CECOM DOTS and DASHES

Sustaining our "competitive advantage" at MILCOM

By Kristopher Joseph, CECOM Public Affairs

As the Army continues its expeditionary transition with an emphasis on evolving to a more robust joint network, the Military Communications Conference (MILCOM) was the ideal setting for Army leadership to discuss key initiatives with industry partners.

Aberdeen Proving Ground Senior Commander and Commanding General of U.S. Army Communications-Electronics Command Maj. Gen. Bruce T. Crawford led a five-person plenary panel at the Baltimore Convention Center in Baltimore, Maryland, Oct. 8, 2014, with the topic of 'Fielding the Army Tactical Network.'

"In addition to discussing the topic of 'Fielding the Army Tactical Network,' we also stressed the importance of sustaining our competitive advantage and identifying those critical areas where Army and industry can team up to make a difference now, as we begin the dialogue on how we will deliver network capabilities for the Force of 2025," Crawford said.

Crawford was joined by Col. Mark Elliot, Director of the Army's LandWarNet Mission

cover story continued on next page

Can you decode what's in this box?

"-.-. -.-- -... . .-. ... . -.-. ..- .-. .. - -.-- .. ..- . .-. -.-- --- -. . .----. ... .-. . ... .--. --- -. ... .. -... .. .-.. .. - -.--"

To find the answer, go to page 26.

Aberdeen Proving Ground Senior Commander and Commanding General of U.S. Army Communications-Electronics Command Maj. Gen. Bruce T. Crawford (right), led a five-person plenary panel during the Military Communications Conference (MILCOM) at the Baltimore Convention Center in Baltimore, Maryland, Oct. 8, 2014, with the topic of 'Fielding the Army Tactical Network.' Crawford was joined (from right) by Col. Mark Elliot, Director of the Army's LandWarNet Mission Command; Col. Paul Fredenburg, representing Army CIO/G6; Dr. Paul Zablocky (Senior Executive Service), Director of Space and Terrestrial for U.S Army Communications-Electronics Research, Development and Engineering Center; and Jennifer Zbozny, Director, Technical Management Division Program Executive Office for Command, Control and Communications-Tactical. (Photo by Kristopher Joseph, CECOM Public Affairs)

cover story continued

Command; Col. Paul Fredenburg, representing Army CIO/G6; Dr. Paul Zablocky (Senior Executive Service), Director of Space and Terrestrial for U.S. Army Communications-Electronics Research, Development and Engineering Center; and Jennifer Zbozny, Director, Technical Management Division Program Executive Office for Command, Control and Communications-Tactical.

One of the key points Crawford touched on was sustainment in terms of enabling the transition to an Expeditionary Army.

"In terms of sustainment, we have to reduce pre-deployment complexities that allow our formations to get out the door," he said. "Optimizing and continuing to leverage and transform our industrial base is critical to success."

Once those formations are out the door and in the fight, the Army is looking for state-of-the-art tactical network solutions to improve battle command within a common operating environment.

"We want to provide a capability that allows our joint force commander to unit task reorganize on the fly with the least amount of friction," said Elliot, who briefed on ways to deliver the network to the 'tactical edge.' "We need industry to help us with that."

Modernization, science and technology, software/hardware integration, and progress on the Joint Information Environment were other topics of discussion by the panelists.

At the end of the briefing, several audience members posed poignant questions to the panel members and Crawford summed up the importance of the discussion.

"In the end, we've got to continue to share what we're doing and why with our stakeholders. The capacity that industry brings is part of the Army's 'competitive advantage.' To get after all the Army sustainment and network modernization goals, it's these kinds of discussions; here at MILCOM and beyond, that we must continue to have with industry and academia."

In its 33rd year, MILCOM is a premier international conference for military communications. The three-day conference attracts decision-makers from government, military, academia and industry. In depth discussions are held and hundreds of technology and solutions are on display for all attendees.

