training for the next group. Also addressed is the exposure of trainees to explosives-related threats.

Question 6: What are your recommendations for improving this course? Figure 4.1 shows the results.

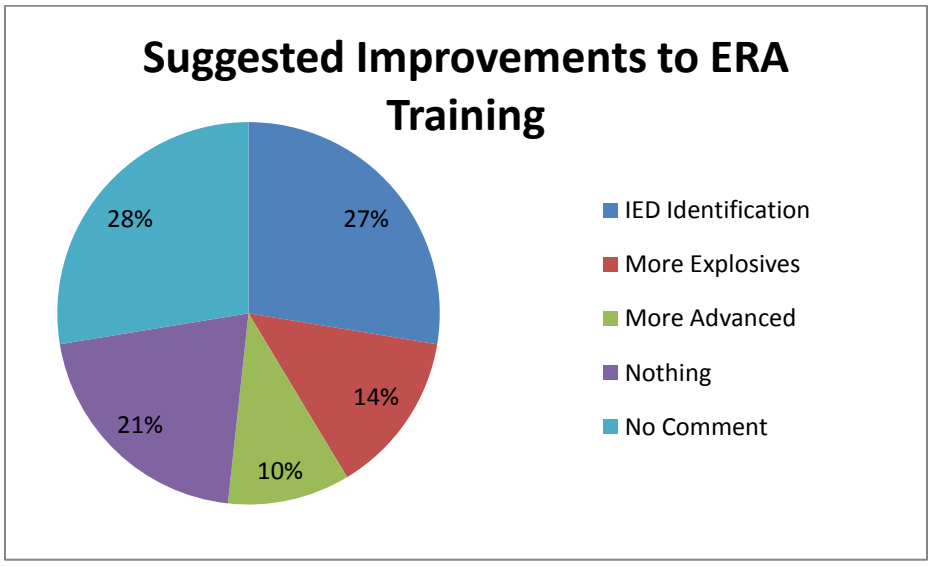


Figure 4.1. Suggested improvements to ERA training

Among the most popular suggestions for improving the training was the addition of more IED identification. Approximately the same number of respondents offered no comment to the question, or leaving the answer blank. If this answer is assumed to mean that officers have no suggestions and were satisfied with the course, then this answer could be married with the group who responded that nothing should be changed. If this is the case, then half of the trainees were completely content with the basic intent of the ERA training. The need for more IED training has been addressed by instructors and IED training simulators, smart cards and references have been added. However, this material has yet to be used in a training session.

In keeping with an authentic AAR, officers were also asked to provide feedback over what they felt should be kept in the training.

Question 7: What did you like most about the training? Figure 4.2 shows the results.

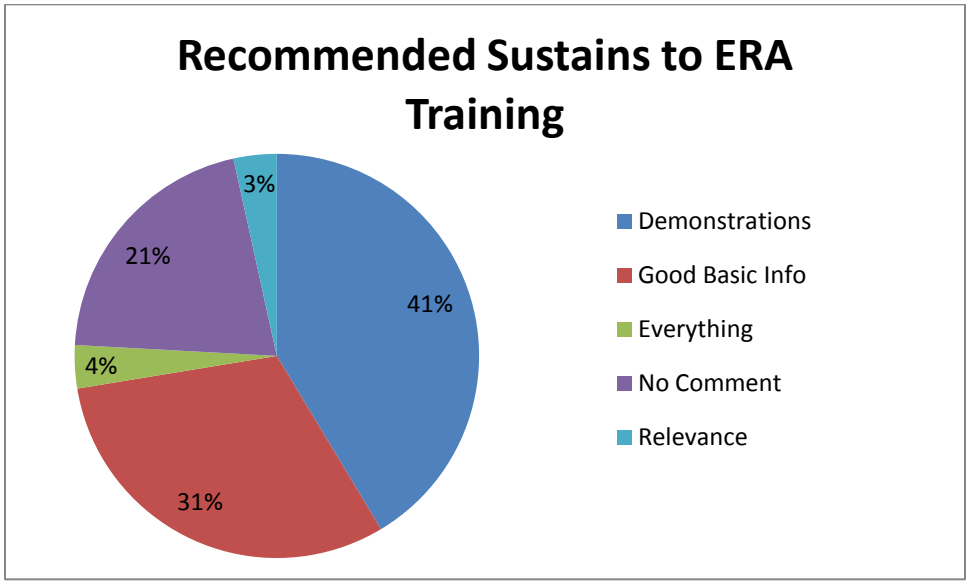


Figure 4.2. Recommended sustains to ERA training

Overwhelmingly, those participating in the training expressed that the explosives demonstrations were the most critical part of the course. Nearly one-third answered that

they felt the training provided a good foundation of explosives knowledge. Out of the 29 respondents, 21-percent offered no answer. Like Question 6, an officer offering no response either had no pertinent feedback or believed the training was adequate.

The final question of the ERA survey addresses the applicability of the training to those serving in a law enforcement capacity. The question was used to determine how often, if at all, local officials were faced with a genuine explosives-related threat.

Question 8: During your career, have you ever experienced an explosives threat on the job? Explain.

Out of 25 responses, 16 revealed that they have indeed come into contact with explosives devices or have been called to an explosives-related threat, the majority being bomb threats. That is 64-percent of first responders who have experienced a significant threat. Marry that number with the absence of previous explosives training and the conclusion is a grim reminder that after so many explosives attacks and threats, the nation's initial response personnel are still not equipped with the knowledge they need to protect the community and themselves. What's more, once discussing particular cases, it was revealed that oftentimes inexperienced officers would carelessly handle and store explosive devices and even transport the "bomb" in the same vehicle as passengers. There were other significant discoveries as well.

During informal discussions with trainees, another important observation was made. Several local officers were unaware of the amount of explosives stored on or near campus and many did not know if the university's explosives storage was part of the local emergency response plan. This pertains to law enforcement officials' perception that they will likely face an explosives-related threat. Even more staggering is the thought that firefighters may also be ignorant of the aforementioned observation. Like a police officer pursuing the source of gun fire, an active shooter, firefighters are trained to extinguish fire. But if these brave souls are unaware of the fact that the fire they are attempting to extinguish is in close proximity to explosives storage, the catastrophic result is many lives lost and many more rescuers subjected to the same fate. This has happened before.

