Keeping Contraband on the Outside

Time for the early afternoon shift change. Day shift is leaving the correctional facility and the afternoon shift is coming in. In this security-minded era, as employees enter the facility, everything possible must be done to verify identity and to ensure employees are not bringing contraband into the institution. Depending on the sensitivity of the institution’s portal technology, uniformed staff may need to remove duty belts, restraint sets, uniform insignia and shoes with metal toes before they can successfully pass through. Those that trigger an alarm must stand aside for a more detailed search with a handheld device, often waiting in another line.

Time given up to this process can be time lost in getting the outgoing shift off duty. For that reason, staff feel obligated to move as quickly as possible, but are also held responsible for any prohibited material that passes through undetected. Staff new to the system typically resent the delay and feel offended at the implication of not being trusted to follow the rules.

Checking for contraband typically occurs at either the perimeter gate house, in a lobby or at control points within the institution. Staff, inmates, contractors and visitors are processed through the perimeter of the facility, as are, similarly, large numbers of inmates moving to work assignments within the facility on a scheduled basis. Successful security operations, including those at the institution portals, are seldom the result of one security system in operation. This article presents a quick look at some of the types of technology available.

- RF Metal Detectors. Project low frequency radio waves. As a person passes through the portal, a radio signal is received and interpreted by software to determine whether the person is carrying a metallic object. If the alarm sounds, it means there is a metallic object on the person that falls within the system’s detection limits. When alarms occur, operators usually take the individual aside for an additional search. It does not detect nonmetallic items such as explosives, paper money, drugs, tobacco and prohibited literature.

- Millimeter Wave Detection Devices. Consist of very high frequency radio waves interpreted by software to determine whether a potentially prohibited object exists on a person’s body next to the skin. This technology, which can be active or passive, detects all foreign substances on the human body with reliable results within a reasonable timeframe. However, it does not detect objects within the body such as in the digestive system, the anal canal or oral cavities. The Office of Justice Programs’ National Institute of Justice (NIJ) Information and Sensor Technologies Division sponsored an operational evaluation of (See Keeping Contraband, page 2)

The Office of Justice Programs’ National Institute of Justice (NIJ) has developed a new standard specifically for chemical/biological/radiological/nuclear (CBRN) ensembles for law enforcement. The standard is a vital part of ensuring that law enforcement officers responding to criminal incidents involving the potential for CBRN hazards have appropriate protective gear.

Why a Standard for Law Enforcement?

Traditionally, operations in CBRN environments were believed to be a firefighting and hazmat issue, and the standards for personal protective equipment (PPE) were written primarily for those responders. None of those existing standards fully address law enforcement...
millimeter wave detection portal technology and other efforts are ongoing (see sidebar, “Scanning for Contraband.”)

- **Passive Magnetic Field Metal Detection.** Senses and reports the earth’s natural magnetic field within the space of an opening, then measures the same space when a human is standing in the portal. Interpretative software shows on a monitor the location of any foreign objects on the body of the person. There are no fields of energy radiated at or through the body; this device simply measures what is there naturally. This mobile sensing equipment is not limited to a fixed portal or archway and may be installed in door jambs, walls or other less conspicuous structures. It does not detect contraband located in body cavities.

- **Electric Field Tomography.** Projects weak electrical energy into the body of the person being examined. An interpretation by software provides a graphical view, as if the operator were looking through a person’s body. This technology has the capability of detecting all objects on and within a human body. An NIJ grantee is expected to produce a working model of this developing technology in fourth quarter 2009.

- **Ion Scan Technology.** Typically used to detect drugs and explosives. It detects the ion profile within an air sample associated with a person’s body, vehicle or living space. This portable handheld device must be in close proximity to the person being examined. Time required to complete the scan can be slow.

- **Heartbeat Detection.** Uses geophone sensors combined with interpretive software to listen to vehicles parked in perimeter sally port enclosures for indications of a human heartbeat. Under proper conditions, the information produced is highly accurate and reliable. Compared to the time normally needed to inspect a vehicle and its contents, this technology requires very little staff time.

- **Backscatter X-Ray Contraband Detection.** Available in walkthrough portal design and as a device that searches for contraband on vehicles in sally ports. Backscatter machines use high-energy, low-dose x-ray beams that pass over a human body. High-energy x-rays tend to scatter, or “bounce” off of a surface, as opposed to penetrating it like lower energy x-rays used for medical purposes. Backscatter technology, along with millimeter wave detection, is being offered to passengers entering airports as an alternative to manual pat searches if they trigger a metal detection alarm. However, it does not penetrate the skin or detect objects inside the body such as in the mouth, anal opening or digestive system.

