domestic preparedness .com

DomPrep Journal

Subscribe Volume 10 Issue 5, May 2014

Safety & Security

Securing Airports – Both Inside & Outside
By Richard Schoeberl, Law Enforcement

The Sewol Ferry Disaster – Cultural Considerations
By Julie Sorrell, Emergency Management

Maryland – A State of Good Repair
By Bernadette Bridges, State Homeland News

Specialized Training for Rail Incidents
By James Metzger, Transportation

Airport Security – Beyond the Perimeter
By Andrew Saxton, Viewpoint

Critical Incident Stress Management & Peer Support
By Tania Glenn, Public Health

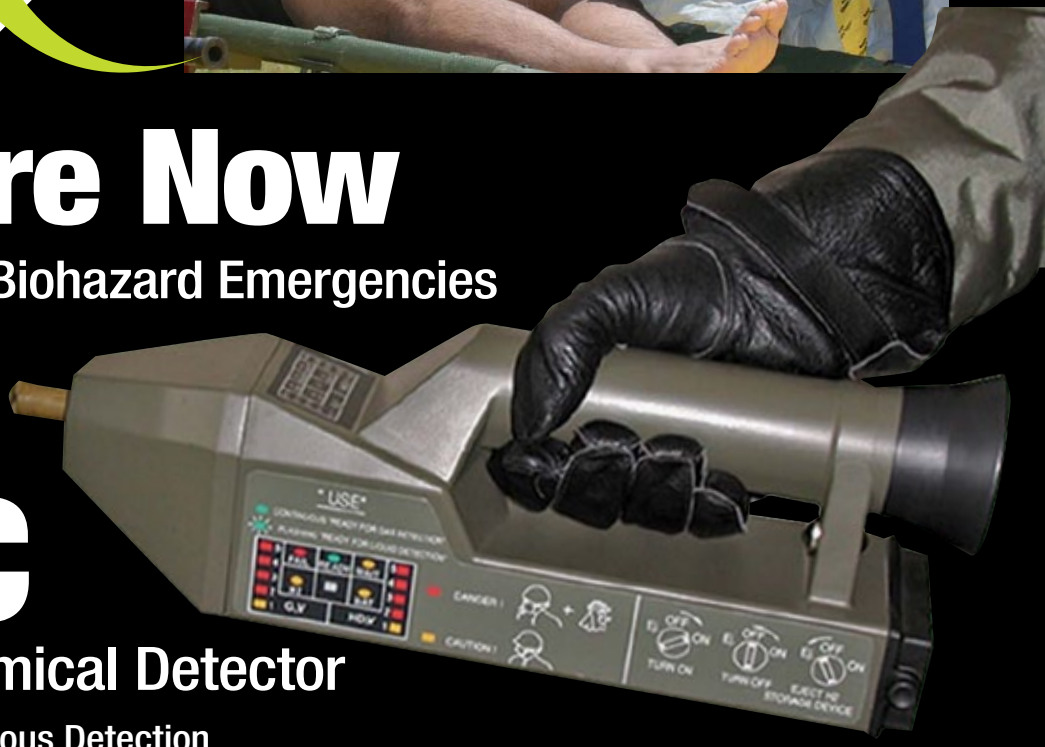
Mexican & U.S. Aviation Security
By Clay W. Biles, Viewpoint

The Team Spirit of Emergency Management
By Stephen Grainer, Emergency Management

Not If, But When?

Prepare Now

For Chemical & Biohazard Emergencies



AP4C

Handheld Chemical Detector

- Unlimited, Simultaneous Detection
- Continuous Detection for Fix Locations
- Low Maintenance and Operation Cost
- Compact Design for Tight Locations

PROENGIN

Chemical and Biological Detection System

PROENGIN, inc.
140 S. University Dr, Suite F
Plantation, FL 33324 USA
Ph: 954.760.9990
contactusa@proengin.com
www.proenginusa.com

Business Office
517 Benfield Road, Suite 303
Severna Park, MD 21146 USA
www.DomesticPreparedness.com
(410) 518-6900

Staff
Martin Masiuk
Founder & Publisher
mmasiuk@domprep.com

Susan Collins
Associate Publisher
scollins@domprep.com

James D. Hessman
Editor in Chief
JamesD@domprep.com

Catherine Feinman
Editor
cfeinman@domprep.com

Mark Perry
Business Development Manager
mperry@domprep.com

Carole Parker
Administrative Assistant
cparker@domprep.com

John Morton
Senior Strategic Advisor
jmorton@domprep.com

DomPrep Journal is electronically delivered by the IMR Group Inc., 517 Benfield Road, Suite 303, Severna Park, MD 21146, USA; phone: 410-518-6900; email: subscriber@domprep.com; also available at www.DomPrep.com

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 Manuscripts are original work, previously unpublished, and not simultaneously submitted to another publisher.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

Editor's Notes

By Catherine Feinman

Security measures for all modes of transportation – by land, sea, and air – have been a priority for many agencies since the 9/11 attacks, when terrorists hijacked several passenger airplanes and used them as weapons of mass destruction. Mitigating, responding to, and recovering from transit disasters require a balance between technologies and human intelligence, safety and sacrifice, training and budget, as well as self-reliance and team efforts.

Richard Schoeberl leads this issue of the *DomPrep Journal* with a look at security risks that still exist at U.S. airports. Recent breaches in security at several airports have pushed law enforcement agencies to examine current security measures and take steps toward closing gaps that otherwise could lead to more breaches in the future. However, ensuring safer and more secure airports and air travel requires passengers to sacrifice some level of convenience.

Andrew Saxton and Clay Biles agree that more security is necessary at airports around the world. Technological advances provide surveillance opportunities that were not available even a decade ago, but a robust security system must include not only layers of various technologies, but better human intelligence as well.

