US Army Corps
of Engineers®

Vol. 1 Issue 1
June 2010
www.hnd.usace.army.mil/esc

The Electronic Security Insider

"Protecting America's resources since 1981"

On page ...

2 New system tests electronic verification of credentials at Letterkenny

7 Ask the MCX

8 Electronic Security Systems Design course dates for 2010

Visit the U.S. Army Engineering and Support Center, Huntsville Electronic Security Center website at www.hnd.usace.army.mil/esc

You can also visit us on Facebook at http://bit.ly/HNCfbPage or Twitter us at http://twitter.com/CEHNC

Technical Bulletin

Photo by Craig Zeigler

New system tests electronic verification of credentials at Letterkenny

The Automated Installation Entry System at Letterkenny Army Depot, Pa., is the Army's first approved installation access control system. For the story go to page 2.

Electronic Security Center has long 27- year history; Utility Monitoring and Controls team multiplies

By John A. Brown Jr.
MCX Technical Deputy
Electronic Security Center

You may have noticed that this newsletter has changed a bit since the last publication. That's because the Utility Monitoring and Controls team has "multiplied" into a new organization. The move means that our previously combined technical bulletin will now be devoted solely to electronic security matters. Consequently, we thought it would be a good idea to re-cap the missions, functions, roles, organization and some history of the Electronic Security Center.

The Department of the Army realized the need existed for a cadre of experts in the specialized field of electronic security systems and they included provision for such a center in AR 190-13, The Army Physical Security Program. AR 190-13 tasked the Corps of Engineers with the

See *ESC history* on page 6

Intrusion Detection system policy: one size does not fit all

By Kevin Haapoja

Determining which policies and standards commanders or directors must comply with when planning for the installation, operation and maintenance of an intrusion detection system (IDS) can be a challenging task.

Policies governing the use of IDS vary depending on the security classification level, along with the type and location of facility or asset you are trying to protect. Trying to use a cookie-cutter approach can get you into serious trouble as one size

See *IDS policy* on page 4

New system tests electronic verification of credentials at Letterkenny

By Debra Valine
Public Affairs Office

Approximately 3,000 employees at Letterkenny Army Depot, in Pennsylvania, are the first to experience a new electronic way to verify an individual's credentials when entering a military installation.

The Automated Installation Entry system is similar to an "easy pass" system used on civilian toll roads to speed up traffic flow.

The U.S. Army Engineering and Support Center, Huntsville, working with the Office of the Provost Marshal General and the Office of the Product Manager, Force Protection Systems, developed a standard Army design for an entry system that will change the way an individual's credentials are verified and speed up the process. The proof of concept demonstration for this type of system was conducted at Fort Hood, Texas.

Other agencies supporting PM-FPS in the endeavor include the Army Test and Evaluation Command for performance evaluation and endurance tests, the Space and Warfare Naval Systems Command for the Defense Information Assurance Certification and Accreditation Program documentation that is processed through Net Command, and the Training and Doctrine Command for review and comment on operators, system administrator and maintenance training documents.

Letterkenny will be the first Army DIACAP-certified Automated Installation Entry system, and one of three installations being used to demonstrate the capability. Huntsville Center is also installing and testing AIE systems at Fort Campbell, Ky., and the Military Ocean Terminal Sunny Point, in Southport, N.C. The three locations represent different types of installations where AIE will be installed.

The technology is mature, commercial-off-the-shelf technology that proves the AIE

continued on next page

Insider

US Army Corps of Engineers®

The Elctronic Security Insider is published by the Electronic Security Center, U.S. Army Engineering and Support Center, Huntsville. Inquiries can be addressed to Electronic Security Center, U.S. Army Engineering and Support Center, Huntsville, Attn: CEHNC-ED-ME-S, P.O. Box 1600, Huntsville, AL 35807-4301. Phone: DSN 760-1740 or commercial 256-895-1740. The Electronic Security Insider is also online at ***www.hnd.usace.army.mil/esc*** *or email* ***Contact-ESC@usace.army.mil.*** *The Huntsville Center Facebook page is located at* ***http: //bit.ly/HNCfbPage.*** *The Twitter page is located at* ***http://twitter.com/CEHNC.***

Printed on recycled paper
30 percent post-consumer

Letterkenny

continued from page 2

system can work in accordance with Army standards. It is likely that the system once perfected, could be adopted by other services and defense agencies, potentially improving security at military installations across DoD.