In November 1988, Kansas City, Missouri firefighters responded to an early morning arson fire on a construction site. The construction company was using a blasting agent comprised of ammonium nitrate and fuel oil, commonly known as ANFO. Although initial emergency response calls indicated that explosives were on site and possibly ablaze, the exact location of the magazines containing the explosives was not known. Firefighters were also unaware of improper storage prior to the response; which included unacceptable safe distances to nearby structures and thoroughfares and between the two magazines that exploded. When firefighters arrived on scene to battle the blaze, two explosions consisting of tens of thousands of pounds of ANFO and dynamite claimed the lives of all six responders. In a subsequent report by the United States Fire Administration, investigator Jack Yates concluded that if the seasoned firefighters had known the exact location of the explosives and the magazines were marked, this tragedy perhaps could have been avoided (Yates, 1989). Although there were no marking requirements for the magazines themselves, and considering the fire would have destroyed the placard anyway, just by having the fire department visit the site and discuss the company's emergency response plan involving explosives would have led to greater communication, a fundamental for ERA.

As discussed in Section 5, ERA is a basic component of a more elaborate site security model that includes all relevant responders. The ERA instructors in this particular instance encouraged law enforcement to become better familiar with emergency management directors and the local emergency management plan. With ERA training, first responders can be better prepared psychologically for appropriately dealing with such instances.

There is a current effort to expand ERA training to other pertinent agencies. Besides law enforcement, fire departments and other emergency relief workers would benefit from such training. The goal is to provide an explosives education to those who may be exposed to such threats. ATF offices and the Missouri State Emergency Management Agency (SEMA) have expressed interest in taking part in the ERA classes. There has also been expressed interest by private security consultants as well. To date, no courses have been scheduled for these entities. However, great strides have been taken to make the advanced explosives education available to the U.S. military.

Also a part of the ERA training was providing Officer Professional Development (OPD) to components of the USAES at FLW. This initial effort was the development of a previously unidentified focus group for the DHS ALERT education initiative. However, the briefings spawned a storm of interest in the recently approved Explosives Engineering Master of Science degree from Missouri S&T.

The first session was conducted with approximately 50 officers and NCOs with the 1st Engineer Brigade. Traditional combat engineers are tasked with explosives demolition, breaching and providing explosives clearance services to supported units. The ERA training consisted much of what was offered at the university as well as presenting ideas of explosives implementation and explosives products. The intent was to establish advanced explosives education to future retirees who would potentially pursue employment with the federal government. As mentioned in previous sections, there are few colleges in the world that can provide this training at an advanced level. In its original capacity, ALERT was designed to recruit such professionals in order to enhance the nation's pool of explosives professionals. While the goal was to incorporate the intent with high school and college students, this researcher organized the military effort to establish a more cooperative explosives education relationship with the USAES. The initial training was attended by commanders at all levels of the brigade and, while there are no official surveys or reviews, received tremendous positive feedback which inspired an OPD with the USAES commandant Brigadier General Bryan Watson. General Watson provided an additional 20 soldiers to attend the same training which resulted in astonishing interest in the explosives engineering program. These participants were oblivious to most of the resources and capabilities of the department, although located less than 30 miles away. There are ongoing efforts to provide a degree track for soldiers interested in the explosives engineering program and it is anticipated that the original intent of the ALERT initiative will be met.

The next step of ERA is to incorporate the training into a genuine site security plan. Although site security personnel have not attended the ERA training discussed in this document, it is vital that those tasked with guarding infrastructure undertake a role in ERA training. This plan is detailed further in the following section.

5. SITE AWARENESS OF FIRING AND EXPLOSIVES DEVICES

Facilities must have the means of routinely verifying their site protection plan. A location, upon its own risk management process, can develop a tactical pilot and then spot check its progress by conducting realistic and applicable exercises. These exercises must be periodic and practical and include a proper evaluation or, as in the military, an AAR. The AAR is used to identify sustains and desired improvements to the training without targeting individual participants. It clearly defines the goal and details the process of execution to determine if pre-exercise goals were met. The AAR includes all participants. Without vital participant feedback, the facility may not meet the continuous improvement requirement as outlined in Section 3.

This program suggests the implementation of human factor solutions to combat bunker mentality and complacency. To alleviate concerns with organizational complacency, employees involved with a task must be routinely challenged. Each month, this author, armed with a uniform and military identification card, is enthusiastically waved onto a Missouri military installation. The guard charged with recognizing threat has become so removed from danger that the identification card is rarely checked. This mentality exists because the guard is not tested and 9-11 has long passed.

When the consequences and threat potential, as discussed in Section 3, weigh heavy on those charged with protection, then a climate of preservation will prevail, but there also must be a focus on crisis management. There are several approaches to motivate participants to remain vigilant in their task. During a 2005 tour supporting Operation Iraqi Freedom, this author was part of a team tasked to train coalition forces in combat operations. The first week in the area of operations, a complex ambush resulted in the deaths of five Iraqi soldiers. Their vehicle, partially destroyed by an IED, was splattered with the blood of the brave soldiers. As a constant reminder of the inherent threat in combat, the Iraqi commander parked the truck near the entrance of the small base. Everyone entering or exiting the base could see the truck and was continuously reminded of the peril. While this is a drastic and grim example, this type of visual reinforcement can be used in other industries. There is reinforcement through repetition training as well.

The military typically trains recruits through redundancy. Warriors are created through constant exposure to repeated tasks, formally known as "battle drills." The purpose of a battle drill is to instill into a soldier an instinctive reaction under adverse circumstances. This is the military approach to implant crisis management skills to the lowest level employee thus ensuring mission success. This realistic trained response incorporates critical thinking skills in order to preserve the mission and resources and allows for soldiers to continue the mission regardless of location, leadership or other influences and surprises. In his book *On Killing*, retired Army Lieutenant Colonel Dave Grossman and former West Point psychology professor states that the military objective during the American Civil War was to use "mind-numbingly repetitive drill" to "turn a soldier into a small cog in a machine…ensuring the he would do his duty on the battlefield" (Grossman, 1995). Grossman stresses that this psychological mechanism, a significant emphasis in the military, is a product of recreating realistic conditions in addition to the redundancy, and is a method used in other professions as well. He says the technique is "used when training firemen and airline pilots to react to emergency situations: precise replication of the stimulus that they will face (in a flame house or flight simulator) and then extensive shaping of the desired response to that stimulus. Stimulus-response, stimulus-response, stimulus-response. In the crisis, when these individuals are scared out of their wits, they react properly and they save lives" (Grossman, 1995). Perhaps the most notable example of this viewpoint is the emergency aircraft landing in the Hudson River.