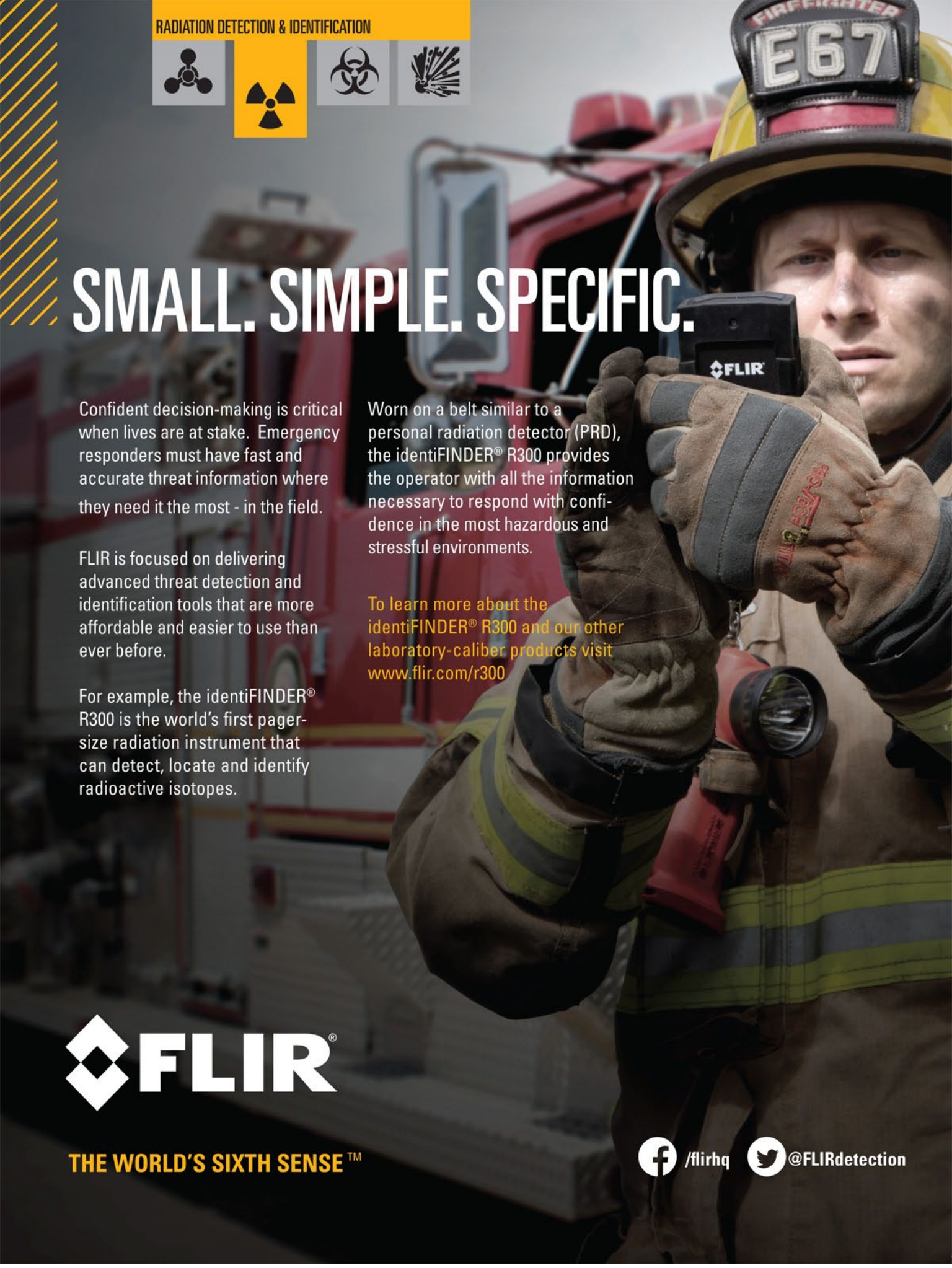
Incidents occurring – either intentionally or unintentionally – on an airplane, a train, or a ship pose unique hazards to response crews. James Metzger shares information about specialized training available to first responder agencies for a variety of rail incidents these responders may face within their communities. Of course, the best defense is a good offense. Bernadette Bridges recognizes the challenges associated with the nation's aging transit infrastructure and describes how Maryland is taking steps to repair its transit system before another incident occurs.

Julie Sorrell provides a South Korean example of safety regulations colliding with culture. Fewer lives would have been lost in the April 2014 Sewol ferry disaster if the company and crewmembers followed these regulations, if crewmembers were adequately trained, if passengers had taken actions other than following the captain's orders, and a lot more ifs.

Regardless of the type of incident, all emergency planners, responders, and receivers must work as a team and be able to depend on each other when needed. Stephen Grainer compares emergency management to football teams and racecar pit crews that devote their time to train together. When emergency response teams activate, the physical and emotional stress can be overwhelming and unique to each member of the team. In such cases, Tania Glenn explains, peer support teams can help build and maintain both personal and organizational resilience.

About the Cover: The U.S. Department of Homeland Security has a vital mission to secure the nation from many threats. To help strengthen and protect the nation's transportation systems, the Transportation Security Administration conducts inspections and provides additional security of boats, airports, and trains.

RADIATION DETECTION & IDENTIFICATION



SMALL. SIMPLE. SPECIFIC.

Confident decision-making is critical when lives are at stake. Emergency responders must have fast and accurate threat information where they need it the most - in the field.

FLIR is focused on delivering advanced threat detection and identification tools that are more affordable and easier to use than ever before.

For example, the identiFINDER® R300 is the world's first pager-size radiation instrument that can detect, locate and identify radioactive isotopes.

Worn on a belt similar to a personal radiation detector (PRD), the identiFINDER® R300 provides the operator with all the information necessary to respond with confidence in the most hazardous and stressful environments.

To learn more about the identiFINDER® R300 and our other laboratory-caliber products visit www.flir.com/r300

FLIR®

THE WORLD'S SIXTH SENSE™

/flirhq @FLIRdetection

DomPrep Writers

Raphael M. Barishansky
Public Health

Joseph Cahill
EMS

Craig DeAtley
Public Health

Kay C. Goss
Emergency Management

Stephen Grainer
Fire/HazMat

Rodrigo (Roddy) Moscoso
Law Enforcement

Glen Rudner
Fire/HazMat

Richard Schoeberl
Law Enforcement

Joseph Trindal
Law Enforcement

Securing Airports – Both Inside & Outside

By Richard Schoeberl, Law Enforcement

With the large number of threats that exist today, there is no doubt the United States will continue to be a target for terrorist activity. The orchestrators of such threats select targets that will cause the utmost fear in the population, impose economic damage, and create a lack of confidence in the government. Despite additional threats since 9/11, U.S. airports continue to have severe deficiencies in security.

Five attempted terrorist attacks on airlines and airports in the United States since 9/11 highlight the importance of making airport security a priority. Recent incidents – the shooting at the Los Angeles International airport in November 2013, the missing Malaysian Airline Flight 370 in March 2014, and a teenager sneaking aboard a Hawaiian Airlines flight after breaching security perimeters in April 2014 – raise the questions of whether airports ever will be completely secure and what it will take to get there.

Current Security Efforts

According to the Transportation Security Administration (TSA), approximately 1.8 million passengers pass through U.S. airports every day. Although the TSA has implemented additional safety methods, some have failed – for example, the Screening of Passengers by Observation Technique (SPOT) program, which is suppose to prepare TSA agents to identify criminals and terrorists by observing the behaviors that may be a sign of fear, stress, and deception. After spending nearly one billion dollars over the past decade, Congress has determined that the SPOT program has "up till now" not proven useful nor effective.

The Government Accountability Office (GAO) issued a report in November 2013 that recommended limiting "future funding support for the agency's behavior detection activities until TSA can provide scientifically validated evidence that demonstrates that behavioral indicators can be used to identify passengers who may pose a threat to aviation security." According to that report, there is no indication that the 3,000 officers trained in behavior detection at some 176 U.S. airports are actually improving airport security at all.

Although there is question whether the TSA can prove qualitatively that the SPOT program works in the United States, a similar program in Israel serves as a best practice in airport security. In Israel, Tel Aviv's Ben Gurion airport faces more terrorist threats than other airports around the world. Israeli security officers use behavioral profiling similar to SPOT to analyze people and their behaviors.