Aberdeen Proving Ground Senior Commander and Commanding General of U.S. Army Communications-Electronics Command Maj. Gen. Bruce T. Crawford (left), watches a demonstration of the Unified Trouble Ticketing System by Ray Maxwell from Program Executive Office, Command, Control, Communications-Tactical Military Technical Solutions Office at the Army booth during the Military Communications Conference (MILCOM) at the Baltimore Convention Center in Baltimore, Maryland, Oct. 8, 2014. Crawford led a five-person plenary panel with the topic of 'Fielding the Army Tactical Network.' (Photo by Kristopher Joseph, CECOM Public Affairs)

Message from THE COMMANDER

"Our Shared Responsibility"
National Cyber Security Awareness Month

Maj. Gen. Bruce T. Crawford

October 2014 marks the 11th Annual National Cyber Security Awareness Month sponsored by the Department of Homeland Security.

As emerging technologies have improved our society and way of life, we must pause to recognize the inherent risks and learn how to act responsibly as we become more interconnected in cyberspace. Strengthening cyber security is also one of the Secretary of the Army's priorities, and everyone plays a vital role in "Our Shared Responsibility" to stay aware of the threats and take the appropriate actions in cyberspace.

When connecting online, remember to "stop, think and connect"

Stop: Before using the Internet or tactical communications systems, take time to understand the risks and learn to spot potential problems.

Think: Watch for warning signs and consider how your actions could affect the safety of yourself, your unit and your family.

Connect: Use the Internet and our mission command networks with greater confidence, knowing all steps were taken to safeguard the team and our efforts.

In the broad strategic environment, the cyber threat to our Army and our nation is becoming increasingly sophisticated.

Our adversaries are turning their sights onto our networks and infrastructures in order to steal personal and sensitive information and degrade our ability to defend the homeland.

This team effort will depend on a high level of accountability from senior leaders down to the individual user. There is simply too much at stake for us to become complacent as more and more of our daily lives are dependent on the technologies we have employed at every level of our society.

You are our first line of defense, and a commitment to cyber security is a commitment to the well being of your family, your Army and your nation.

Ever Vigilant, Army Strong!

Bruce T. Crawford
Major General, USA
Commanding

CECOM welcomes new senior enlisted leader

By Pamela Leigh, CECOM Public Affairs Office

The U.S. Army Communications-Electronics Command (CECOM) hosted a change of responsibility ceremony for its senior enlisted advisor at the C4ISR Center of Excellence Campus at Aberdeen Proving Ground, Maryland, Oct. 22, 2014.

CECOM Commanding General and APG Senior Commander Maj. Gen. Bruce T. Crawford presided over the ceremony that transferred responsibility from Command Sgt. Maj. Kennis J. Dent to Command Sgt. Maj. William G. Bruns.

Crawford praised both Dent and Bruns as "tremendous noncommissioned officers (NCOs)" crediting his own personal success on his enlisted counterparts. "I can honestly say that I would not be standing here today without the NCO Corps," he said. "The reason, year in and year out, that we are considered the most trusted profession, is because of the Soldiers in the NCO Corps."

Dent joined CECOM in November 2011 and served as the senior enlisted advisor for three commanding generals during his tenure with the command. During his speech he recognized the pride that both he and his wife, Gloria Dent, felt as part of the Aberdeen Proving Ground (APG) team.

"As I stand here today, I have much to be grateful for," said Dent. "CECOM has consistently monitored and sustained readiness. CECOM is a major player in support of our Army; what an awesome organization that I'm proud to have been a part of."

Dent said he is getting ready for life after the Army as he prepares for his upcoming retirement next summer after 32 years of service. He thanked CECOM employees, both military and civilian, by stating that their "loyalty, trust and dedication will never be forgotten."

Crawford welcomed the Bruns family to the APG team offering his support during their transition to the command.

Prior to his assignment at CECOM, Bruns served as the commandant for the Henry H. Lind NCO Academy, I Corps, at Joint Base Lewis McChord, Washington. During his remarks he stated that his family was excited to become part of the APG community, both on and off post.