"AIE incorporates access control technology, combined with policy and procedure revisions, that will enhance security, standardize access control point technological requirements and provide commanders a flexible force protection solution," said Gregory R. "Jay" Jones, Office of the PM-FPS.

Before the AIE system can be installed, the existing infrastructure at the Access Control Point has to be upgraded. This work is being executed by Huntsville Center's Access Control Point Equipment Program for the U.S. Army Corps of Engineers. Upgrades include guard booths, active vehicle barriers, traffic islands, overhead canopies, power/conduit/wiring and incidental paving.

Installation of the AIE system includes electronic and computer assemblies, optical and mechanical assemblies, conduit and wiring. The major elements of the AIE are the ACP with vehicle lanes, an enrollment center, a visitor control center and data centers.

The AIE mission is to automate access control in order to:

- Enhance security by verification/ authentication of credentials, vetting of individuals and establishing permissions to control access
- Reduce guard requirements/costs at access control points
- Maintain or increase traffic throughput at gates.

To be able to use the system, individuals and vehicles must be registered on the installation.

"The AIE work at Letterkenny was awarded in two phases," said Jeffrey Mitchell, Electronic Security Systems program manager, Huntsville Center.

"In phase one, the prep work at the site was assessed to ensure AIE equipment could be procured and installed. Follow-on was to complete and deliver a technical design. In phase two the equipment was procured and installed.

"The project presented unique challenges because this was a PM-FPS 'program of record' where we had to engage other agencies through PM-FPS to execute this project," Mitchell said.

"Whenever you have a new system that will be tied to an Army network, you have to ensure the information processed on that system will be secure," said Craig Zeigler, ESS physical security specialist. "The system has to be certified and accredited to be networthy; that it can be plugged in and talk computer to computer without corrupting the Army network."

"Once the system was installed, it was tested in accordance with an Interim Authority to Test provided by NETCOM," Mitchell said. "Performance Verification Tests were completed by ATEC in August 2009 and follow-on Endurance Tests that started in September were completed Oct. 22, 2009. The next step is the Authority to Operate, which is approval to use the system on the Army network."

"The automated installation entry program has the potential to be one of our greatest assets. It would be like owning a tricycle and then upgrading to a '65 Ford Mustang," said Lt. Col. Robert Leasure, deputy director of Risk Management at Letterkenny. "The project at Letter-kenny will be the tip of the spear for the Army and could lead us into a joint venture with other services."

"Whenever you have a new system that will be tied to an Army network, you have to ensure the information processed on that system will be secure"

— Craig Zeigler
ESS physical security specialist

IDS Policy

continued from page 2

clearly does not fit all. Your first step when determining which policies are applicable should be to coordinate with your installation and organization's security specialist.

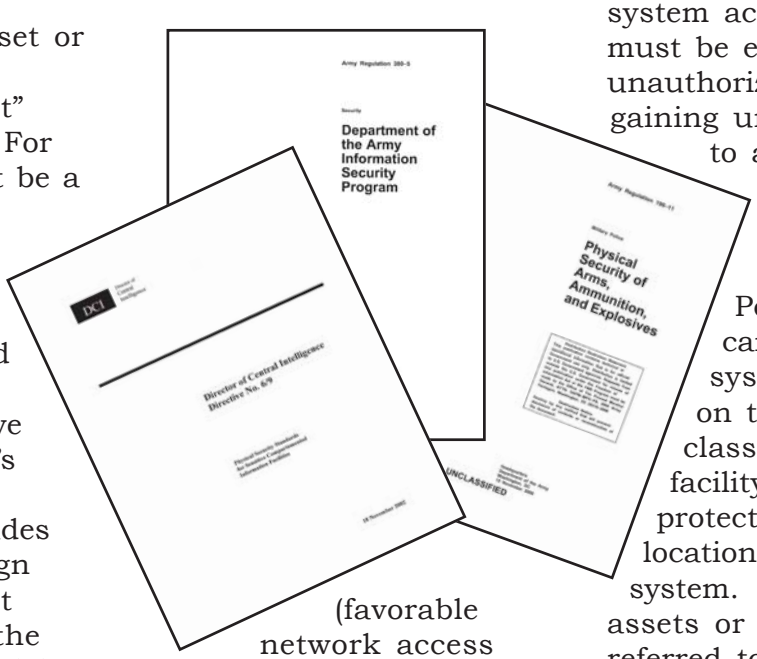
Location, location, location

Determining which policies and standards are applicable becomes even more challenging when the asset or facility you are trying to protect resides on a "host" installation or property. For example, your host might be a different U.S. military service or even a "host nations" military or government property. Not only are you required to comply with your own policies, but you may have to comply with your host's policies as well.