After asking intrusive questions to elicit a response, officers target a passenger for further questioning and search if he or she exhibits

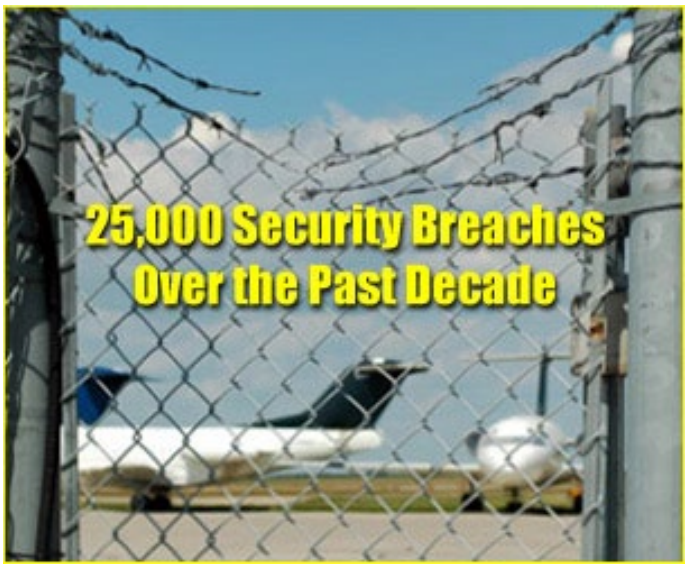
guarded actions. The Israelis have been the model for establishing and maintaining security in many forms. Much of the airport's security protocol combines comprehensive layers of due diligence, common sense, and consistency. Although the cost associated with maintaining a similar program in the United States is high, the benefits could outweigh the cost.

Law Enforcement Responsibilities

In addition to SPOT, the TSA has suggested the need for armed law enforcement officers to safeguard airport checkpoints in response to a shooting at Los Angeles International Airport. The TSA released a report to Congress in March 2014 focused on the safety and security of the TSA workforce and recommended how to prepare for and respond to an emergency. The recommendations, though, are dependent on the local authorities that currently provide airport security and have no costs associated with them.

That report particularly notes that local police officers, not TSA officers, should be the ones conducting the armed security details and recommends that more armed law enforcement officers be present at airport security checkpoints and ticketing counters. These recommendations include: mandatory training for all TSA officers on how to respond to and notify federal air marshals during an active shooter situation; mandatory biannual evacuation drills; the installation of panic buttons at airports currently without the alarm system; more security cameras; better equipment and technology; linking duress alarms to CCTV systems; and alternate local airport emergency phone numbers. All these safety efforts, though, come with associated costs.

Terrorists are still looking for a means to smuggle bomb-packed items and explosive-laden shoes onto airlines. Imaging technology has been an integral part of TSA's security efforts at airports since 2008, when the TSA began using advanced imaging technology (AIT) that can detect a wide range of threats. AIT is another layered approach in airport security for detecting smuggled items or weapons. Because specific security measures vary from country to country, the nation must harden its security at home.



Breaches in Security

More than 25,000 security breaches – averaging nearly seven per day and more than five per airport per year – have occurred at more than 450 TSA-regulated airports over the past decade, according the U.S. Department of Homeland Security. The breaches include everything from people who unintentionally leave a bag on a checkpoint conveyor belt to those who decisively evade security and board airplanes without proper screening. Following are some examples:

- 14,322 breaches of secure entries, passages, or other access points to the secure side of the airport;
- Approximately 6,000 breaches involving a TSA screener failing to screen or improperly screening a passenger or a passenger's carry-on property; and
- 2,616 breaches involving an individual getting past the checkpoint or exit lane without submitting to all screening and inspections (1,388 of these occurred at the airport perimeters).

Unfortunately, enforcement efforts must be effective every time, whereas a terrorist only needs one successful attempt.

The inside of an airport cannot be completely secure if the exterior is not secure. Most recently, a breach in San Jose led to the unbelievable survival of the teenage boy that flew more than five hours from San Jose, California, to Maui, Hawaii, in the wheel well of a

jet airliner. The young man crept unobserved past all the perimeter security measures of San Jose Airport – a major U.S. airport. However, this is not an isolated case.

In December 2013, two major airport perimeter breaches took place: (a) Newark Liberty International in Newark, New Jersey; and (b) Sky Harbor International in Phoenix, Arizona. The breach at Newark exposed a failure of a $100 million system designed to protect New York City area airports. The Phoenix "fence hop" was the fifth in a decade at that airport.

The Perimeter Intrusion Detection System (PIDS) at Newark combines radar with video cameras, motion detectors, and "smart" fencing. The technology worked but the monitors also must report the intrusion alerts for them to be effective. In August 2012, the same PIDS failed in New York City, when a person swam three miles from a disabled jet ski and swam ashore near John F. Kennedy International Airport. He climbed a fence and crossed two runways – without the PIDS spotting him. When the exterior intrusion systems do not stop an uncalculated intrusion, interior airport security must be prepared for a calculated intrusion.

Balance Between Convenience & Security

Equilibrium is very important in today's society because airport security must balance customer convenience with overall safety. The public stakeholders must decide what conveniences and civil liberties they are willing to give up in exchange for safety. No single tool, no single program will impede an attack. Airport security, like all other security, is successful in layers as no single technique can eliminate all threats. Even with security employees trained to be on the watch for and confront intruders, as well as police agencies patrolling the airport's perimeter, no security system is infallible.

To address all these concerns, government agencies must be aware, remain diligent, and raise concern about the "insider" threat in which someone who desires to do harm has a "right of entry" to secure areas such as those in airports. Terrorists have used insiders to access overseas targets in the past and collect sensitive information to aid terror operations. Similar to a soccer game, people often remember security efforts not by the number of saves, but rather by the one that got by.

Richard Schoeberl has more than 17 years of counterintelligence, counterterrorism, and security management experience, most of it developed during his career with the Federal Bureau of Investigation, where his duties ranged from service as a field agent to leadership responsibilities in executive positions both at FBI Headquarters and at the U.S. National Counterterrorism Center. During most of his FBI career he served in the Bureau's Counterterrorism Division, providing oversight to the agency's international counterterrorism effort. He also was assigned numerous collateral duties during his FBI tour – serving, for example, as a Certified Instructor and as a member of the agency's SWAT program. He also has extensive lecture experience worldwide and is currently a terrorism and law-enforcement media contributor to Fox News, Sky News, al-Jazeera Television, and al-Arabiya.

The Sewol Ferry Disaster – Cultural Considerations

By Julie Sorrell, Emergency Management

Navigating swift and unpredictable waters during the morning hours of 16 April 2014, the South Korean ferry named the Sewol made a sharp turn, began listing, and within two hours was completely on her side – 12.5 miles from the southwestern coast of the Korean peninsula. Of more than 470 passengers and crew onboard, the majority were high school students on an extended field trip.

One Disaster, But Many Bad Decisions

A month after the disaster, 288 have been confirmed dead and 16 are still unaccounted for. After days of searching, the rescue became a mission to recover bodies. Survivors began telling their accounts of what happened on the ferry. The students who escaped the wreckage publically claimed that those students who died were simply obeying the crew's orders to stay below deck and await further instruction. As one CNN report stated following the disaster, "Obedience in the young is prized. Parental protection is the reward."

There are plenty of reasons why the Sewol sank, including the following series of events:

- An inexperienced third mate at the helm made a sharp turn in notoriously unsure water.
- Improperly secured and excessively heavy cargo shifted.
- Previous work to refit the number of sleeping cabins onboard affected the ferry's balance.
- "Watertight" doors allowed hallways and rooms to flood.
- Confusion sparked panic as inexperienced crew tried to decide what to do.
- Crewmembers failed to notify the proper authorities. Instead of contacting the nearby Coast Guard, the crew contacted a vessel traffic service 50 miles away. This in turn caused a 53-minute delay in rescue mobilization.