All of these systems depend on electronics to support or focus their search efforts. NIJ’s Center Sensors, Surveillance and Biometric Technologies of Excellence (CoE) has many ongoing projects related to portal detection. To learn more about this CoE’s activities, visit [http://www.justnet.org/coe_surveillance/Pages/home.aspx](http://www.justnet.org/coe_surveillance/Pages/home.aspx) or call (888) 424-8424. The Weapons and Protective Systems Technologies CoE, in partnership with the National Law Enforcement and Corrections Technology Center (NLECTC) Rocky Mountain, coordinates research and activities in the correctional environment. Visit [http://www.justnet.org/coe_ppe/Pages/home.aspx](http://www.justnet.org/coe_ppe/Pages/home.aspx) or call (814) 865-7098.

NIJ is currently in the process of revising its standards on both walkthrough and handheld metal detectors. New versions of these standards should be published in the near future. The Rocky Mountain Center provided background research for this article.
A baggie containing aspirin, tucked in a pocket. A vinyl cell phone, dropped down inside a tacked-in shirt. Extra cash folded and put away outside of a wallet. All contraband items inside a correctional facility, none of them detectable by a standard walk-through metal detector, able to slip through the system.

That is, until now. The Pennsylvania Department of Corrections (DOC) State Correctional Institution at Graterford has had so much success using a new active millimeter wave scanner that during its testing phase, visitors who had been caught by it on prior trips began calling to ask if the day of their next planned visit was a day the scanner would be in operation.

Graterford, the largest maximum security facility in Pennsylvania with an inmate population of approximately 4,000, handles around 32,500 visitors annually, all of whom must be checked to ensure that they are not bringing contraband into the facility. Contraband, in the eyes of correctional facility staff and administrators, is not limited to weapons; it also includes money, controlled and uncontrolled pharmaceutical or chemical substances, pornographic materials, cell phones and pagers, and digital storage devices. None of these items can be detected by standard walk-through metal detectors.

With that in mind, the Pennsylvania DOC, an active member of the National Law Enforcement and Corrections Technology Center (NLECTC)-Northeast Regional Advisory Council, decided to evaluate active millimeter wave scanning technology as a possible solution and called on NLECTC-Northeast for assistance in evaluating its effectiveness. NLECTC is a program of the Office of Justice Programs’ National Institute of Justice.

Millimeter wave detection technology consists of very high frequency radio waves at extremely low power levels that are interpreted by software to determine whether a foreign object exists on a person’s body next to the skin. Some devices actively project the energy at the person’s body and others passively compare the level of illumination emitted by the body compared with a spot blocked by an item. The limitations of this type of system are that it is expensive (more than $150,000 per unit) and does not detect objects within the body such as in the digestive system, anal canal or oral cavities.

This same technology is presently in use by the U.S. Department of Defense in support of the global war on terrorism and the Transportation Security Administration. Its scanning capability penetrates clothing to reveal hidden weapons, explosives, drugs and other contraband.

A vendor installed the equipment and trained correctional personnel in October 2007, and NLECTC staff members made a site visit to perform the evaluation in January 2008. A preliminary report, Millimeter Wave Body Scanning Technology in a Corrections Environment, is undergoing review for publication in the future.

“We did an exercise to gather information, including observing visitors entering the facility,” says Fred Sestito of NLECTC-Northeast. “Graterford has a very detailed and successful operation, and we were able to collect some lessons learned that made the technology even more valuable.”

The evaluation showed a major deterrent effect and a positive ability to detect a wide variety of nonmetallic contraband, thus stopping far more items from entering than using standard walkthrough detection equipment alone. Some of this deterrent effect could be attributed to their concept of operations (ConOps), because as noted previously, perception of the capabilities of this system caused visitors to not attempt to bring in as much contraband.

“It’s an incredible technology, much more effective than standard metal detectors,” Sestito says. “In the correctional environment, there are all types of contraband that aren’t weapons, but can cause some very big problems if they’re smuggled inside. This can look right through the clothing all the way to the skin, although it can’t see through the skin. If someone is trying to bring in something hidden in a pocket, they’re going to find it.”