"Teamwork is a key ingredient in making a great place even better," said Bruns. "I look forward to building the bonds that advance CECOM forward…I continue to look forward with positive ideas to advance the Army."

Command Sgt. Maj. William Bruns (right) accepts the colors of U.S. Army Communications-Electronics Command from CECOM Commanding General and Aberdeen Proving Ground Senior Commander Maj. Gen. Bruce T. Crawford (left) during a change of responsibility ceremony in the Myer Auditorium at Aberdeen Proving Ground, Maryland. Oct. 22, 2014. Bruns replaces outgoing CECOM and APG Senior Enlisted Advisor Command Sgt. Maj. Kennis Dent. (Photo by Kristopher Joseph, CECOM Public Affairs)

THE DECISIVE EDGE

Test tower helps operators see targets miles away

By Justin Eimers, CECOM Tobyhanna Army Depot

High above Tobyhanna Army Depot's Powder Smoke Ridge a 70-foot test tower makes it possible for operators to precisely survey targets at distances up to nearly a dozen miles away.

The Long-Range Advanced Scout Surveillance System (LRAS3) Test Tower platform is slated for completion early next month after a one-year, $1.25 million construction process. Corey Petruncio, electronics engineer in the Production Engineering's Counter Fire/Electro-Optics Systems Engineering Branch, said the tower provides testing capability to support a wide range of laser-based line-of-sight systems.

"The primary workload intended for the tower is the AN/TAS-8 LRAS3 overhaul program, a system that is expected to be fielded until at least 2025," he said. Tobyhanna will overhaul roughly 140 sight sensors per year, bringing them back to like-new condition.

The tower serves as the platform for line-of-sight testing of laser-based surveillance systems. At 70-feet tall, the tower allows the operator to see targets located at distances up to 11.5 miles.

The LRAS3 is an Army-only system managed by Product Management Ground Sensors. Although the LRAS3 is a standalone program, Tobyhanna

supports other systems in the ground sensors family including Driver's Vision Enhancer, Boomerang and the Vehicle Optics Sensor System.

The platform tower structure consists of a vertical reciprocating conveyor that safely and efficiently lifts assets from the ground level workroom to the platform level for testing, and a cold room at the ground level for thermal stabilization.

Engineers encountered several challenges during planning and construction of the tower, including issues with technical data, software and structural concerns. Overhaul of an LRAS3 had never been done, requiring the development of a 1,600-page Depot Maintenance Work Requirement to outline the entire process.

During this capability development, depot personnel worked with the Night-Vision Electronics Sensors Directorate at Fort Belvoir, Virginia, to design the test bench and develop custom software for sight sensor testing. This software is currently being expanded to support other systems including the Thermal Imaging System and Commander's Independent Thermal Viewer, and will likely become the depot standard for testing other similar systems.

Petruncio said the unique landscape of Tobyhanna presented an equally unique challenge in building the test tower.

"Because of the topology and geographic location of the depot, the test platform needed to be elevated well-above the depot's primary operating area," he said. "For this reason, the tower was constructed on Powder Smoke Ridge, with the test platform itself located atop the structure. Because of the target distances, the platform was designed to be extremely stable, even under high-wind conditions."

In addition to the 140 overhauls each year, Tobyhanna supports the LRAS3 program through an Automatic Reset Induction program, repair of theater-provided equipment and secondary repairables.