In January 2009, Captain Chesley Sullenberger, coincidently a former U.S. Air Force pilot, conducted the emergency landing of a U.S. Airways passenger jet after multiple bird strikes to the aircraft's engines. Following the landing, Sullenberger, whose voice transmissions to both flight control and the passengers were remarkably calm throughout the ordeal, only exited the plane after checking the cabin twice. The pilot responsible for saving 155 lives that day later admitted in an interview that Grossman's observations are with merit. The hero told interviewer Katie Couric "It was the worst sickening, pit-of-your-stomach, falling-through-the-floor feeling I've ever felt in my life" and credited a lifetime of education and training as the deciding factors (CBS News, 2009). The same methods of realistic, repetitive training that prepared Sullenberger must

be included when directing site security operations. There also variety contained within the mission.

To alleviate boredom, rotational work must be emplaced. An event must occur and be unpredictable to test the security staff and emergency response personnel. Site security personnel must be tested within the scope of their duties. Additionally, the preferred method of sustainability is via positive reinforcement, such as in canine training, rather than negative repercussions. To achieve complete site awareness of firing and explosives devices (SAFE-D), an all-inclusive approach must be established. This section provides a five-phase outline for a suggested program in which facility managers can employ, but does not serve to address every aspect of concern specific to every industry. This psychological training model begins with ERA in the "familiarization" phase; incorporates knowledge and practical exercise in the "application" phase; develops sensible SOPs with third-party review in the "validation" phase; conducts comprehensive review during the "evaluation" phase; and finally utilizes the "retention" phase for continuous focus on the protection plan. An easy acronym to recognize the tool: Facilities must do themselves a "faver" [sic] by implementing SAFE-D. A comprehensive decision-making matrix for SAFE-D implementation is included in Appendix E. The SAFE-D cyclical model in shown in Figure 5.1.

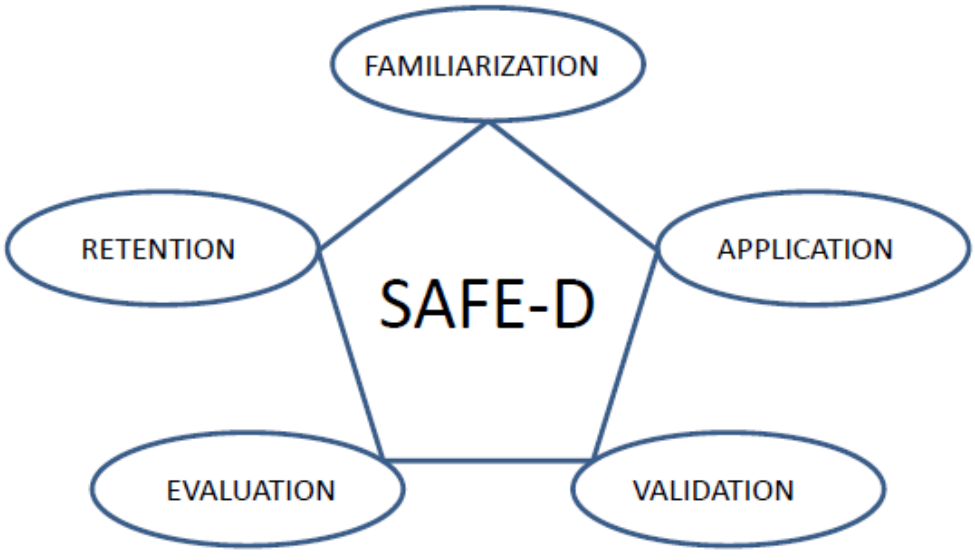


Figure 5.1. The SAFE-D model

Phase 1 focuses on obtaining ERA training for appropriate personnel. Depending on the institution, the facility managers should also be familiar with the LERP, especially for facilities storing explosives. As discussed in Section 4, local police officers were not aware of the storage of explosives in their community nor could they recall the emergency management director for the city or the LERP. To establish a legitimate risk management plan and SOP, all of those involved in disaster response must come to the table. The time to meet these officials is not when there is an explosives incident. Rather, initial ERA training should include site security personnel and the local and state agencies responsible for supporting the facility in the event of an explosives attack. In keeping with the goals outlined in Section 1.2, providing ERA training to all of those potential actors in a location in close proximity to the potential target allows familiarization and networking functions to occur during the training. Officials can take this time to exchange contact information, ideas and further critique the LERP as it pertains to the facility. Much of this will naturally occur during informal discussions, but the initial ERA training is not only to serve as a foundation for explosives and component awareness, but also as a conduit for original thought and information sharing. The initial training should be designed to put names to faces and identify who should respond to an explosives-related threat in order to prevent crowding of onsite personnel. This point is revisited in Phase 5.

Considering many emergency response personnel have little experience with explosives, as seen in the surveys of the ERA training conducted at Missouri S&T, the initial training should encompass basic explosives training lasting 16-24 hours. Principles, like those listed in Section 4, should act as a transitional function. The training must bring the threat to the participants by using realistic material to which the trainees can relate. Baird's ERA session accomplished this goal. The explosives educator begins the training event by showing video of international law enforcement improperly handling IEDs. While graphic, the video serves to remind police officers of the consequences carelessness can cause. Additionally, demonstrations of high explosives are also used to fortify the point that just a small amount of explosives can have a major impact in close proximity. By witnessing firsthand the power of a high explosive, officers can put into perspective future training scenarios where proper standoff can be

implemented. Initial ERA training should be annually reinforced with no less than an 8-hour refresher course. This is discussed in Phase 4.

The next phase is the practical exercise portion of the SAFE-D program. It encompasses all the training acquired by security professional and first responders and brings together a realistic test of the effectiveness of the training. Each training scenario must be followed by an immediate AAR to ensure timely feedback of the participants. Security professionals and first responders can alternate hosting exercises, but each training event should always occur within the professionals' operational scope and in the location of the potential attack or incident. Training aids can consist of make shift IEDs or suspicious components of explosives devices. Exercise participants must focus on applicable explosives counter measures and effective response. The key is to prevent the detonation, and not to necessarily respond to a blast. Drawing again on the military, these exercises can be community based and phased into a crawl, walk, run application; meaning that a briefing on the exercise should be orally delivered to actors and an onsite walk-through should occur prior to a live exercise. This is when the ERA training should be incorporated into site security and SOPs originate. The exercise pilot should be a standard event which pertains to the facility. More elaborate schemes can be devised from the AARs and SOP revisions occurring in the evaluation phase.