The system in use at Graterford, the ProVision 100 Body Scanner, has potential peak throughput levels of 300 to 600 people an hour, far faster than most other screening methods. It can be configured for single scanner or multilane use, and requires only a brief multidimensional scan to identify contraband hidden anywhere on an individual’s person.

The system can easily be configured to meet specific throughput and facility requirements. With the system in operation, an individual walks into the portal and raises both arms. One bank of transmitter/receivers is located in front of the individual, and the other to the rear. The device rotates around the individual, emitting millimeter waves and recording the results in a three-dimensional holographic image of the individual, who then steps out of the portal. A trained operator analyzes the scan, and if nothing is detected, the person continues on through the checkpoint. However, if a suspicious object is detected, the individual may then be subjected to a search directed at the general area where the suspected contraband was indicated.

In addition to the previously mentioned phone calls during the training period (when the technology was not in daily use), Graterford is finding less and less contraband as repeat visitors learn they are going to be caught, so it is pointless to try to smuggle items in. Visitors caught with legal items, such as cell phones or extra cash, can continue with their planned visits after the property is confiscated and placed in a locker. However, if correctional staff find individuals carrying illegal substances, the officers hold them as suspects for local law enforcement.

NIJ’s Sensors, Surveillance and Biometric Technologies Center of Excellence (CoE) has many ongoing projects related to body scanning devices. To learn more about this CoE’s activities, visit http://www.justnet.org/coe_surveillance/Pages/home.aspx or call (888) 424-8424.


For more information on this project, contact Fred Sestito of NLECTC-Northeast at (888) 338-0584, e-mail Fred.Sestito@L-3COM.COM.
The use of lasers to disrupt aviation operations was designated as a threat and research focus by NLECTC-West in 1997. Since then, the Center has documented more than 300 case incidents of attempted or actual disruption by lasers. Significant case studies have been identified in the NLECTC-West publication, “Tactical Laser Devices and Weapons, A Guidebook for Law Enforcement.” This occasional paper has been available for law enforcement use through the NLECTC-West system of publications, outreach and technical assistance since 2001. It has been revised and updated within the past two years.

For more information, contact the West Center at (888) 548-1618.
Offering no-cost assistance to law enforcement and corrections agencies and crime laboratories — large or small, rural or urban — in the implementation of current and emerging technologies, the National Law Enforcement and Corrections Technology Center (NLECTC) system is an integrated network of centers, specialty offices and criminal justice technology Centers of Excellence located across the country.

Established in 1994 by the Office of Justice Programs’ National Institute of Justice (NIJ) as part of its research, development, testing and evaluation initiatives, the NLECTC system serves as an “honest broker” resource for technology information and assistance and helps introduce technologies into practice within the criminal justice community.

The NLECTC system seamlessly delivers its expertise to the Nation’s 19,000-plus police agencies; 50 state correctional systems; thousands of prisons, jails, and probation and parole departments; and crime laboratories in a number of technology areas. These technology areas are supported by technology partners who provide the leveraging of unique science and engineering expertise. In addition, technology working groups and a national advisory council provide guidance relating to the technology needs and operational requirements of the public safety community for NIJ’s various technology focus areas and ensure a focus on the real-world needs of public safety agencies.

Contact NLECTC for:  

Technology Identification  
The NLECTC system provides information and assistance to help agencies determine the most appropriate and cost-effective technology to solve an administrative or operational problem. We deliver information relating to technology availability, performance, durability, reliability, safety, ease of use, customization capabilities and interoperability.

Technology Assistance  
Our staff serves as proxy scientists and engineers. Areas of assistance include unique evidence analysis (e.g., audio, video, computer, trace and explosives), systems engineering, and communications and information systems support (e.g., interoperability, propagation studies and vulnerability assessments).

Technology Implementation  
We develop technology guides, best practices and other information resources that are frequently leveraged from hands-on assistance projects and made available to other agencies.

Property Acquisition  
We help departments take advantage of surplus property programs that make federal excess and surplus property available to law enforcement and corrections personnel at little or no cost.

Equipment Standards and Testing  
We oversee the development of performance standards and a standards-based testing program in which equipment such as ballistic- and stab-resistant body armor, double-locking metallic handcuffs and semiautomatic pistols is tested. NLECTC also conducts comparative evaluations (testing equipment under field conditions) on patrol vehicles; patrol vehicle tires and replacement brake pads; and cut-, puncture- and pathogen-resistant gloves.