Another example includes facilities located in foreign countries that have strict laws/policies regarding the use of closed circuit television (CCTV). In many countries, these policies may affect the use, panning ability, viewing angle, and recording ability of a CCTV system.

Installation/Maintenance

Policies governing who can install and maintain your system is also dependent on the level of security classification of the facility or asset you are trying to protect. Again, each proponent for the asset may have published their own regulation with varying security criteria. For example, AR 190-11 states that Civilian contractors must be U.S. citizens possessing a minimum of a CONFIDENTIAL clearance to install and maintain IDS in an arms storage facility. On the other hand, Director of Central Intelligence Directive (DCID) 6/9 states that certified alarm technicians need only be U.S. citizens who have been subjected to a trustworthiness determination



(favorable network access control [NAC] with no clearance required) to be able to initially install and maintain an alarm system in a sensitive compartmented information facility (SCIF).

System Administration

Published policy regarding who may program the systems monitoring end (head-end) during initial installation and who may administer/operate the head end after installation is limited. Many policies don't distinguish between the equipment installed in the protected area from that installed in a centralized monitoring station. Legacy systems did not store personal identification numbers (PIN) in the system and the functions that an administrator could perform were limited. However, newer state of the art systems allow greater ability to control all functions of the systems and can store sensitive user and PIN information. Therefore, strict policies and controls regarding system access or permissions must be enforced to prevent unauthorized persons from gaining unauthorized access to areas in the system/software.

Monitoring

Policies governing who can monitor your system largely depend on the level of classification of the facility or asset you are protecting as well as the location of the monitoring system. For example, if the assets or areas, otherwise referred to as "zones", are considered unclassified, SECRET, or below work or storage areas, organizations have greater flexibility choosing who will monitor the systems. However, if the monitoring is centralized and the monitoring zones are categorized as Classified, TOP SECRET or part of a Special Access Program then the monitor(s) must be operated by U.S. citizens who have been subjected to a trust-worthiness determination (favorable NAC with no clearance required).

continued on next page

IDS Policy

continued from page 4

DIACAP

Originally, IDSs were designed with generic relays and switches and were not very sophisticated. Today's IDSs are computer hardware and software-based and more sophisticated to program and administer. Because these newer systems are IT-based systems, they may be required to be certified and accredited in accordance with the DoD Information Assurance Certification and Accreditation Process (DIACAP) to ensure proper IT security baselines and encryption standards are met. Having an approved DIACAP is required for all information systems including IDS if transmitting signals over a shared network. It's critical for IDS planners to coordinate with their Information Assurance (IA) professionals early in the design process.

Questions planners/commanders need to know that will assist with determining which policies/standards should be considered are:

1. Who owns the asset or facility? (i.e., U.S. Army, Air Force, GSA, government, commercial company, etc.)
2. What is the asset or facility you are trying to protect? (i.e., people, classified information, AA&E, Chemical/BIO, etc.)
3. Where is the asset or facility? (i.e., CONUS or OCONUS, on a controlled installation or off)
4. Who will be operating and monitoring the system(s)? (i.e., U.S. civilian or military security, contract security guards, local nationals, etc.)
5. Where will the system be monitored and where will the response force come from? (i.e., military police, local civilian police, private security company, etc.)
6. How do you plan on maintaining the system? (i.e., in-house technicians, contracted technicians, etc.)
7. What existing infrastructure is available and could be used to establish the necessary communication link required for monitoring and administering the system? (i.e., internal copper or fiber network, government or commercial telephone lines, etc.)
8. Has an Information Assurance manager been included in the planning process to ensure all required Information Assurance policies are complied with?

Remember, one size (policy) does not fit all. Determining which policies and standards must be complied with can be a challenging task. Your installation or higher headquarters security professionals are available to assist you when planning for IDS. Our great teams here at the U.S. Army Engineering and Support Center, Huntsville, Mandatory Center of Expertise are also available to help you ensure compliance with the appropriate policies governing the design, installation and maintenance of your systems.