- The crew hesitated to follow the directions provided by a port operator, heard on recordings frantically yelling at the crew to evacuate the ship. The crew claimed that the public announcement system was broken, that the ship was listing at too severe an angle to move about, and that there were too many passengers to board the arriving helicopters. "It's completely impossible for the Sewol ferry to evacuate," one crewmember said.

Most of the crew and some of the passengers were rescued before the ship disappeared under the water. Unfortunately, the majority of deaths were high school students and adults who heeded the crew's instructions to remain below deck and await further instruction. Those instructions never came.

Profits, Deadlines & Obedience

The Confucian-influenced teachings of young people in Korea stress obedience. In fact, authoritarianism is prevalent in many facets of Korean society. In addition to youths being taught to obey their elders, there is also a *hoobae-sunbae* (translated as "junior-senior") order of obedience that is not age dependent. *Hoobae* are those with less experience in business or in academic settings. *Sunbae* are their seniors (at their jobs or schools) and hold greater social power.

Hoobae are expected to speak politely and respectfully to *sunbae*. When the crew of the Sewol told the passengers

to stay where they were in the lower decks, this *hoobae-sunbae* "pecking-order" dictated that they do so. When told to wear their life vests, which may have prevented them from moving out of the quickly rising waters, they did so. They obeyed because, to do otherwise, would have been socially unacceptable.

There are other cultural aspects important to understanding the sinking of the Sewol. Among developed nations, South Korea has the highest rate of accidents. NBC News reported in May 2014 that, according to the Organisation for Economic Cooperation and Development (OECD), each year an estimated 31,000 South Koreans die from various types of accidents – automobile crashes to fires – accounting for 12.8 percent of yearly mortality. Regulatory enforcement also may contribute to this death toll.

"The majority of deaths were high school students and adults who heeded the crew's instructions to remain below deck and await further instruction. Those instructions never came."

The same NBC News report noted that the Korean economic phrase *ppali ppali* (meaning "hurry hurry") is often used in the Korean work environment. Protecting the dignity and reputation of a company and its workers are important in Asian cultures. With myriad rules and regulations, some business professionals choose to skirt basic rules and navigate around safety regulations to meet strict deadlines.

In a desire for rapid economic growth in the era of post-colonial rule, South Korean authorities may have sacrificed safety and paid for it in the lives of its own people. Following the Sewol sinking, South Korean prosecutors discovered that a sister ship, named the Ohamana (also owned by the Chonghaejin Marine Company), was operating with unsafe equipment, including 40 defective life rafts and unusable emergency slides. Of the 44 lifeboats aboard the Sewol, only two were launched; it is unknown at this time if they would have worked had they been deployed.

In a similar Japanese ferry disaster in 2007, the cabins added to the top deck to increase passenger capacity shifted the center of gravity and led to that ferry capsizing. The Sewol's sleeping cabins were refitted as recently as 2013, which may have made the ship too top-heavy. In light of recent developments, South Korean authorities arrested the Chonghaejin Marine Company's chief executive officer on charges of death by negligence. The Sewol was carrying twice the ferry's limit of cargo, which crewmembers failed to secure properly.

The firm's business practices are now under scrutiny. On the ill-fated April trip, the Sewol's excess cargo was earning the company some 62 million won (the equivalent of $62,000 U.S. dollars). Since the beginning of the Sewol's routine route along the western coast of South Korea in March 2013, the company has grossed approximately 3 billion won (2.9 million dollars) for the extra cargo hauled above the legal limit.

Lessons to Be Learned by All

First responders and emergency managers around the world can learn a lot from the cultural aspects of the Sewol disaster. Culture defines the attitudes and responses of all persons and agencies involved in the risk management, disaster planning, emergency response, and disaster recovery phases. Culture can even define victim survival.

The lukewarm relationship between safety and expediency in the case of the Sewol disaster serves as a stern warning to all transportation authorities. Putting profits and deadlines ahead of adherence to safety regulations can lead to unsafe conditions, defects in equipment, and greater potential for loss of life. During the response phase, emergency responders also must be cognizant of the cultural aspects of those they are attempting to save. Although it may not be possible to change cultural attitudes, planners and responders can better manage disasters by considering the cultural attitudes and behaviors of all those involved during every phase of disaster planning, response, and recovery.

Julie Sorrell is a biosecurity and disaster preparedness specialist in Springfield, Missouri. She is a member of the Community Emergency Response Team of the Greene County Office of Emergency Management (since 2008) and a member of the American Red Cross's Disaster Assistance Team (2011-2012). She has an MA in political science and an MS in biosecurity. She also created the Countering Bioterrorism Blog in 2011 and "Bioterrorism Response for the First Responder," a written text for teaching first responders about biological agents and bioterrorism response, in 2012.

Maryland – A State of Good Repair

By Bernadette Bridges, State Homeland News

The transit industry is evolving with new technology, new regulatory requirements, and better use of historical data and information to report to the industry and to other transit professionals the best practices and recommended ways to manage safety and security. Traditionally, after designing and building bus and rail facilities and vehicles to predetermined specifications, the project managers completed and approved the quality assurance checks, performed a test run of the system, readied the line for full-service operation, and commissioned the system. In modern transit systems, safety and security are an integral part of the design and build phases.

Building & Maintaining Transit Systems

According to the Federal Transit Administration's (FTA) 2010 National State of Good Repair Assessment, "Roughly one-third of the nation's transit assets (weighted by replacement value) are in either marginal or poor condition, implying that these assets are near or have already exceeded their expected useful life." As budgets decrease, it may be difficult to rebuild and maintain a safe and secure operating system and infrastructure – including highways, bridges, transit systems, and transit vehicles. Although a jurisdiction may repair a cracking bridge, replace a bus garage or rail maintenance facility, or overhaul the vehicles, some decision makers may question whether these actions make the community any safer. However, being in a "state of good repair" – as defined by the FTA's Transit Economic Requirements Model (TERM) – is relevant to safety and security.

When original equipment manufacturers and designers build transit systems, safety professionals prefer to conduct risk assessments and hazard analysis during the preliminary design phase. This allows designers, engineers, and operating staff to build and design safety and security features into their projects. There also are federal requirements on new startup projects that require risk-based assessments. These assessments can be for safety and security as well as for the operating environment – for example, high-crime areas, dark or poorly lit roads or rights of way, or areas where there is the potential for crimes against or injuries to passengers or employees. Risk assessment for insurance purposes, such as what a property or company is willing to accept, is also an important and necessary part of the process. There are many ways to enhance safety and security in new or existing projects.

Transit professionals should first ask how to improve the facilities, equipment, employees, procedures, and environment in which they operate. The safety culture should include managing risks early during the planning and design phases of critical systems. These early reviews assist in eliminating and mitigating potential hazards and risks. By managing assets and using various integration techniques, safety professionals can begin the process of establishing guidelines for maintaining a state of good repair throughout the life of a project, including when modification of equipment and facilities is necessary.

Certifications, Assessments & Management Systems

Integration techniques used by the Maryland Transit Administration (MTA) and other agencies include: (a) safety and security certifications; (b) hazard assessments; and (c) safety management systems. The safety and security certification process verifies, confirms, and identifies that the safety and security components of a system's design are ready for revenue operations and were developed, constructed, and tested in accordance with the applicable codes, standards, criteria, and specifications.