In the third phase, managers will use lessons learned from the exercise and incorporate improvements and seek additional resources. The SOP will be continuously refined as threats vary, but this should be the main effort in developing a facility's original, and most complete, SOP. The most critical aspect of SOP guidelines is communicating the standard and distributing to all levels the owner's intent as it pertains to combating explosives-related threats. While common sense is a great tool for onsite security professionals to mitigate their own risk, managers should seek additional low-cost resources. These can come in the form of academic expertise, industry partner review and governmental input that validates the organization's efforts. During this phase, the facility should attempt to deliver a final product that addresses fully the risk management process and hazards identified as well as any special criteria that each location must consider. For example, for a plant located in close proximity of school,

additional criteria would include school hours and traffic. Once these guidelines have been reviewed appropriately, it is time to test the full product.

Phase 4 is a training evaluation. Site operators will use the refined SOP, current threat and updated intelligence, and pending a third party audit, to retrain as necessary. This is the time to develop a routine method of testing security plans and personnel. The testing must develop several criteria in order to be successful, it must:

- Be unpredictable and unannounced
- Test within the scope of the training
- Assign no personal blame for security flaws
- Be measurable
- Ensure feedback is timely
- Allow for variance
- Be incentive based

In the military, many of these approaches are undertaken in evaluating battle drills. Once a platoon or squad has rehearsed continuously the applicable drill, variations are added to enhance the crisis management potential of the soldiers. One of the favorite approaches for first line supervisors is to remove the traditional leader from the training and evaluate the remaining troops' ability to continue the flow of the mission with minimal interruption. In just one battle drill, a leader can evaluate all of the criteria mentioned above and follow up the training with an AAR that addresses pertinent successes and shortcomings and assigns those to the method and not the individual soldier. Incentives in the military often come in the form of general competiveness and satisfaction of being a well-trained, ready-for-combat unit. Soldiers respond to training evaluation the same as winning a football game. Except the triumph in battle certainly has greater weight. This approach again allows for each facility to develop its own standard, but there are simple approaches to consider.

The military uses "spot checks" to ensure soldier readiness. This is a sporadic check of equipment or knowledge that is assumed to be readily available. However, the scope guarantees a soldier will not be tested on something he is not expected to know. The psychological effect of having a leader randomly perform this function keeps the soldier aware. Site security personnel must undergo the same scrutiny, however, like the

soldier, should not be tested on something outside of ERA or the scope of the site security training. Once these tests take place, the site's security teams will develop the same "esprit de corps" as a platoon and challenge each other to be diligent for nothing more than bragging rights. The feeling of success gained by these teams will pay extraordinary dividends and challenge others to excel. In contrast, the identification of defects must not be personal. One security guard missing a simulated IED does not constitute a failure in the entire system or a lack of concern from that individual. The collective process should be addressed and not the blame game. Incentives can also be used.

Perhaps the most significant, driving force in a time of peace is money. However, in a time of war, preservation of life and property become more prevalent. Like investing in risk management, a company is best served investing in the prevention of injury rather than the compensation to hurt employees. The same applies to SAFE-D. Even small non-monetary bonuses, for instance a pool of company merchandise or a company certificate, convey the pertinence of the program. Having time off will work as well. Another approach in the Army is to reward attentiveness. For example, a unit's maintenance program may test individuals by purposely creating mechanical flaws on a vehicle. Soldiers identifying and correcting all of the flaws may be permitted to leave work early or may simply be recognized in the presence of their peers and leaders. This is effective and contagious, as long as the soldiers are astute to the procedure and tested within the scope of their ability. Like previously discussed scenarios, incentives, along with the other criteria, should be based on the company's needs and project a continuing investment in site security from explosives-related threats. A well-trained security force is comparable to any detection measure a facility can purchase.

The fifth phase is the retention phase. Tests and scenario-based exercises will continue as deemed necessary. Local law enforcement must participate in the training as a means of total understanding of explosives-related threats. As well, this should include other pertinent emergency response possessing a genuine role in the training. As seen with Eric Rudolph, the Atlanta bomber during the 1996 Olympics, an actual explosive event may just be a method of gathering more targets for a more intense detonation. Agencies can alternate training responsibility and take turns hosting significant training

events. During this phase, ERA refresher courses are given and daily intelligence is addressed in risk management. Anytime a pertinent change in physical or operational structure occurs within the facility, the SOP must be revisited and altered plans must be conveyed again to all members who hold a stake in the site's protection. As discussed Section 3.2, this is a time for review and improvement, just as the environmental management system implies. These adjustments could be additions or alterations to the plan, such as investing more money into equipment or canines. As well, it is a time to inform the surrounding community that significant safeguards are in place to protect the infrastructure and the population.

As mentioned, the SAFE-D program, although strictly based on explosives-related threats, is not intended to cure entirely a facility's security woes. Like the Army's approach to risk management, it is indeed designed to teach security professionals "how to think" and not "what to think." Elaborate detection systems are designed to present possible risks as a computer may interpret the threat. This method takes away the initial gut instinct and critical thinking process the human factor brings to the table. SAFE-D is also not a substitution for standoff barriers and detection systems. Rather, it is designed to be coupled with existing technologies and protective measures. It gives a facility the opportunity to design low-cost, sensible solutions to what consultants may claim is a complex problem. Complacency is an ongoing problem for site managers. SAFE-D is a constant reminder to first responders and security forces that the danger is real and unpredictable.

6. CONCLUSIONS

The United States obviously has a legitimate policy in place to deter and detect explosives-related threats. Each year, massive spending is allocated to provide the force with the most sophisticated sensor equipment and barriers. However, absent from the well-intentioned strategy is a cost-effective training program that focuses on explosives recognition and awareness and not just the technological aspect of detection and protection. This psychological shortcoming, albeit a simplistic one, has created a substantial effort to invest hundreds of billions of dollars into systems without marrying that bankroll with a common-sense approach to train security professionals on the basic principles of explosives-related threats. SAFE-D can enable first responders and facility managers to create and sustain their own policy; one of which is free of government reliance and error.