The following are some of the policies, standards and reference documents used by the Army:

U.S. Army Publications: www.apd.army.mil/
- AR 25-2, Information Assurance
- AR 190-11, Physical Security of Arms, Ammunition, and Explosives
- AR 190-13, The Army Physical Security Program
- AR 380-40, Policy for Safeguarding and Controlling COMSEC Material
- AR 380-381, Special Access Programs (SAPS) and Sensitive Activities

U.S. Army Corps of Engineers Publications:
www.hnd.usace.army.mil/techinfo/engpubs.html
- UFGS 28 20 02 - Central Monitoring Services for Electronic Security Systems
- UFGS-28 16 00.00 20 - Basic Intrusion Detection Systems (IDS)
- UFGS-28 20 01.00 10 – Electronic Security System (ESS)

Department of Defense Publications:
- DoD Financial Management Regulation (DoDFMR), DoD 7000.14-R, Vol 5, Chp 34 "Financial Institutions on DoD Installations" (i.e., Banks and Credit Unions and other Finance Distribution Centers / Activities) www.defenselink.mil/comptroller/fmr/
- DoD Instruction 8510.01, DoD Information Assurance Certification and Accreditation Process (DIACAP) www.dtic.mil/whs/directives/corres/pdf/851001p.pdf

Defense Central Intelligence Directive:
- DCID 6/9 Security of Sensitive Compartmented Information (SCIF) www.fas.org/irp/offdocs/dcid.htm.

NOTE: DCIDs will be converted to an ICD (Intelligence Community Directive) and those can be found at www.fas.org/irp/dni/icd/index.html.

Photo by Becky Proaps

The Electronic Security Center team from left to right, first row: Lavance Griffin, Daryl Britton, John Corcetti, Leigh Young, Joy Jackson, Donna Lawson, Mike Lewis and Kimberly Torrence; second row: Donnie Lambert, Buland Mahmood, Steve Willoughby, Darrel Anerton, Sara Covey, Michael Bailey, Aaron Scott and John Brown. Third row: Wayne Grantham, Ken Johnson, Kevin Haapoja, Bill Goff, Piet Vanderhoeven and Craig Zeigler.

ESC history

continued from page 1

mission. Soon thereafter, the establishment of the center of expertise came about when the U.S. Army Engineering and Support Center, Huntsville was officially designated the intrusion detection systems mandatory center of expertise (IDS-MCX) on Dec. 2, 1983. The roles of the new organization were formalized in the initial Program Management Plan issued on Dec. 4, 1984.

Consisting of a staff of only five engineers, the IDS-MCX became a resource for U.S. Army elements at both the major command (MACOM) and installation level. The development of a technical manual and a family of Corps of Engineers guide specifications began and these documents have set the standard for procurement and application of electronic security systems ever since.

The technical manual formed the basis for an Electronic Security Systems Design Course which has been taught to thousands of students around the world. Since then, the Electronic Security Center (ESC), as it has come to be known, has evolved into a major organization within Huntsville Center. After several years of providing only engineering and technical support, our customers' needs drove expansion of the team's capabilities to include system procurement and installation, maintenance and other specialized support.

As ESC capabilities grew, so did our customer base. In addition to our primary mission customer (U.S. Army), relationships with customers from other Department of Defense agencies and a number of non-DoD agencies were established. ESC customer relationships have resulted in hundreds of successful projects such as the Smithsonian Institution, chemical demilitarization facilities, and landmarks such as the Statue of Liberty. These projects cover the full range of scope and complexity from special studies to criteria documents to site surveys, designs, and installations, maintenance and monitoring.

Today, the ESC provides engineering, training and other specialized technical support to our customers. These types of support are generally provided by our MCX team while our procurement and installation team provides customers the capability to buy and install electronic security systems and related equipment anywhere in the world. Within Huntsville Center, the functional directorates are called upon to staff the ESC integrated product delivery team. The team is made up of approximately 40 talented individuals primarily from the Engineering, Installation Support and Programs Management, and Contracting directorates. Additional support is provided by Resource Management, the Office of Counsel and other offices. The ESC's people are the primary resource used

continued on next page

Ask the MCX!

Q: Which type of electronic locking mechanisms are preferred when designing a new C2 facility, electronic locksets or electric strikes? Should the concern be strictly cost or fail safe, fail secure criteria?

A: We recommend the use of heavy duty electric strikes over electrified locks for the following reasons — safety and security, ease of installation and familiarity with installation for most installers.

Electric strikes are commonly used on most installations and are generally preferred because they maintain the mechanical functionality of the door. In short, if they fail, you can still use the lock and key to secure the door. The preservation of this mechanical functionality is also popular with the Authority Having Jurisdiction (AHJ) for life safety concerns. Also, strikes are commonly used and relatively easy to install.

Electrified mortise locks are secure and generally provide a safe solution as well. In fact, some door hardware installers prefer this type because they feel they are more secure. However, there are several things you must consider prior to using this solution.