Hazard assessment – a formal process used to identify, analyze, and mitigate the hazards associated with the design, construction, testing, and start-up of new or modified projects – is another tool used to mitigate hazards during the planning and project design phase. Assessments help categorize hazards by severity and probability of occurrence and analyze hazards for their potential impact on a system.

A safety management system is another tool the MTA uses to manage transit operations, but it can be applicable to any type of business operation. Four

components associated with this type of integration of safety and security include:

- *Safety policy* – safety commitment and accountability, safety roles and responsibilities, and safety resource allocation to support safety performance;
- *Safety risk management* – safety hazard identification, safety risk-based analysis, and implementation of safety risk controls;
- *Safety assurance* – monitoring of safety risk controls to ensure achievement of the intended objective while assessing the need for new risk-control strategies; and
- *Safety promotion* – achievement of the safety mission through clear communication channels and safety training programs.

MTA considers "state of good repair" when designing and building its transit systems. MTA's procedures, inspections, and mitigation tools listed above ensure the safety and security of the transit system when designing, modifying, or redesigning its systems, or when required to do so by new local, state, or federal regulations. By looking ahead and anticipating issues, the MTA knows when it is time to replace a vehicle, repair a bridge, or modify a right of way, and develop budgets that reflect keeping the transit systems in a state of good repair. Good safety pays now, but delaying the budget expenses until later can become extremely costly.

Bernadette Bridges is the chief safety officer and officer of safety for quality assurance and risk management at the Maryland Transit Administration (MTA) in Baltimore, Maryland. She has more than 28 years of experience in the area of mass transit, and over 17 years experience in the area of safety. She began her transportation career as a bus operator and then spent five years as a rail supervisor and controller for MTA's Light Rail System. In her present assignment, she oversees agency system safety, emergency management, claims, risk management, Owner Controlled Insurance Program (OCIP), environmental compliance, and quality assurance. She is a certified safety director through the World Safety Organization, an associate staff instructor for the Federal Transit Administration's (FTA) Transportation Safety Institute, and a member of American Public Transportation Association's safety committees for both bus and rail. She previously served a one-year term on the Tri-State Oversight Committee. Appointed by the Federal Department of Transportation administrator, she currently serves as a member of the Transit Rail Advisory Committee for Safety (FTA-U.S. Department of Transportation).

Specialized Training For Rail Incidents

By James Metzger, Transportation

In 2012, Amtrak created the Emergency Management and Corporate Security (EMCS) Department, which focuses on emergency preparedness, continuity of operations, and corporate security risk strategy. EMCS promotes Amtrak's security and safety goals by focusing on preparing first responders on how to respond to passenger train emergencies. It is imperative that the more than 26,000 emergency response agencies along the Amtrak rail system understand how to best respond to incidents involving passenger trains.

Amtrak follows the Transportation Code of Federal Regulations' Passenger Train Emergency Preparedness (49 CFR Part 239), which focuses on reducing "the magnitude and severity of casualties in railroad operations by ensuring that railroads involved in passenger train operations can effectively and efficiently manage passenger train emergencies." To meet these preparedness regulations, as set forth by the Federal Railroad Administration, Amtrak conducts Passenger Train Emergency Response (PTER) trainings for employees and external partners for stakeholders in its widespread service area – 46 states, District of Columbia, and three Canadian provinces.

Emergencies on passenger rail cars and equipment require special knowledge, preparation, and training. Amtrak currently has 11 regional emergency managers across the nation who help prepare the first responder community for emergencies along America's Railroad®. These regional emergency managers use the five core competencies of the Incident Command System to provide instruction during train incidents and emergencies: assume position responsibilities; lead assigned personnel; communicate effectively; ensure completion of assigned actions to meet identified objectives; and assume position responsibilities.

The PTER course provides first responder agencies – law enforcement, fire, emergency medical services, healthcare, emergency managers, public health, public works, government agencies, private sector, and anyone else who may have to respond to a rail incident – specific knowledge on how to ensure responder safety

by providing information on a variety of topics related to railroad safety, including:

- Railroad right of way dangers and safety concerns
- Safe evacuation of passengers, including those with functional needs
- Mainline switches (remotely controlled)
- Passenger and freight railroad relationships
- Emergency phone numbers
- Average frequency of passenger and freight trains
- Maps and schedules
- Passenger loads
- Train speeds
- Train crew orientations
- Challenges of extraction
- Railroad mileposts, signals, crossings, flagging distances, and bungalows
- Access points to the railroad
- Secondary access points if primary is blocked
- Safety equipment diagrams
- Trespassing on railroad property
- Bent rail
- Pneumatic and electrical hazards
- Tunnel and bridge preplanning
- Environmental issues

With Amtrak having more than 500 stations and 31.6 million passengers in 2013, the EMCS's goal is to promote safety and security for all of its customers, employees, and community partners. The one-day PTER training is offered free of charge to all community response agencies that may have to respond to a train incident within their jurisdictions or neighboring jurisdictions.

To find out more or to schedule a PTER training course with Amtrak, please contact the EMCS at: EMCS@Amtrak.com

James Metzger is the deputy chief of emergency management and corporate security for the National Railroad Passenger Corporation – Amtrak. Previously, he was a station action team coordinator for Amtrak from 2008 to 2012. Before joining Amtrak, he served in various positions in the Southeastern Pennsylvania Transportation Authority Police Department (1991-2008) – including lieutenant, commander special operations division, and counterterrorism coordinator. From 1986 to 1990, he was a sergeant in the U.S. Marine Corps.

Airport Security – Beyond the Perimeter

By Andrew Saxton, Viewpoint

To counter the various threats to airports in the 21st century, airport operators must extend their awareness beyond the airport's perimeter. Detecting intruders as they are climbing the fence is too late. As such, an effective beyond-the-perimeter, intrusion-detection system requires both threat detection and assessment capabilities from a variety of sensing technologies. These sensors integrate into a comprehensive command-and-control platform that is not dependent on video analytics.

Comprehensive Command & Control

An intelligent command-and-control solution is the crux of an integrated perimeter security solution. This core element draws intelligence from the raw sensor data and improves the airport's security position. Solutions that integrate multiple types of sensors – radar, thermal imaging, and other technologies – provide comprehensive, decision-support intelligence.

Ground surveillance radar provides early detection and alarm-zone configuration. Radar as an initial detection sensor also has several advantages over fence-line-based sensors. Unlike visible camera systems, radars deliver maximum performance regardless of the amount of light available, and better penetrate atmospheric obscurants like fog, smoke, and dust. In addition, cameras typically use video analytics based on video management systems, which may be unreliable for detecting intrusions.

Vibration-based sensors – like seismic sensors and fence cables – also have inherent drawbacks. First, they provide no information that would allow security personnel to assess the threat level posed by whatever initiated the alarm. Even more problematic, though, is the fact that they only alarm on triggering events at or even on the fence itself. They do not provide information about the intrusion beyond the point and time it took place, whereas radar provides speed and heading. Radar also can hand tracks off from one camera to another automatically. Using ground surveillance radar as a primary sensor integrated with

thermal cameras and other technologies can help overcome these shortcomings.

Advantages of Radar

Tightly integrated ground-surveillance radar solutions can detect potential threats well beyond an airport's perimeter fence. Such systems provide security personnel with important information on the nature of the potential threat the system detected, even in dynamic environments.