Countless companies today offer consultancy services for those willing to pay for a relatively sensible approach to IED detection. As part of these services, IED training kits and lessons on standoff protection are included as necessary components of ERA. SAFE-D, a comprehensive approach pertinent to any location grants the liberty for each facility to assess its own risk and apply dynamic SOPs in a continuous manner; all the while empowering the facility to develop low-cost solutions to site protection. These third-party-review methods, as specifically outlined in the previous text, already exist in other industry and can be appropriately adapted to fit the needs of the facility. Additionally, better crosstalk between interested parties must be incorporated.

A company cannot rely solely on the federal establishment or a single technological solution. Like the attempted Time's Square bombing in 2010, in which an attentive police officer noticed a smoking device inside a vehicle, ERA must trickle down to the lowest level, where those professionals are likely to come into contact with the threat. By knowing just the fundamentals of explosives, that police officer will not only be able to recognize the threat, but also would understand the potential of the blast and the necessary evacuation area and can ultimately prevent devastating blast effects like those in the 1988 explosion in Kansas City. By observing components of the explosive device, that police officer may be able to make a determination as to whether the threat is

legitimate or a distracter for a secondary event. It makes little sense for an executive to attend the training outside of an assessment perspective. Psychologically, security professionals must know they are being equipped with not only the best gear, but also updated knowledge.

7. RECOMMENDATIONS FOR FUTURE WORK

The next logical rung for research progression would be to test SAFE-D at a legitimate facility and expand ERA to a network of professionals with a shared interest in explosives-related threat protection.

Any company, school or hospital, has a legitimate concern for site safety. To move forward, the SAFE-D outline must be tested under a voluntary basis for the applicable facility. Site security managers can take these principles and incorporate the phase into the SSP, the risk management process and their own SOPs. Each facility can task employees, who are already the experts on the hazards present in the work environment, to produce a genuine plan that begins with ERA and validates under a collective training exercise involving local and state officials. Further, SAFE-D can be a supplementary program to a site's already functioning security plan. Operators can take phases of the plan and adjust them to fit specific needs intrinsic to the site.

Perhaps the easiest aspect of this research to advance is the ERA training. Creating a network, in which much of the leg work has already been started, to bring explosives-related threat training from governmental entities and academia to not only first responders, but significant security contractors tasked with protecting CIKR and the nation's most valued resources, people, is an obligation. The training must be available to school resource officers, law enforcement and security forces tasked with guarding vulnerable patients. As seen in Russia, this training can prove invaluable in thwarting future attacks.

Lastly, to expand fully the advantages of SAFE-D, it must be incorporated into the LERP for each community. For example, for each facility concerned either with housing significant numbers of employees or visitors, or those involved with CIKR, there must be a development of SOPs that involves emergency response. SAFE-D allows for all incident responders, whether manmade or natural, to come together in rehearsal rather than waiting for the tragedy to transpire to establish vital communications and procedures for a broad-response catastrophe.

APPENDIX A

NIPP'S TABLE 2-1: SECTOR-SPECIFIC AGENCIES AND ASSIGNED CIKR SECTORS

Sector-Specific Agency	Critical Infrastructure and Key Resources Sector
Department of Agriculture[a] Department of Health and Human Services[b]	Agriculture and Food
Department of Defense[c]	Defense Industrial Base
Department of Energy	Energy[d]
Department of Health and Human Services	Healthcare and Public Health
Department of the Interior	National Monuments and Icons
Department of the Treasury	Banking and Finance
Environmental Protection Agency	Water[e]
Department of Homeland Security *Office of Infrastructure Protection*	Chemical Commercial Facilities Critical Manufacturing Dams Emergency Services Nuclear Reactors, Materials, and Waste
Office of Cybersecurity and Communications	Information Technology Communications
Transportation Security Administration	Postal and Shipping
Transportation Security Administration *United States Coast Guard*[f]	Transportation Systems[g]
Immigration and Customs Enforcement, Federal Protective Service	Government Facilities[h]

[a] The Department of Agriculture is responsible for agriculture and food (meat, poultry, and egg products).

[b] The Department of Health and Human Services is responsible for food other than meat, poultry, and egg products.

[c] Nothing in this plan impairs or otherwise affects the authority of the Secretary of Defense over the Department of Defense (DoD), including the chain of command for military forces from the President as Commander in Chief, to the Secretary of Defense, to the commander of military forces, or military command and control procedures.

[d] The Energy Sector includes the production, refining, storage, and distribution of oil, gas, and electric power, except for commercial nuclear power facilities.

[e] The Water Sector includes drinking water and wastewater systems.

[f] The U.S. Coast Guard is the SSA for the maritime transportation mode.

[g] As stated in HSPD-7, the Department of Transportation and the Department of Homeland Security will collaborate on all matters relating to transportation security and transportation infrastructure protection.

[h] The Department of Education is the SSA for the Education Facilities Subsector of the Government Facilities Sector.

APPENDIX B

CSETAT INFORMATION FLYER

This workshop is free of charge.

The DHS Chemical Sector Specific Agency (SSA) offers a series of one-day Chemical Sector Explosive Threat Awareness Training (CSETAT) training sessions nationwide to chemical facility security officers.

Who Should Attend

Chemical Facility Security Officers, Chemical Sector Security Professionals, and stakeholders. This workshop provides exposure to essential elements pertaining to the threat of improvised explosive devices (IED's) and vehicle-borne improvised explosive devices (VBIED's). The objectives benefit security professionals dealing with explosive incidents and the chemical sector's ability to deter, prevent, detect, protect against, and respond to attacks that use IED's. The workshop illustrates baseline awareness, prevention and mission essential actions that reduce vulnerabilities and counter the threat, along with collaborating information sharing resources to improve preparedness.

The workshop will provide the participants with information to:

- Identify options for consideration
- CFATS Update
- Improve understanding of each agency's capabilities and limitations
- Communication, Cooperation, and Collaboration

2010 Scheduled Trainings Were Held In:

Dallas, TX, Tampa, FL, Plaquemine, LA, St. Louis, MO, Seattle, WA, and Buffalo, NY.

2011 scheduled trainings will be announced in late 2010.

Please email chemicalsector@dhs.gov for a schedule or for more information.

Participants will receive a Certificate of Participation upon completion of the course .