Testing from a 70-foot platform on Tobyhanna Army Depot's Powder Smoke Ridge allows operators to see targets up to 11.5 miles away when using laser-based surveillance systems. The Long-Range Advanced Scout Surveillance System (LRAS3) Test Tower platform is slated for completion early next month after a one-year, $1.25 million construction process. The tower provides testing capability to support a wide range of laser-based line-of-sight systems. The primary workload intended for the tower is the AN/TAS-8 LRAS3 overhaul program, a system that is expected to be fielded until at least 2025. Tobyhanna will overhaul roughly 140 sight sensors per year, bringing them back to like-new condition. The LRAS3 is an Army-only system managed by Product Management Ground Sensors. Although the LRAS3 is a standalone program, Tobyhanna supports other systems in the ground sensors family, including Driver's Vision Enhancer, Boomerang and the Vehicle Optics Sensor System. (U.S. Army photos)

Tobyhanna Office Express open for business at depot

By Betsy Kozak-Howard, U.S. Army Contracting Command

Col. Gerhard P.R. Schröter (center), commander of Tobyhanna Army Depot, Pennsylvania, chats with depot personnel as they and other personnel inspect items available in the just-opened office supply center. The center was made possible through a National Industries for the Blind contract. (U.S. Army photo by Steve Grzezdzinski, Tobyhanna Army Depot)

Tobyhanna Army Depot celebrated the grand opening of the Tobyhanna Office Express Store on Sept. 17 with a ribbon cutting ceremony.

The store provides supply items and was established by a National Industries for the Blind contract facilitated through the Army Contracting Command Aberdeen Proving Ground's (ACC-APG) Tobyhanna Division.

The contract was initiated by the Central Association for the Blind and Visually Impaired, a non-profit organization with a mission to assist people who are blind and visually impaired to achieve their highest level of independence. The association is headquartered in Utica, New York.

It is the fifth store to be opened by the organization. Many of the items available for sale at the supply center are made by people who are blind or disabled.

"The store will be a great asset to the depot community and will stock about 1,500 products including typical office supplies and other common use items," said Judy Haff, chief of ACC-APG's Tobyhanna Division.

Construction began in early 2014 to transform an existing building into a 5,000 square-foot store front and storage area.

According to Tobyhanna Army Depot Contract Specialist Mark Buonomo, the store is a win-win situation for the community and the AbilityOne Program.

"The new service is a convenient supply source for the depot's tenant agencies and will also support local National Guard and Reserve units," said Buonomo.

During the ribbon-cutting, Depot commander Col. Gerhard P.R. Schröter noted in his speech that Team Tobyhanna takes great pride in being responsible stewards of taxpayer resources and credited the efficiency and productivity of the dedicated workforce.

Emerging Leadership Cohort created to aid career development

By Sandy Curley, CECOM G1

(From left to right, standing) – Lauren Johnsky, Program Executive Office IEW&S, chair; Janet Penaherrera, CECOM G8, mentor coordinator; Rita Savage, CECOM Logistics and Readiness Center, secretary; Genevieve Brimat, Communications Security Logistics Activity, vice chair; Sandy Curley, CECOM G1, events coordinator; and Alex O'Ree, Communications-Electronics Research, Development and Engineering Center, information technology coordinator.

Seated: Gary P. Martin, SES, deputy to the commanding general. (Photo by Alissa Atanasio, CECOM)

The newly established Emerging Leadership Cohort (ELC) was formed to foster an environment of collaboration, knowledge and encouragement by providing members with resources to further career development. The ELC is a unique organization created for members by members, comprised of personnel that have completed the Aberdeen Proving Ground (APG) Emerging Leaders Program. The ELC intends to cultivate the skills learned in the program by providing its members with networking opportunities, training resources, and a mentorship program with senior leaders, including members of the Senior Management Association. In addition to these facets, members will support the APG Community by participating in events to include town halls, change of charter ceremonies and local volunteer efforts.

The first board was established by the following founding members: Lauren Johnsky, Program Executive Office Intelligence Electronic Warfare & Sensors, chair; Genevieve Brimat, Communications Security Logistics Activity, vice chair; Rita Savage, CECOM Logistics and Readiness Center (LRC), secretary; Jamie Plakosh, CECOM LRC, secretary; Janet Penaherrera, CECOM G8, mentor coordinator; Traci Flemons, Army Test and Evaluation Command, training coordinator; Sandy Curley, CECOM G1, events coordinator; and Alex O'Ree, Communications-Electronics Research, Development and Engineering Center, information technology coordinator.