For example, most airports have one or more perimeter roads that run adjacent to the fence line. Radars offer an extended range not only to monitor traffic as it travels near the airport perimeter, but also to detect certain behaviors that can trigger alarms. Radar identifies an object by timing the return of the signal broadcast. Each pulse that goes out will provide "returns" off surfaces, and as those returns change, the radar knows something has moved or is in the wrong place. For instance, users can configure the radar to alarm when a car stops on the road, or when a single return turns into two returns, indicating that a person has exited a vehicle. Similar behaviors extend to boats approaching the perimeter from the water, or people approaching on foot, making ground surveillance radar the most effective and flexible tool for detecting threats before they reach the fence line.

"An effective beyond-the-perimeter, intrusion-detection system requires both threat detection and assessment capabilities from a variety of sensing technologies."

Radar and thermal imaging work together and provide great functionalities. Beyond simply detecting a potential threat, the radar logs the threat's location, heading, speed, and track. After initially detecting a threat, radar has the ability to automatically track the return. If a person does breach the perimeter, security personnel would have an accurate, current record of the intruder's location. The thermal camera provides reliable identification, even in total darkness.

When integrated with daylight, low-light, and thermal cameras through command-and-control software, the cameras automatically slew-to-cue and stay locked on the return of interest, giving security personnel instant image analysis tools they can use to assess the threat level and respond accordingly. When the intruder leaves one camera's visual field, the radar could automatically pass the threat cue to the next camera, so operators never lose sight of the event, without having to manually reconfigure the system.

With powerful command-and-control software, security personnel can set up customized trip wires, exclusion zones, and alarm areas based on map locations within the facility. All of these capabilities illustrate 21st century solutions to airport perimeter security: technology that detects, tracks, and assesses threats well beyond the perimeter boundary, while leaving security personnel free to decide on the appropriate course of action and response.

Andrew Saxton is the director of marketing for FLIR Systems, a global leader in thermal imaging for military, law enforcement, commercial, and industrial applications. He has been with FLIR for 10 years, and previously served as the director of airport security. He received an M.B.A. from University of Washington, and a B.S. in mechanical engineering from Columbia University. FLIR Systems has developed and delivered reliable and intelligent solutions for the protection of civil and government aviation facilities around the world. Please visit www.flirairports.com or follow @flirdef on twitter for more information. He can be reached at asaxton@flir.com.

Critical Incident Stress Management & Peer Support

By Tania Glenn, Public Health

In the aftermath of 9/11, aviation and other transportation incidents have become the focus of much national and international attention. Commercial aviation incidents like U.S. Airways Flight 1549 making an emergency landing on the Hudson River in January 2009, Asiana Airlines Flight 214 making a crash landing onto the San Francisco runway in July 2013, and Malaysia Airlines Flight 370 disappearing in midair in March 2014 raise legitimate concerns over aviation safety, standardization, and security. However, regardless of the type of incident, the personal resilience levels of those affected may vary greatly.

Lasting Effects of Critical Incidents

Frequent land, sea, and air travelers feel the effects of these incidents as new regulations, rules, and standards arise and change almost daily. Some transportation incidents touch lives in unexpected ways, leaving a lasting effect (both negative and positive) that shapes both professional and personal lives. Ultimately, these catastrophic incidents severely influence the psyche of flight crew members, commercial passengers, and their respective associations such as co-workers, family members, and close friends. They each may experience stress and trauma after such life-changing events.

Large-scale events that involve loss of life often are known as "critical incidents" – sudden and extreme events that can overwhelm the usual coping mechanisms of rescuers, bystanders, and travel personnel. At any given point, an incident could affect even the most experienced and seasoned rescuers. It is human nature to have a coping capacity or threshold, beyond which a person no longer tolerates stress in a productive manner. In addition, the definition of a critical incident may change or evolve over time as people grow and acquire new life experiences.

The most debilitating type of critical incident is one that involves death. The repercussions that such incidents have for personnel and responders are powerful and very painful.

Proactively Managing Stress

During the mid-1980s, Jeffrey Mitchell, Ph.D., ex-firefighter and now psychologist, created the concept of critical incident stress management (CISM). Mitchell researched the stress responses of police officers, firefighters, paramedics, and emergency room nurses and found that, across the board, people in these professions experience the same types of reactions both during and after traumatic events. Some of these reactions include, but are not limited to: nausea, vomiting, diarrhea, pupil dilation, headaches, indigestion, tremors, muscle aches, increased smoking, insomnia, nightmares, social isolation, anger, depression, increased startle response, restlessness, and increased use of alcohol.

Mitchell also found that, for the most part, people in these professions were trying to cope with these symptoms in unhealthy and unproductive ways. Attempts to "forget" or repress recurring thoughts and memories have resulted in frightening rates of alcoholism, divorce, and suicide among emergency personnel.

The concept of CISM became the focus of Mitchell's career. In 1983, he created the Mitchell Model for debriefings, which rescuers and transportation professionals worldwide have used successfully. The strength behind the model lies in the fact that it is a nonthreatening, peer-driven process that enables police

officers to talk to police officers, paramedics to talk to paramedics, and so on. In aviation, flight personnel can talk to others who understand their culture, terminology, lifestyle, and stressors.

This is not psychotherapy, just a chance to sit down with people who care enough to be there to talk about the incident, to receive stress management reminders, and to "cuss and discuss" if they so choose. Repeatedly, studies have shown this model to be quite successful in mitigating the stress response of those serving in the line of duty. Additionally, this process has facilitated connections to professional counselors when follow up is necessary for personnel.

When proactively dealing with critical incidents, the aviation, first responder, law enforcement, and military communities often develop and employ CISM teams and peer support teams in response to manmade and natural disasters. Hence, in preparing for an emergency, it is useful for both the private and public sectors to develop and employ similar capabilities in advance of an unexpected disaster response. Ultimately, during a critical incident, whether manmade or natural disaster, people will experience stress and trauma. The goal of any organization always should be to create a safety net for all personnel, and to ensure that no one falls through that safety net. Mission first, people always.

Tania Glenn, PsyD, is the president of Tania Glenn and Associates (TGA) PA, a clinical practice in Austin, Texas, and the TGA Readiness Action Division (RAD). As a licensed clinical social worker and certified trauma specialist with 22 years experience treating anxiety and depression, she deployed to Oklahoma City in 1995, New York City in 2001, and New Orleans in 2005 in support of law enforcement officers, firefighters, and national guardsman who responded to the Oklahoma bombing, 9/11, and Hurricane Katrina. Her broad experience includes serving as: the clinical director for several critical incident response teams; the traumatic stress management coordinator for Austin/Travis County Emergency Medical Services and Round Rock Police Department; an active faculty member and trainer for the International Critical Incident Stress Foundation; an advisory board member for the Brattleboro Hospital Uniformed Services Worker's Retreat, Brattleboro, Vermont; and a regular contributor to Air Beat: The Official Journal of the Airborne Law Enforcement Association.

Mexican & U.S. Aviation Security

By Clay W. Biles, Viewpoint

As allies and neighbors that share nearly two thousand miles of border land, there are many similarities between Mexico and the United States – and just as many differences. Mexican airports, including Benito Juárez Mexico City International Airport and Cancun International Airport, comply with U.S. Federal Aviation Administration specifications and have similar restrictions for carry-on items. Although there are similarities in the regulations themselves, the differences in their implementations at security checkpoints can be significant.