APPENDIX C

EXAMPLE RISK MANAGEMENT WORKSHEET

RISK MANAGEMENT WORKSHEET

1. Organization and Unit Location:	2. Page		of	
3175th Chem Co		1		1

3. Mission/Task:	4. Begin Date:	5. End Date:	6. Date Prepared:
Conduct Range Firing (Includes Transportation to and from Range)	080800 Sep 07	091700 Sep 07	071405 Sep 07

7. Operational Phase in which the Mission/Task will be conducted:
Throughout training phase.

8. Tasks	9. Identify Hazards	10. Initial Risk Level	11. Develop Controls	12. Residual Risk Level	13. Implement Controls ("How To")	14. Who/How Supervised
Transportation to /from range.	Driver Fatigue	L	Ensure driver gets adequate rest.	L	AR 385-55,Prevention of Motor Vehicle Accidents.	Driver – Self
	Traffic/Congestion	L	Drive slower and defensively.	L	Be aware of traffic flow	Driver – Self
	Weather Conditions (rain on road)	L	Drive slower than posted speed limit.	L	AR 600-55,Army Driver and Operator Standardization Prg.	Driver – Self
Range Firing	Inexperienced firers.	M	Instruct and demonstrate: (1) PMI, (2) Fundamentals of BRM and (3) How to properly perform SPORTS.	L	Give classes and do hands-on practical exercises.	All firers and leadership.
	Negligent discharge	M	Positive control of all weapons; weapons touched only when instructed to/always cleared and on safe. Have right and left limit firing stakes.	L	Ensure safeties rod and clear all weapons between firing cycles. Check for wpn safety. Show R/L firing limits.	All firers; safeties and cadre monitor.
	Equipment failure	M	Conduct a safety inspection of weapons and equipment prior to training.	L	Perform function check prior to firing/rod and clear all weapons on and off the firing line.	Range Safety Officer will inspect.
	Heat Injury or Dehydration. Inclement weather	L	Monitor Heat Index, advise all to drink water at frequent intervals, and know location of water points, cover for storms	L	FM 21-10 and safety brief.	CLS on site. Cadre monitor weather and PI will supervise water.
	Medical emergency	M	Combat lifesaver present/directions to GLWACH hospital.	L	Ensure all cadre know emergency procedures for evacuation.	All cadre
	Wildlife, insects and plants.	L	Brief firers to avoid wildlife, insects and plants. Use insect repellent. Have site inspected prior to cadet arrival.	L	Continue to monitor wildlife.	Cadre monitor. Use buddy system.

15. Determine Overall Mission/Task Risk Level After Countermeasures Are Implemented: (Circle Highest Remaining Risk Level) **LOW (L)** **MODERATE (M)** **HIGH (H)** **EXTREMELY HIGH (E)**

16. Medical Support: Advanced Trauma Life Support (ATLS) is required within 1 hour. On-site Medical Support provided (Circle one): Medic (Combat Lifesaver) ARC/NSC First-Aid Responder None

17. Prepared by: (Rank, Last Name, Duty Position)	18. Reviewed by Action Officer/Commander: (Rank, Last Name, Duty Position and Signature):
James Hawkins, SFC, 2nd PLT Chem Recon	Eric Kuenke, CPT, 3175th Chem Co

19. Risk Decision Authority (Signature Block and Signature):	**Extremely High Risk**: Theatre Command **High Risk**: CG or DCG **Moderate Risk**: Bn/Brigade Cdr **Low Risk**: Co. Cdr.
Eric Kuenke, CPT, 3175th	

APPENDIX D

ERA TRAINING SURVEY EXAMPLE

Explosives-Related Threats, Recognition and Awareness
Dr. Jason Baird, Associate Professor Missouri S&T

Please indicate Rank/Position/Agency_____

Circle one: Public/Private

For numerical ratings, circle the applicable score:

1-not at all, 2-slightly, 3-somewhat, 4-very, 5-extremely

---

1. How effective was this training in reinforcing your knowledge of explosives?
   1 2 3 4 5

2. How effective was the instructor(s) at presenting the material?
   1 2 3 4 5

3. At your present level, how significant are explosives-related threats?
   1 2 3 4 5

4. How interested are you in participating in more advanced explosives training?
   1 2 3 4 5

5. Prior to taking this training, how familiar were you with explosives and explosives-related threats?
   1 2 3 4 5

6. What are your recommendations for improving this course?
   _____
   _____

7. What did you like most about the training?
   _____
   _____

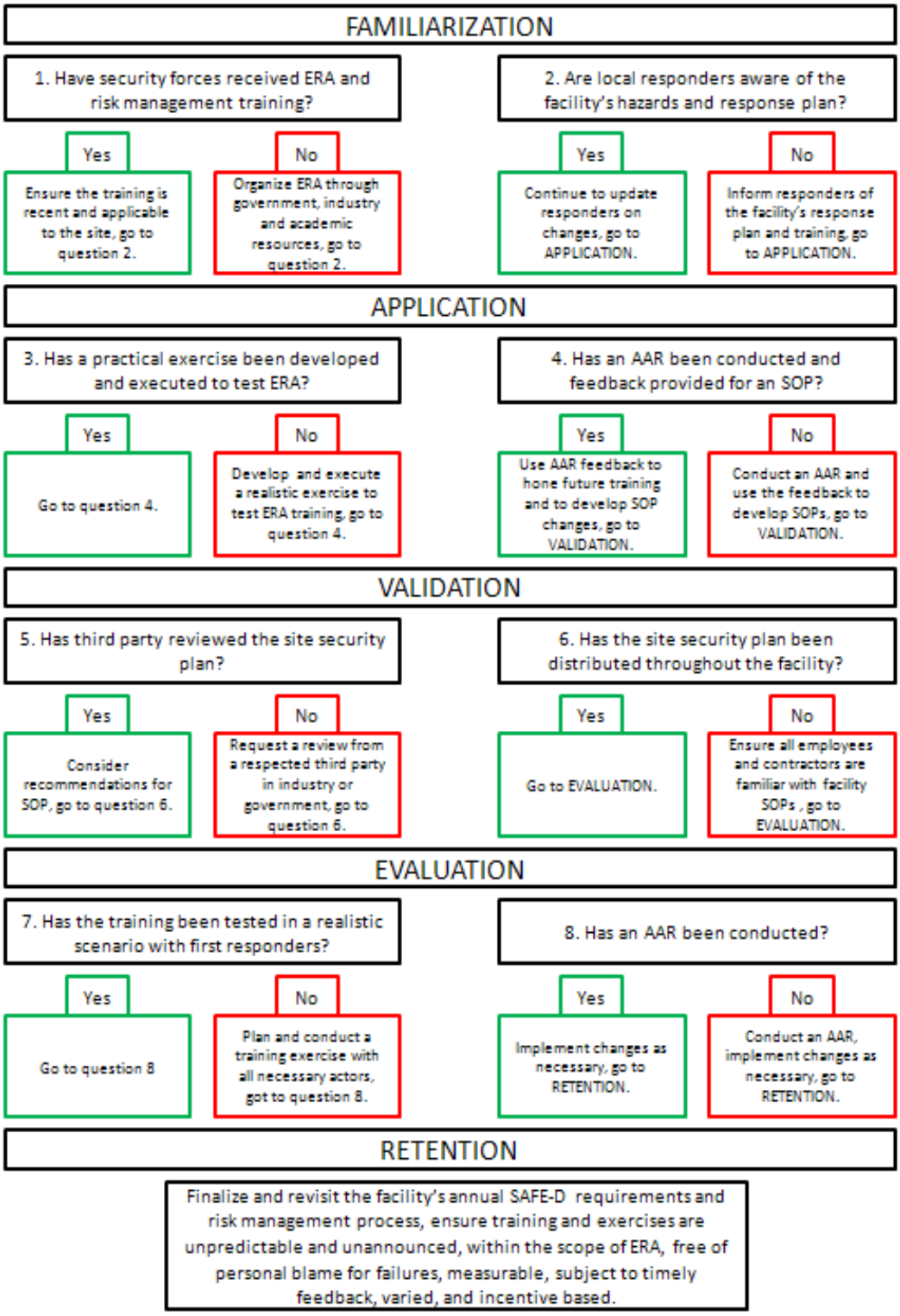
8. During your career, have you ever experienced an explosives threat on the job? Explain.
   _____
   _____
   _____
   _____