With full support and encouragement, Gary P. Martin, deputy to the commanding general, endorsed the ELC by signing its charter and strategic plan on Sept. 8, 2014.

Depot equipment featured in blockbuster film

By Jacqueline Boucher, Tobyhanna Army Depot

(Photo by Sean Namlick, Tobyhanna Army Depot)

Actors portraying members of Navy SEAL Team 10 in last year's award-winning movie "Lone Survivor" autographed communications equipment on loan from Tobyhanna Army Depot, Pennsylvania. A prop liaison from a company called Independent Studio Services asked Communications Systems Directorate employees if the depot could provide several pieces of communications equipment for use in the movie. At the suggestion of a Navy SEAL tech advisor for the film, Tobyhanna sent an AN/PSC-5 Radio Set, two AN/CYZ-10 Data Transfer Devices, two AN/KYK-13 Electronic Transfer Devices and all associated hand microphones, cables, and antennas to New Mexico, where most of the film was shot, according to Sean Namlick, Logistics Management Branch chief. An actor portraying one of the team members killed during Operation Red Wings, in Afghanistan on June 28, 2005, would be filmed carrying the equipment. The movie is a heroic depiction of the Navy SEALs based on a book written by former Navy SEAL Marcus Luttrell about events that took place.

New Army training support packages for crypto-products

By Denise Y. McConnell, CECOM Communications Security Logistics Activity

The U.S. Army Cyber Center of Excellence (USA Cyber CoE) and Fort Gordon's, Directorate of Training (DOT), New Systems Integration Branch (NSIB), Project Director Network Enablers (PD NET E), and CECOM's Communications Security Logistics Activity (CSLA) have successfully completed training verification for two new cryptographic products, the ViaSat KG-250X Inline Network Encryptor (INE) and a secure telephone system.

The new system is a voice and data encryption telephone that supports both newer digital and legacy analog communications (Internet Protocol and public switched telephone networks, which is better known as plain old telephone service). The training for this specialized telephone system supports all the skills required by the system administrator to prepare the phone for operations, such as loading keys, network configurations and recovering from crashes in the field.

CSLA, PD NET E, and the U. S. Army Training and Doctrine Command (TRADOC) USA Cyber CoE Directorate of Training brought together personnel to set up an encrypted network, similar to what is found in an operational environment, to verify the KG-250X INE and the secure, commercial telephone system New Equipment Training (NET) Support Packages. The NET verification ensures training packages and equipment are ready for Soldiers. Training material verification was held in conjunction with technical manual verification over an intense, two-week period at Fort Huachuca, Arizona. Soldiers holding 25 series military occupational specialties from the Network Enterprise Technology Command Headquarters Company and 40th Expeditionary Signal Battalion participated in both events.

"My role in training verification is to ensure all procedures can be performed by the operator and that they don't infringe on any safety regulations and the procedures are doctrinally sound," says Gerald Evans, chief of Strategic and Tactical Section, USA Army Cyber CoE, DOT. For technical manuals (TMs), "verification ensures that the device/system functions or performs in accordance with the written procedures of the TM and also ensures that the procedures are written at the appropriate level for the target audience. The COMSEC [communications security] training packages are important because the transfer of knowledge is lost when training is not executed effectively."

Evans further stated, "It is important to remember that training accomplishes several things. One, it develops technical and tactical individual and collective skills through instruction and repetitive practice. Two, it uses a progressive approach that systematically builds on the successful performance of each task. Three, training prepares individuals and organizations by developing the skills and teamwork necessary to accomplish a task or mission successfully. Four, training is associated with 'what to do.' Well trained organizations and individuals tend to react instinctively even in unknown and complex situations."