Technology Demonstrations and Capacity Building  
We introduce and demonstrate new and emerging technologies through special events, conferences and practical demonstrations such as the Mock Prison Riot™ and an annual public safety technology conference. We also provide hands-on training assistance for the latest technologies through workshops and software programs dealing with crime mapping, community corrections and critical incident management. In addition, on a limited basis, NLECTC facilitates deployment of new technologies to agencies for operational testing and evaluation.

Technology Information  
NLECTC disseminates information to the criminal justice community at no cost through educational bulletins, equipment performance reports, guides, consumer product lists, product information databases, news summaries, meeting/conference videotapes and CD-ROMs. Most publications are available in electronic form through the Justice Technology Information Network (JUSTNET) at www.justnet.org. Hard copies of all publications can be ordered through NLECTC’s toll-free number, (800) 248-2742, or via e-mail at asknlectc@nlectc.org.

Technology Product Network  
The Technology Product Network (TPN) provides one-stop access to information on currently available products for law enforcement and corrections. Vendors and technologists who register with the TPN can upload information about their products, while registered practitioners can participate in discussion forums about the products found in the database. Registered users also receive e-mail notifications of new products that match their specified interests.

I f you could learn more about how to stop people who hang out in chat rooms looking for unsuspecting victims and send fraudulent e-mails about money scams, and the only cost to you would be for transportation, would you be on the next plane, train or car out of town?

Thanks to the National Institute of Justice (NIJ) and Office of Justice Programs (OJP), Mississippi State University operates the National Forensics Training Center (NFTC) to train law enforcement officers about fighting cybercrime, all at no cost to the officers or their agencies. Meals and lodging are provided during the free training; all students have to do is go online to the NFTC Web site and register, then get themselves to the class for which they have enrolled. Classes take place at the Mississippi State University Campus in Starkville and at the Cyber Crime Fusion Center in Jackson, Miss.

If officers cannot come to the training, in some instances the training will come to them. “When the distance is great, so that it doesn’t make sense for single officers to come to Mississippi, and a central agency or resource center will serve as a host, we will discuss coming out to provide training,” says Dr. David Dampier, associate professor of computer science and engineering and director of the center at Mississippi State. “We take it on a case-by-case basis and it just really depends on the situation. We just did one in Marietta, Ga., where they got together a group of people from all over the area.”

NFTC has also previously offered training through the National Law Enforcement and Corrections Technology Center (NLECTC)-Northwest in Anchorage, in February and June 2009. One session was a four-day advanced training course and the other featured back-to-back two-day classes at a more introductory level.

“Obviously, law enforcement officers from Alaska would have a hard time traveling to Mississippi to attend our training, so we were happy to do that,” Dampier says.

NLECTC-Northwest is a program of the Office of Justice Programs’ National Institute of Justice. Bruce Richter, deputy director at NLECTC-Northwest, said the Center was tipped off about the free training by the local FBI field office.

“Compared to other alternatives in the commercial marketplace, the price certainly is right,” Richter says. “The instructors have solid backgrounds and they offer a wide variety of instruction. This is a good venue that law enforcement agencies should be aware of and we’re going to try to keep working with them to schedule more sessions in the future.”

Participants in the sessions at NLECTC-Northwest came from around the state of Alaska and filled every seat in the Center’s training center.

“We had federal, state and local officers from a whole variety of agencies. It was really good stuff,” Richter says. “The courses have this great mix that addresses the practical needs of the law enforcement community and it’s something that agencies need to know about.”

Students were responsible for paying for their own travel, but funding from the state’s Internet Crimes Against Children Task Force supplemented that for officers outside the immediate Anchorage area.

“It was a nice mix. The local FBI was interested, the task force brought in people, and everything all came together to make it a nice opportunity,” Richter says.

Dampier says that when the program started in 2005, NFTC initially had difficulty getting the word out, but as the program continues, word of mouth from agencies such as NLECTC-Northwest is helping publicize the training. NFTC is currently funded through FY 2010, and Dampier says as long as DOJ continues to provide funding, the university plans to continue to operate the program.

NFTC offers 11 different classes onsite, ranging from basic computer use through legal aspects of search and seizure and running the gamut in between. Individuals can also receive certification as a digital crime scene technician or a bit stream imaging technician after completing specific courses and successfully passing an exam.