Please use the space below for any additional comments. For information regarding explosives training, email Buck Hawkins at buckhawkins@hotmail.com, or call 573-201-4052.

APPENDIX E

SAFE-D IMPLEMENTATION GUIDE

Facility SAFE-D Implementation Guideline



BIBLIOGRAPHY

Borja, Elizabeth. 2008. *Brief Documentary History of the Department of Homeland Security 2001-2008.* Washington D.C. : History Associates Inc., 2008.

British Petroleum. 2010. Press Releases. *BP.* [Online] BP, September 29, 2010. [Cited: October 6, 2010.] http://www.bp.com/genericarticle.do?categoryId=2012968&contentId=7065250.

Bureau of Alcohol, Tobacco, Firearms and Explosives. 2010. Accelerant and Explosives Detection Canines. *ATF.* [Online] U.S. Government, 2010. http://www.atf.gov/explosives/programs/explosives-detection-canines/.

Bureau of Alcohol, Tobacco, Firearms and Explosives. 2010. Bomb Arson Tracking System. *Bureau of Alcohol, Tobacco, Firearms and Explosives.* [Online] U.S. Government, 2010. [Cited: September 20, 2010.] http://www.atf.gov/applications/bats/.

—. 2010. Certified Explosives Specialists. *Bureau of Alcohol, Tobacco, Firearms and Explosives.* [Online] U.S. Government, 2010. http://www.atf.gov/explosives/programs/certified-explosives-specialists/.

—. 2010. Explosives Enforcement Officers. *Bureau of Alcohol, Tobacco, Firearms and Explosives.* [Online] U.S. Government, 2010. [Cited: September 20, 2010.] http://www.atf.gov/explosives/programs/explosives-enforcement-officers/.

—. 2007. *Federal Explosives Law and Regulations.* Washington D.C. : U.S. Department of Justice, 2007.

—. 2002. *Safe Explosives Act Fact Sheet.* Washington D.C. : U.S. Government, 2002.

CBS News. 2009. CBS News. *60 Minutes.* [Online] CBS News, February 2009, 2009. http://www.cbsnews.com/stories/2009/01/30/60minutes/main4764852.shtml.

Chemical Sector Security Summit. 2010. *Summit Gazette.* Baltimore : DHS, 2010.

Department of Homeland Security. 2010. 2010 Chemical Sector Security Summit. *Homeland Security.* [Online] U.S. Government, July 14, 2010. http://www.dhs.gov/files/programs/gc_1176736485793.shtm.

—. 2010. Chemical Sector Training and Resources. *Homeland Security.* [Online] June 15, 2010. http://csat-help.dhs.gov/csetat/csetat_dallas_tx.pdf.

—. 2010. Department Subcomponents and Agencies. *Homeland Security.* [Online] U.S. Government, July 14, 2010. http://www.dhs.gov/xabout/structure/#1.

—. 2010. *Effective Risk Communications Against the IED Threat.* Washignton D.C. : s.n., 2010.

—. 2009. Homeland Security Presidential Directive 19: Combating Terrorist Use of Explosives in the United States. *Homeland Security.* [Online] February 25, 2009. http://www.dhs.gov/xabout/laws/gc_1219260981698.shtm#0.

—. 2009. *National Infrastructure Protection Plan.* Washington D.C. : U.S. Government , 2009.

—. 2009. Science & Technology Directorate Explosives Division. *Homeland Security.* [Online] U.S. Government, August 4, 2009. http://www.dhs.gov/xabout/structure/gc_1224522488810.shtm.

Department of the Army, HQ. 2006. *Composite Risk Management FM 5-19 (100-14).* Washington D.C. : U.S. Government, 2006.

Environmental News Agency. 2010. Newmont Gold Mine to Pay Ghana Millions for Cyanide Spill. *ENA.* [Online] ENA, 2010. [Cited: October 6, 2010.] http://www.ens-newswire.com/ens/jan2010/2010-01-22-01.html.

Federal Bureau of Investigation. 2010. Explosives. *Federal Bureau of Investigation.* [Online] U.S. Government, 2010. [Cited: September 15, 2010.] http://www.fbi.gov/hq/lab/html/eu1.htm.

—. 2010. FBI Working Dogs. *Federal Bureau of Investigation.* [Online] U.S. Government, 2010. [Cited: September 15, 2010.] http://www.fbi.gov/multimedia/workingdogs112508/transcript.htm.

Garcia, Dawn. 2009. *An Introduction to the International Cyanide Code.* s.l. : SRK Consulting, 2009.

Giduck, John. 2005. *Terror at Beslan.* s.l. : ArchAngel Group Inc., 2005. 0-9767753-0-1.