Simon Baik, PD NET E Secure Voice Products lead, who heads the effort for specialized telephone system supportability commented, "PD NET E is responsible for fielding to the requirements that have been identified. Just having the devices available doesn't necessarily mean that the knowledge to use the devices has been imparted as well. When our end Crytographic Units are delivered to the end user, we must ensure that the full COMSEC capability is delivered, not just the hardware; and training ensures that the users have the knowledge and skills to operate the devices successfully."

PD NET E oversees the effort for crypto-modernization and part of their responsibility is to ensure a training support package (TSP) is in place and verified in conjunction with equipment fielding. The equipment fielding plan includes a training package that resources all leader training, as well as logistical and technical resources for each item fielded. The CSLA NET trains the unit on the operation, employment of the device/system, and provides the complete TSP with all the necessary training materials that are left with the unit for use as a basis for sustainment training.

SEC provides systems training to Soldiers

By Sok Kim, CECOM Software Engineering Center

Software Engineering Center (SEC) Far East Region personnel provided maintenance training to Military Intelligence (MI) Soldiers in September on Camp Casey, South Korea.

Eight Soldiers from the 2nd Infantry Division, U.S. Army Eighth Army, and the 501st Military Intelligence Brigade, Korea, received instruction on the latest version of the Distributed Common Ground System – Army (DCGS-A) Mobile Intelligence Fusion Servers (IFS) and Portable Multi-Function Workstations.

The Soldiers hold the military occupational specialty 35T (Military Intelligence Systems Maintainer/Integrator) and are responsible for the maintenance of Army Electronic Warfare Command, Control, Communications, Computers, and Intelligence, Surveillance, and Reconnaissance (C4ISR) systems. The 35T Soldiers attend a rigorous 42-week advanced individual training program covering the maintenance and troubleshooting of a variety of Army systems; however, none of them had been trained on the new DCGS-A equipment.

During their time with the SEC, local intelligence system maintainers learned how to use the system to answer their commander's Priority Intelligence Requirements. SEC personnel made sure that the units would be able to keep these systems running to support exercises and real world missions.

In light of the unforeseen training deficit, the SEC and Program Manager DCGS-A are working with the Army Training and Doctrine Command to leverage new ideas that increase the Army's ability to be a more self-sustaining force. Training 35T Soldiers to maintain the DCGS-A system helps the Army reduce system sustainment costs while still providing responsive, agile support. It also builds confidence in both the units and Soldiers who depend on them for critical intelligence. The maintainer training has already proven itself successful during key, high visibility training exercises, providing these Soldiers the skills they require to repair and maintain their respective systems.

This was the second iteration of this training for SEC Far East Region personnel. The first training was conducted in February 2014.

Soldiers holding the Military Intelligence Systems Maintainer/Integrator military occupational specialty traveled to Camp Casey, South Korea, for training in September. Reporting from the 2nd Infantry Division, U.S. Army Eighth Army, and the 501st Military Intelligence Brigade, Korea, the Soldiers received instruction on the latest version of the Distributed Common Ground System – Army (DCGS-A) Mobile Intelligence Fusion Servers (IFS) and Portable Multi-Function Workstations from the Software Engineering Center's Far East Region personnel. (Official U.S. Army photo)

PROVIDING THE CRITICAL LINK

SEC is working with U.S. Army Training and Doctrine Command and the Army's Intelligence Center of Excellence to ensure Soldiers are trained and confident in their systems. Here, SEC's Field Software Engineers are providing Military Occupation Specialties 35T Soldiers in Korea Distributed Common Ground System-Army maintenance training, ensuring they can provide their units responsive intelligence system support. (U.S. Army photo by Software Engineering Center staff)

Information Systems Engineering Command (ISEC)

Support to the U.S. Army Intelligence and Security Command

ISEC continues to provide IT engineering in support of the Army Intelligence and Security Command for improved intelligence dissemination capabilities at the Fort Belvoir Trojan Network Control Center. The communications upgrades ISEC recently completed at the control center will provide larger and quicker data transfers, improve network management, and enhance security of worldwide intelligence dissemination.