For more information, visit the National Forensic Training Center Web site at http://www.security.cce.msstate.edu/ftc/.
Streamlining Standards

The National Institute of Justice (NIJ) has adopted a revised method to streamline development of standards.

When NIJ wanted to develop a standard for chemical/biological/radiological/nuclear (CBRN) protective ensembles for law enforcement, the agency set up a special technical committee (STC) in August 2007 composed of practitioners from the field and subject matter experts. The panel met monthly and within a year produced a draft standard that went out for public comment. Previously, development of a standard could take three or more years.

The CBRN ensemble standard was the first developed using the STC method. NIJ was pleased with the relatively speedy development of the standard and is applying the method to develop or update standards for gun-retention holsters and restraints.

“It’s just been great,” says Casandra Robinson, a visiting scientist with NIJ who has been involved in development of the CBRN standard and others that are underway. “That’s why we are repeating the process with other standards.

“We wanted to put out a good standard in a compressed timeframe of one year. Debra Stoie of NIJ came up with the STC process as a means to develop a comprehensive standard in as short a time as possible with all the points of view represented. The practitioners drive the requirements.”

Law enforcement practitioners on the panel came from organizations such as the International Association of Chiefs of Police, the Fraternal Order of Police, the National Tactical Officers Association, the National Sheriffs Association, the Federal Law Enforcement Training Center and the FBI. Also included were representatives from the National Fire Protection Association, the National Institute for Occupational Safety and Health, the U.S. Department of Defense and the Drug Enforcement Administration.

NIJ technical partners like the National Institute of Standards and Technology and the U.S. Army Natick Soldier Research, Development and Engineering Center were also involved in the standards development process. What is unique about the STC process is that it brings practitioners and technical experts together to collaboratively develop the standard.

“It is a standard for police by police, which is an accomplishment by NIJ,” says Edward Bailor, a retired U.S. Capitol Police Inspector who serves as chair of the CBRN Ensemble Standard STC. “We developed it to satisfy the safety and scientific requirements to make the law enforcement professionals safe. NIJ selected a really good team. Others can follow what we have done to make the development of standards easier.”

For information about the STC standards development process, contact Casandra Robinson of NIJ at (202) 305-2396 or casandra.robinson@usdoj.gov.
are similar to those previously mentioned with the exception that there is no potential for flash fire.

**LERL-3.** An LERL-3 ensemble might be worn during a tactical building search where chemical warfare agents or toxic industrial chemicals are present and monitoring has determined the level to be below IDLH or appropriate for the defined limit of the respiratory protection.

This type of mission may require slow and deliberate movements of the team as they systematically clear all areas of a building. Slow and deliberate movements allow the team to search using mirrors, cameras and shields to locate a suspect while limiting exposure to gunfire.

Tasks performed during a slow and deliberate search include remaining in a stationary position at low ready for extended time periods, carrying a ballistic shield as temporary cover, opening doors while maintaining a position of cover, searching remotely using pole mirrors and/or pole cameras and communicating with and securing suspects. Hazards could include moving past barricades or trip wires set by the suspect, combative subjects and kneeling or crawling on sharp objects.

**LERL-4.** An LERL-4 ensemble might be worn when police are establishing a perimeter around an area where chemical warfare agents or toxic industrial chemicals are present and monitoring has determined the level to be below IDLH or appropriate for the defined limit of the respiratory protection.

This type of mission may require officers to remain on a fixed post for an extended period of time. Officers may potentially need to control contaminated persons from exiting the area or other persons from entering a contaminated area.

Tasks performed during a perimeter security operation include communicating over a radio; directing vehicular and pedestrian traffic; controlling agitated, panicked and/or sick individuals; communicating with groups of people and securing non-compliant individuals. Hazards could include moving traffic, combative individuals, kneeling on sharp objects and heat stress from exertion for extremely long durations.

**Related Documents**

In addition to the standard, NIJ will be publishing the *NIJ CBRN Protective Ensemble Certification Program Requirements* and the *NIJ CBRN Protective Ensemble Selection and Application Guide*. The certification document addresses how ensembles will be certified as compliant with the standard. The selection and application guide provides procurement, selection, care, maintenance, training and administrative guidance for law enforcement officers, administrators, managers and purchasing agents.