Golder Associates Pty Ltd. 2008. *INTERNATIONAL CYANIDE MANAGEMENT CODE GOLD MINING OPERATION VERIFICATION AUDIT AHAFO MINE, GHANA.* Greenwich : Godler Associates, 2008. 077622030/013.

Grossman, Dave. 1995. *On Killing.* New York : Hachette Book Group, 1995. 0-316-33011-6.

Groves, John. 2010. *Explosive Related Threat Training.* Waynesville, July 20, 2010.

Hawkins, James. 2010. Explosives Programs. *Explosives Engineering.* [Online] Missouri S&T , 2010. http://explosives.mst.edu/explosives_programs.html.

HSNW. 2010. Homeland Security NewsWire, Explosives Detection. [Online] 2010. [Cited: July 22, 2010.] http://homelandsecuritynewswire.com/topics/explosive-detection?page=4.

International Cyanide Management Institute. 2010. About the Code. *International Cyanide Mangement Code for the Gold Mining Industry.* [Online] ICMI, 2010. http://www.cyanidecode.org/about_code.php.

International Organization for Standardization. 2010. International Standards for Business, Government and Society. *ISO.* [Online] ISO, 2010. http://www.iso.org/iso/home.htm.

Keil, Todd. 2010.*Chemical Sector Security Summit Remarks.* Baltimore : U.S. Government, 2010.

Miller, Theresa. 2010. CSETAT Course Outline. 2010.

Morris, Alan. 2004. *ISO 14000 environmental management standards: engineering and financial aspects* . Chichester, England ; Hoboken, NJ : Wiley, 2004. 0470851287.

National Research Council. 2008. *Disrupting Improvised Explosives Device Terror Campaigns: Basic Research Opportunities.* Washignton D.C. : The National Academies Press, 2008. 978-0-309-12420-4/0-309-12420-4.

Norman, Michael. 2009. *The Infrastructure Protection Security Survey. What's in It for You?* [Online Webinar] s.l. : U.S. DHS, 2009.

Northeastern University. 2010. ALERT: Awareness and Localization of Explosives-Related Threats. *Northeastern University.* [Online] Northeastern University, 2010. http://www.northeastern.edu/alert/.

Office of the Inspector General. 2005. *Review of the Bureau of Alcohol, Tobacco, Firearms and Explosives 'Implementation of the Safe Explosives Act.* Washington D.C. : U.S. Government, 2005. I-2005-005.

Sector Security Council. 2010. *Chemical Sector Security Summit.* Baltimore : U.S. Government, 2010, Vol. Summit Gazette.

Smith, Joseph. 2003. *Anti-Terrorism: Criteria, Tools & Technology.* Vicksburg : Applied Research Associates, Inc, 2003.

U.S. Department of Homeland Security. 2010. Homeland Security Advisory System. *Homeland Security.* [Online] U.S. Government, August 17, 2010. http://www.dhs.gov/files/programs/Copy_of_press_release_0046.shtm.

—. 2008. Homeland Security Presidential Directive 1: Organization and Operation of the Homeland Security Council. *Homeland Security.* [Online] U.S. Government, August 22, 2008. http://www.dhs.gov/xabout/laws/gc_1213648320189.shtm.

U.S. Department of Justice, Office of the Inspector General, Audit Division. 2009. *Explosives Investigation Coordination Between the Federal Bureau of Investigation and the Bureau of Alcohol, Tobacco, Firearms and Explosives.* Washington D.C. : s.n., 2009. Audit.

U.S. Government (OMB). 2010. Office of Management and Budget. *The White House.* [Online] August 2010. [Cited: August 11, 2010.] http://www.whitehouse.gov/omb/fy2010_department_homeland.

U.S. State Department. 2010. National Counterterrorism Center: Annex of Statistical Information. *U.S. State Department.* [Online] U.S. Government, Office of the Coordinator for Counterterrorism, August 5, 2010. [Cited: September 20, 2010.] http://www.state.gov/s/ct/rls/crt/2009/140902.htm.

UNC Department of Public Policy. 2003. *Environmental Management Systems: Do They Work?* Chapel Hill : National Database on Environmental Management Systems, 2003.

University of Maryland. 2010. National Consortium for START. *START.* [Online] University of Maryland, 2010. http://www.start.umd.edu/start/announcements/announcement.asp?id=185.

Yates, Jack. 1989. *Six Firefighter Fatalities in Construction Site Explosion, Kansas, City, Missouri.* Kansas City, MO : FEMA, United State Fire Administration, 1989. EMW-88-C-2649.

VITA

James Wade "Buck" Hawkins was born June 30, 1974 in West Union, Ohio. During high school, he joined the Army National Guard and in 1992 shipped to Fort Leonard Wood, Missouri for basic training. Upon completing his training as a Combat Engineer, he returned to Ohio where he worked in residential construction.

In 2000, he started his college career at Morehead State University in Morehead, Kentucky. Over the next four years, he worked as a radio broadcaster for Morehead State Public Radio and continued his military career as a Chemical Operations Specialist. He graduated Summa Cum Laude in 2004 with a Communications degree and emphasis in Electronic Media and was recognized as the department's Top Undergraduate and received Kentucky's Academic Achievement Award.

That same year, he applied to the University of Missouri-Rolla (UMR) to seek a career working in explosives and began coursework in August 2004. Later that fall, he received orders to deploy in support of Operation Iraqi Freedom. In the spring of 2005, Buck deployed to Iraq where he was a squad leader for a brigade military transition team (MiTT), a group tasked to train the Iraqi Army and coalition forces in combat operations. One of his primary missions was the development of the non-commissioned officer corps. Later that summer, he was wounded by an IED and recovered at home before returning to theater to complete his deployment in the summer of 2006.

In 2006, he returned to UMR, later renamed Missouri University of Science and Technology and resumed his studies in Mining Engineering. He graduated Magna Cum Laude in 2010 and immediately started his thesis work which was completed in December earning him an MS in Explosives Engineering.

Buck's work experience includes departmental recruiting at Fort Leonard Wood for the Explosives Engineering program and a summer internship at Three Oaks Mine in Elgin, Texas. He has completed numerous leadership and professional development courses in the military as well where he holds the rank of First Sergeant for the 3175th Chemical Company. Organizations include the International Society of Explosives Engineers, the Association of the United States Army, the Society of American Military Engineers and the Military Order of the Purple Heart.