Communications upgrade

ISEC is supporting Program Executive Office Enterprise Information Systems (PEO EIS) with Defense Information Systems Agency (DISA) Unified Network Capabilities Testing for Department of Defense (DoD) communications. DISA is currently pursuing a Unified Capabilities (UC) communications upgrade for enhancing voice, video and collaboration services over the network. PEO EIS is the Army's lead agent for the Army's integrated portion of the DoD UC solution. Leaders from the respective service components recently met to discuss an implementation plan and formulate a way-ahead strategy.

Support to the Air Force

ISEC is supporting the United States Air Force's Distributed Mission Operations Center in testing a multi-level cross domain solution. This is significant because it will provide capability to connect a single desktop device to multiple networks. Upon completion of testing, ISEC will present their results and findings to the advisory board of the United Cross Domain Security Management Office for potential implementation. If successful, this solution could be implemented on Army networks.

Logistics and Readiness Center (LRC)

Communications Security training events

The LRC Communications Logistics Security Activity (CSLA) together with Project Director Network Enablers of the U. S. Army Training and Doctrine Command (TRADOC) Directorate of Training recently brought together personnel to set up an encrypted secure phone, similar to what is found in an operational environment, to verify the secure telephone New Equipment Training (NET) Support Packages. This training verification was held in conjunction with technical manual

story continued on next page

verification over an intense two-week period at Fort Huachuca, Arizona. Soldiers, who hold the 25 series military occupational specialty, from the Network Enterprise Command Headquarters Company and 40th Expeditionary Signal Battalion, participated in both events. The TRADOC NET verification ensures the training packages are ready for Soldiers.

Soldiers perform exercises during the secure telephone system training verification at Fort Huachuca, Arizona, on Aug. 21, 2014. Pictured from left to right back row are: Spc. Derric L. Smith, Multi-channel Transmission Systems Operator-Maintainer, Vince Naputi, INE instructor, CECOM CSLA, Spc. Alex Lopezromaniz, Multi-channel Transmission Systems Operator-Maintainer. (Photo by Doug Smith, Communications Logistics Security Activity)

The CSLA Communications Security (COMSEC) Training Team recently provided training on the AN/PYQ-10 Simple Key Loader (SKL) and universal secure phone system to six Border Patrol agents. The training assisted in their preparation, with the necessary knowledge and skill, to successfully operate leading edge key loading and secure voice communications equipment, thereby contributing to national security and our nation's critical infrastructure.

A Command COMSEC Inspectors Certification course (CCICC) was conducted by CLSA at the Professional Education Center in North Little Rock, Arkansas. The two week long course prepares students to successfully conduct Command COMSEC inspections on unit COMSEC accounts. Students from the National Guard Bureau, U.S. Army Forces Command, U. S. Army Intelligence and Security Command, and the Army Corps of Engineers attended the course. CSLA conducts, on average, five CCICC courses per fiscal year taught by CLSA's most senior auditors. This course helps prepare students to conduct mandatory Command COMSEC Inspections on their Command's COMSEC Accounts. Each year CSLA hosts two training events at Fort Huachuca and the remaining three training events are sponsored by other Army Commands such as the National Guard or United States Forces Korea. In accordance with Army Regulation 380-40, Command COMSEC Inspections are required to be conducted by command inspectors. The inspection provides commands with an opportunity to assess the readiness, security posture, and accounting practices of their COMSEC accounts.