Mexican Security Efforts

At security checkpoints in Mexico, airports rely heavily on the personnel. Security regulations allow most passengers to keep their shoes on and place metallic items that they are carrying on a small tray. Depending on the individual and situation, security personnel also may ask passengers to remove their laptops and place them in large bins for x-ray inspection, or to step to the side for wanding with a handheld magnetometer. When the security personnel are professional and respectful, the passengers tend to remain calm throughout the process.

"It is much easier to spot a nervous passenger when everyone else is calm. Mexican aviation security professionals take advantage of this environment on a daily basis by relying greatly on its people."

Despite the perceived lower level of security, though, a lot happens "behind the scenes" in the Mexican aviation security effort. Security agents constantly watch for telltale behavioral signs of distress or deceit among passengers entering the checkpoints. It is much easier to spot a nervous passenger when everyone else is calm. Mexican aviation security professionals take advantage of this environment on a daily basis by relying greatly on its people.

In addition, Mexican aviation authorities follow the core elements of the International Air Transport Association's Security Management Systems for Air Transport Operators: senior management commitment; resource management; threat assessment and risk management; management of emergency and incidents (resilience); quality control and quality assurance; and aviation security program.

U.S. Security Efforts

In the United States, the aviation security environment is much different. After having their identifications checked and entering the airport's security area, passengers encounter scanning equipment in a variety of shapes and sizes, remove their laptops and other electronic devices from their bags, take off their shoes, and remove their jackets. After placing metallic items in a bin with their other belongings for x-ray examination, they await their turns to move on to the body screening process.

Passengers then walk through a magnetometer or pause in a large tube while raising their hands above their heads. Not knowing what the machines see, detect, or take pictures of can make people who are normally calm exhibit behavioral patterns that security personnel could confuse with potential criminal indicators. After this, depending on the behavioral indicators they are exhibiting, security personnel may pull passengers aside to undergo additional screening. During the body-screening process, passengers are temporarily separated from their personal items. The increased possibility of forgetting or misplacing something also could compound passenger stress.

In the United States, the multiple layers of security to enhance aviation transportation security tend to rely more on machines than on people. The U.S. Transportation Security Administration (TSA) acknowledges on its website that, "The suite of technology has grown considerably in the years since TSA took over airport security…. You may notice some new and unfamiliar machines at your local

airports." Security devices are more costly, and often perceived as more effective, than their human counterparts. Unfortunately, this perception may compound security problems at U.S. airports nationwide.

Training – An International Priority

Training all personnel, especially at the high level required for a truly robust aviation security program, is not easy and can be costly. This is as true in the United States as it is in Mexico. Effective training for personnel on the ground as well as in the air – in addition to advanced technology – creates a more robust, and more reliable, multilayered security environment.

Security managers and politicians in both countries should examine their own aviation security training programs. By training personnel to use observations to fill in the necessary security gaps and by establishing a culture of teamwork and reliance on personnel, the governments and security agencies in both the United States and Mexico could build a safer and more effective aviation transportation system.

Clay W. Biles is a former U.S. Federal Air Marshal (13 April 2008 to 30 May 2013). He currently lives and works in Mexico assisting high-risk personnel. He received the Distinguished Honor Graduate Award for his air marshal training class, and from 2011 to 2012 served as the lead firearms instructor for the Service's San Francisco Field Office. He is a former U.S. Navy corpsman, Stanford Medical Center researcher, and bodyguard (for President Hamid Karzai of Afghanistan). His new book and first-hand account of the Federal Air Marshal Service will be available in August 2014.

The Team Spirit of Emergency Management

By Stephen Grainer, Emergency Management

The primary purpose of every emergency management system is to bring about change. Fundamentally, the purpose of an emergency services organization is to change the outcome of a potential or actual emergency from that which might occur if there is no intervention. This includes a series of tasks that emergency services must continuously repeat:

- Preventive measures intended to avert an incident;
- Mitigation steps intended to reduce the consequences of an adverse situation;
- Preparedness steps (including training) to develop a readiness to act quickly and appropriately when an incident begins to evolve;
- Response actions once an incident occurs; and
- Post-incident recovery activities.

Agents of Change – Teams & Organizations

In order to achieve desirable change, the emergency services community frequently employs various organizations often referred to as "teams," including: hazardous materials response teams; technical rescue teams; incident management teams; spill response teams; special weapons and tactics teams; technical assistance teams; community emergency response teams; and highway incident response teams. Organizations and "teams" are an integral part of the emergency management system by providing a framework for conducting missions and performing tasks based on identified or perceived needs. Therefore, whether referred to as an organization or a team, all are "agents of change."

In order to develop a "team," it is important to first establish an organization. According to the *Webster's New World Dictionary (Second College Edition)*, an organization is "a body of persons organized for some specific purpose as a club, union, or society." The *Business Dictionary* defines an organization as, "A social unit of people that is structured and managed

to meet a need or to pursue collective goals." This definition continues to note that, "Organizations are open systems – they affect and are affected by their environment." As such, all of the above-mentioned "teams" are certainly organizations because they are assemblies of people for a specific purpose. However, although organizations frequently exist or evolve for specific purposes, the degree to which those organizations function as teams can vary greatly and, therefore, produce greatly varied outcomes.

Webster's New World Dictionary (Second College Edition) offers one definition of a team as, "a group of people working together in a coordinated effort." Certainly, all of the above listed organizations are teams based on this definition. The *Business Dictionary* has a more descriptive definition of a team as follows: "A group of people with a full set of complementary skills required to complete a task, job or project." In addition, the definition states, "Team members (1) operate with a high degree of interdependence, (2) share authority and responsibility for self-management, (3) are accountable for the collective performance, and (4) work toward a common goal and shared reward(s). A team becomes more than just a collection of people when a strong sense of mutual commitment creates synergy, thus generating performance greater than the sum of the performance of its individual members."

Football teams, pit crews, and emergency management each require effective teamwork in order to be successful. One "superstar" is not enough.

Team Traits – Trust & Anticipation

When assessing if there may be a difference between the capability, the capacity, or even the productivity of an organization versus that of a team, these definitions, particularly the statements drawn from the *Business Dictionary*, offer some insight. According to both sources, organizations largely support the emergency management system and provide the primary framework and personnel management system to perform the personnel's assigned or assumed activities. Therefore, organizations are essential to emergency management. Beyond that, however, the evolution or development of teams from organizations provides a higher level of performance by the personnel involved. When members develop a "mutual commitment" and "operate with a high degree of interdependence," as characterized in the *Business Dictionary* definition, the team can deliver results that are greater than the sum of its parts.

Teams are often identifiable by two key traits: trust and anticipation. Team members trust that their teammates are capable of and will perform at maximum output for the betterment of the team as a whole. Trust most often develops through familiarity – the greater the degree of familiarity, often the greater the degree of trust that occurs among members. As each member becomes familiar with the other members and learns their strengths and weaknesses, he or she can readily anticipate what the other team members will do.

The ability to accurately anticipate or forecast actions or reactions on the part of each other enables all members to be intimately involved in all team activities without hesitation or uncertainty. This significantly increases the efficiency and effectiveness of the team. Additionally, as an organization evolves into a team, all members develop the ability to foresee situational or incident-related actions more effectively. As such, the team can better position itself and be prepared for impediments or disruptions that may occur.