First, you MUST have an experienced door hardware installer. If not properly installed, these locks will cause the door handles to heat up and may cause the lock to malfunction such that the door cannot be locked and secured. The electric current draw required for electric latch retraction can be up to 16 amps for a Von Duprin model which well exceeds the current requirement of the commonly used 22 AWG (American wire gauge) conductors and requires a much larger (and more expensive and difficult to work with) conductor. For frequently used doors, you must use Electric Power Transfer

See *Ask the MCX* on page 8

ESC history

continued from previous page

to meet our customers' requirements and needs. Our open-ended contract families allow us to provide architect-engineer services, engineering services, and procurement/installation services to meet customers' needs anywhere on the planet.

The Electronic Security Center will continue providing the full complement of high quality support available to our customers today. Our fifth-generation procurement/installation contracts will be awarded this year and they will become our mechanism to execute projects for the next several years. The ESC monitors technological and product developments within the industry and is postured to incorporate new systems and equipment to enhance customers' security needs and help mitigate risk in the most cost effective manner possible.

For example, as our world continues to morph into a network-centric enterprise, ESC is seeking out every opportunity to help maximize the impact of our customers' resources by leveraging existing network infrastructure without compromising the integrity of the time critical event reporting associated with electronic security. No doubt, the ESC will recommend and apply network-based electronic security systems for some customers' requirements as technology and reliability of commercially available systems matures within the industry. The ESC will seek to establish new customer relationships while we continue to strive to be the provider-of-choice for our existing customers as well.

Now in its 27th year, the ESC has established itself as a leader in electronic security systems engineering and application. As the MCX for electronic security systems, ESC provides the full range of engineering support including engineering criteria development, conceptualization, criteria documents, training and testing.

ESC also provides the full complement of electronic security systems technical services including survey, design, procurement, installation, testing, acceptance, maintenance and monitoring. As technology matures and requirements evolve, the ESC is postured to adapt by employing proven systems and equipment to meet customers' specific needs.

2010 Electronic Security Systems (ESS) Design Course Dates

June 14 - 18 — Huntsville, Ala.
July 26 - 30 — Germany
Aug. 16 - 20 — Destin, Fla.

If you have any questions, please call 256-895-1740

2010 Integrated Commercial Intrusion Detection System (ICIDS) System Administrator Training Dates

June 7-11 — Huntsville, Ala.
Sept. 13-17 — Huntsville, Ala.

For more information, please call 256-895-1740

Security related courses

Defense Information Systems Agency (DISA)	
Information Assurance	http://iase.disa.mil/eta/
Defense Security Service (DSS) Academy	
DoD Security Specialist	http://dssa.dss.mil/seta/courses.html
Sensitive Compartmented Information (SCIF)	
Physical Security Seminar	http://dssa.dss.mil/seta/courses.html
Industrial Security Courses	http://dssa.dss.mil/seta/courses.html
Information Security Courses	http://dssa.dss.mil/seta/courses.html
Personnel Security Courses	http://dssa.dss.mil/seta/courses.html
Physical Security Courses	http://dssa.dss.mil/seta/courses.html
Special Access Program Courses	http://dssa.dss.mil/seta/courses.html
Federal Law Enforcement Training Center (FLETC)	
Critical Infrastructure Protection Training Program	http://www.fletc.gov/training
Physical Security Training Program	http://www.fletc.gov/training
Army Training Knowledge Online (ATKO)	
Physical Security	http://www.train.army.mil/
U.S. Army Corps of Engineers	
Security Engineering & Design Course	https://pdc.usace.army.mil/training/secengg
U.S. Army Military Police School	
Antiterrorism Officer (Basic)	https://www.atrrs.army.mil/
Antiterrorism Officer (Advanced)	https://www.atrrs.army.mil/
Conventional Physical Security/Crime Prevention	https://www.atrrs.army.mil/

Ask the MCX

continued from page 7

(EPT) instead of electric hinges. If electric hinges are used, the wires must be twisted together to achieve the required voltage drop.

Currently, there are issues concerning newly installed electrified locks where they are experiencing the doors heating up and being unable to lock. In fact, some of the door handles have required replacement because they are burning out. We are noticing with all of the new MILCON/BRAC projects that we are reviewing that there appears to be significant use of this type of lock from AE designers. The reason for this is not currently understood.

If you would like our assistance with reviewing your project locking hardware, we stand ready to serve. Please do not hesitate to email or call us if you have further questions or concerns.

If you have a question that you would like to submit, please send your question to Contact-ESC@usace.army.mil.