**Method Used for Standard Development**

The *NIJ CBRN Protective Ensemble Standard for Law Enforcement* was the first NIJ standard to be developed using a special technical committee composed of law enforcement practitioners, subject matter experts and scientists. The panel worked together for more than a year to develop the standard and companion documents. (See sidebar, "Streamlining Standards."

“What is important is that the standard was defined and guided and managed under the direction of law enforcement practitioners,” says Stoe. “The practitioners articulated their needs and the scientists and research experts identified or developed the appropriate test methods to measure the specific requirements that were identified by the practitioners.”

NIJ worked closely with partners such as the U.S. Departments of Homeland Security and Defense and the National Fire Protection Association to leverage related efforts where possible to expedite release of the standard. The standard, like all NIJ standards, is voluntary.

To view a copy of the standard, certification document or selection and application guide, visit [www.ojp.usdoj.gov/nij](http://www.ojp.usdoj.gov/nij) or [www.justnet.org/ctp](http://www.justnet.org/ctp).
Fortunately, the above situation happened only in a tabletop exercise: Intrusion Forensic Experiment 2 (IFX 2), held in September 2008 in Rome, N.Y., and designed by the National Law Enforcement and Corrections Technology Center (NLECTC)-Northeast. The exercise’s 19 participants visited virtual offices and labs, collected evidence, listened to video statements and collaborated on a theory of responsibility. When the exercise ended, a post-analysis session helped participants understand the method and motive behind the attack and the actual computer forensic findings. In addition to developing closer working relationships with each other, participants took information on how to create their own tabletop exercises back to their agencies.

The Northeast Center, a program of the Office of Justice Programs’ National Institute of Justice, used lessons learned from IFX 1, held in June 2007, to build on and create IFX 2. Developed at the request of the Upstate New York Electronic Crime Coalition, IFX 1 focused on an incident at a financial institution. Both tabletop exercises were scalable in size, scope and location, all of which would help an agency develop its own exercise.

In IFX 1, developers created a fictitious credit union, including employees, a Web site, a network diagram and information technology policies and procedures such as an incident response plan, acceptable network usage policy and an operations manual. IFX 1, a heavily scripted exercise, had strategically placed decisions for each participant; in IFX 2, the scenario took on a more free-flowing form.

The primary objectives of IFX 2 included raising the awareness level of the participants regarding insider threats, developing and strengthening relationships with and among law enforcement agencies, emphasizing the importance of indications and warnings in identifying cybersecurity issues and stressing the importance of defense in depth and total enterprise/agency security. IFX 2 also had secondary objectives of increasing awareness related to malware capabilities, technology exploitation, insider threats, security countermeasures and the need for strong audits and awareness programs. Participants and observers came from the Air Force Research Laboratory/Information Directorate, the FBI, the U.S. Secret Service, and the Utica (N.Y.) Police Department, in addition to private sector and academia representatives.

“The goal for the first exercise was primarily to build relationships between law enforcement, the private sector and government agencies,” says Tracy Nitti, IFX project manager. “We wanted to get them in the same room and working together so they would be comfortable if they did have to collaborate on a real case.” The majority of the participants in the first exercise belonged to the coalition and its members wanted to build on the groundwork for relationships laid within that group.

“With the second one, we took the success we had with the first exercise and scaled up technically,” Nitti says. “By using a different sector for the crime, we were able to introduce an exercise where the motive and means were different.” Some of the original participants returned for IFX 2; for others, it marked their first exercise.

“We really enjoyed the interaction we had from a technical/social perspective and the way we were able to determine suspects, method of modus operandi, the motivation behind the criminal enterprise and what the individual’s background was,” says Agent Tim Kirk, U.S. Secret Service, of his participation in IFX 2. “All those things together really made a great exercise.”

“I thought the exercise was an excellent opportunity to not only preplan some of our operations and the way we do business, but also a great opportunity to meet the other participants,” says Sgt. Anthony Martino, a computer forensics specialist with the Utica Police Department.

Both exercises were designed for 15 to 20 participants to keep the group at a manageable size. However, for IFX 2, a separate group of observers did watch the exercise from a second room.

“They became so involved and excited, they wanted to participate too,” says the Northeast Center’s Debra Cutler. “These vulnerabilities exist pretty much across the board. Every part of the country could experience these types of problems.”

For more information or to request a copy of the NLECTC-Northeast developed report titled, How to Design a Cybersecurity Tabletop Exercise, contact the Northeast Center at (888) 338-0584.