Two Team Examples – Football & NASCAR

A dedicated team typically reflects collective excellence rather than individual stardom. For example, when a sports team has a "superstar," the individual may standout whereas the group's performance may be mediocre. Conversely, a team composed of "average" performers who trust each other can achieve a much higher level of output by anticipating each other's actions. Sports replays often reveal the teammates' trust and ability to anticipate. For example, the so-called "timing pass" in football demonstrates a series of steps requiring trust and anticipation between the quarterback and his teammates:

- The quarterback and wide receiver trust that the other players will execute their blocks and diversionary pass routes;
- The quarterback trusts that the wide receiver will be at a certain point on the field at a certain moment;
- The quarterback throws the pass while the receiver is still running, sight unseen, to that spot;
- The receiver anticipates the arrival of the pass to that point at a specific moment in time; and
- By trusting and anticipating each other's actions as well as the collective team performance, the receiver has the opportunity to complete the pass.

In another example, the actions of a NASCAR (National Association for Stock Car Auto Racing) pit-crew are interdependent yet performed with a choreography that visually demonstrates intense trust and anticipation on the part of every member of the crew. The ability of the team to change four tires, manually refill a tank of fuel, and return the car to the track in under 20 seconds with the deafening roar of many engines and other cars whizzing by is nothing short of remarkable. Both sports-team examples reflect a commitment and a common focus that require much time and repetition. Of course, in both instances, disruptions can and do occur; however, an experienced and seasoned team typically finds a way to overcome those disruptions with minimal adversity.

Key Factors – Time & Repetition

Two factors in the evolution of a team from a basic organization are time and repetition (practice). The most practiced (time together) teams generally perform at a higher level of productivity. If nothing else, the opportunity afforded by the time to practice and refine skills and team productivity enables all members, and the team as a unit, to elevate its output. Over time, the team members develop shared values, embrace the team mission, and reinforce team engagement and commitment from within.

One relatively frequent impediment to full "team" performance involves circumstances that require ad hoc team formation – sometimes referred to as "plug and play." In this scenario, either an organizational framework is not in place or a member(s) of a team is unavailable, thus requiring alternate staffing. Individuals assembled may have minimal, if any, familiarity with each other and may not have a commitment to the mission or to specific tasks. A period of familiarization often is required before a team can begin functioning at the organizational level. When two or more people come together without previous interaction, it is necessary that they develop a degree of familiarity and a comfort zone with the others' expectations and performances. This can delay effective interaction and productivity for hours, days, or perhaps even longer.

In essence, teamwork becomes both an objective and a process as an organization evolves toward true team capability. To achieve these objectives, organizations seeking to achieve full "team" capacity must dedicate themselves to a regular plan or schedule of activities that promote working together. Some organizations have or create regular opportunities to drill or practice annually, semiannually, or quarterly. This ensures that the team philosophy and performance capability does not atrophy, especially when there are no actual or impending emergencies. Frequent interaction also builds a stronger level of trust through greater familiarity. Often these organizations also direct efforts to self-analysis in order to identify areas for improvement and strengths to build upon for future trainings, practices, or drills.

In summary, whether an emergency management organization can be characterized as a team consistent with the definitions provided or not, it should continuously capitalize on the efforts and opportunities afforded to develop a dedicated team. The public as well as stakeholders within the organization or team deserve to have every member of the organization support the purpose and efforts of the team and assume responsibility for its performance. To ensure a high quality of service during any disaster, it is critical that each organization strives to perform as a team.

Stephen Grainer is the chief of IMS programs for the Virginia Department of Fire Programs (VDFP). He has served in Virginia fire and emergency services and emergency management coordination programs since 1972 – in assignments ranging from firefighter to chief officer. He also has been a curriculum developer, content evaluator, and instructor, and currently is developing and managing the VDFP programs needed to enable emergency responders and others to meet the National Incident Management System compliance requirements established by the federal government. From 2010 to 2012, he served as president of the All-Hazards Incident Management Teams Association.

BioFire Defense has led

the industry for over 15 years

in pathogen identification

technologies.

Now, more than ever

we remain committed

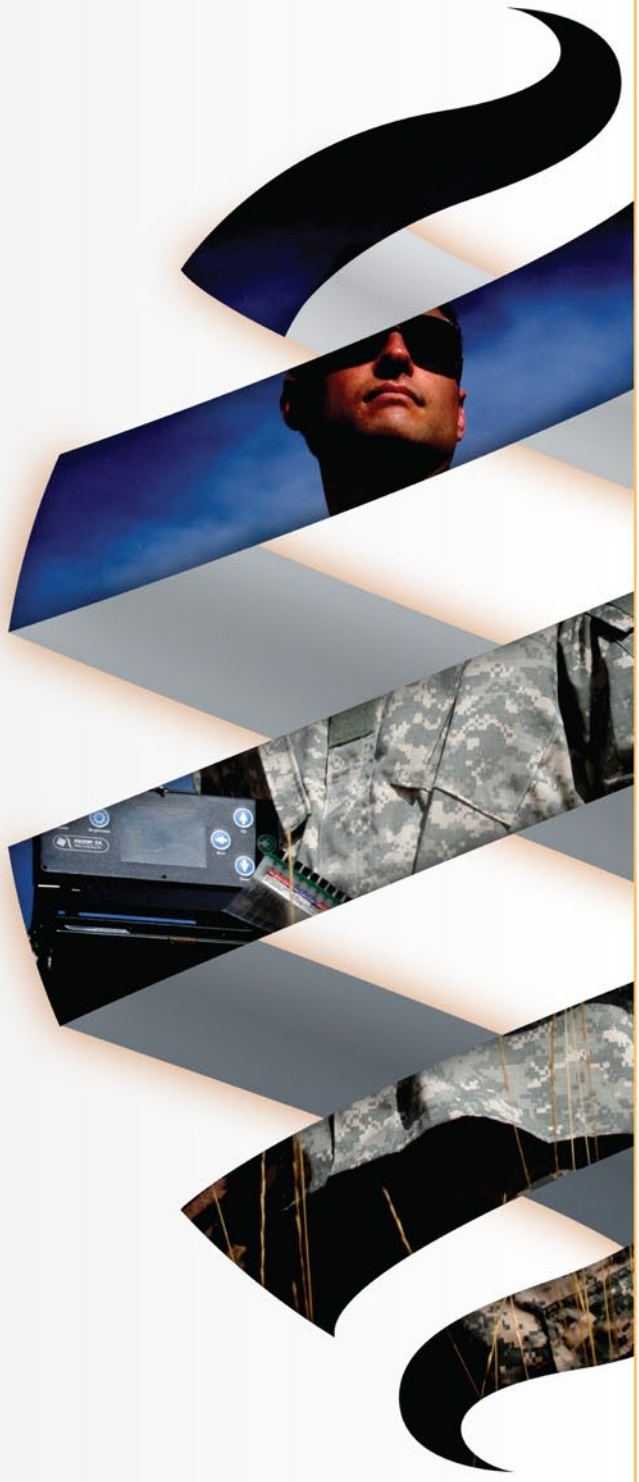
to providing the industry

with superior products,

unsurpassed customer support,

and a solid future of

innovation and design.



Follow us, we'll show you how.

BIOFIRE™

DEFENSE

Follow us at www.BioFireDefense.com