Software Engineering Center (SEC)

Pilot program for Distributed Common Ground System-Army (DCGS-A) Information Assurance Vulnerability Alert (IAVA) releases

SEC developed and released the pilot program for monthly intelligence system Information Assurance Vulnerability Alert (IAVA) releases, increasing system security by over 50 percent while reducing the time and effort required for installing system IAVA patches. IAVA releases are critical to ensure the continued security of fielded systems. Due to the level of effort and resources required, SEC normally develops and releases IAVA patches on a quarterly schedule. However, SEC's Intelligence Fusion Support Division has been investigating the feasibility of providing IAVA patches on a monthly basis to improve the timeliness of these patches. The Distributed Common Ground System-Army (DCGS-A)v3.1.7.3 monthly IAVA release is the first monthly IAVA patch release, made possible in part owing to its new IAVA Installer tool, which simplifies installation to such an extent that units can quickly and easily install IAVA patches (reducing installation and verification time by more than seven hours per baseline), making it possible to install patches more frequently with minimal system downtime. The pilot, which was tested by units in Operation Enduring Freedom, was lauded for its ability to remove vulnerabilities and strengthen system security posture.

SEC's Bobbie Hilton and Mike Malave present the new Information Assurance Vulnerability Alert (IAVA) installer tool to Larry Muzzelo (not pictured), director, CECOM Software Engineering Center. (Photo by Software Engineering Center staff)

Support to the Unmanned Aircraft System (UAS) Software Depot Maintenance Integrated Process Team (IPT)

The UAS Software Depot Maintenance IPT visited SEC on Sept. 17, 2014 to observe processes and obtain information about SEC's core capabilities and best practices supporting UAS domains. Their objective was to view/review SEC software depot facilities and obtain a better understanding of SEC capabilities. SEC provided information to the IPT on various systems/functional capabilities where depot maintenance is currently performed, including representatives from Program Executive Office Aviation, CECOM, Army Aviation and Missile Life Cycle Management Command, Headquarters Army Materiel Command, Department of the Army G4, Navy, Air Force and Office of the Secretary of Defense. The IPT discussed at length the appropriate correct software core capability based on the requirements of public law. The interest centered around prioritization, configuration control and code adjustment/analysis. Software versioning and relationships with the program managers, along with what point SEC gets involved in the process were also areas of interest for the IPT members.

Providing Global Rapid Response Information Package deployment support for Operation United Assistance

SEC is supporting Program Executive Office Command Control Communications-Tactical (PEO C3T) Global Rapid Response Information Package (GRRIP) deployment, providing secure communication capabilities to Soldiers in support of Operation United Assistance. PEO C3T requested SEC's support to field the GRRIP to deploying units to give them secure data, voice, chat and video communications capabilities in the AFRICOM region. The GRRIP is a small rapid response secure and encrypted communications package (laptop, router, firewall, INE device) that uses an L band commercial satellite connection for forces operating in austere and demanding environments. It deploys in a single transit case that can fit in the overhead bin of an airplane and can be set up in minutes. SEC manages the GRRIP project for Product Manager Satellite Communications. This is the first GRRIP to deploy for the Ebola mission in AFRICOM - there are other GRRIPS deployed in the Horn of Africa (separate mission set). Eventually, there are ten GRRIPs projected for deployment to Operation United

Joe Pham, Software Engineering Center, explains the MUXTOOLKIT software sustainment process to members of the Unmanned Aircraft System Software Depot Maintenance Integrated Process Team during a recent visit to determine Depot Maintenance efficiencies and best practices. The team was impressed with SEC processes and procedures. (Photo by Jim Hayes, SEC)

story continued on next page

4th Infantry Division leaders explain the use of the Mission Support Command (MSC) to the Colorado Springs Regional Business Alliance Military Affairs Council during a visit to Piñon Canyon Maneuver Site, Sept. 21, 2014. The MSC is used as the division's first expeditionary element to deploy to any operation when called upon by national leaders. (Photo by Sgt. Eric Glassey)

Assistance. The Global Rapid Response Information Package (GRRIP) is designed for small teams entering locations where the infrastructure has either been dismantled, destroyed or hasn't been built up yet, and it is perfect for first responder communications.

Coordination of field support efforts for the 4th Infantry Division

SEC coordinated the field support efforts for the 4th Infantry Division's Field Training Exercise (FTX) Iron Horse and Simulation Exercise (SIMEX) Iron Focus as they prepared for their upcoming National Training Center (NTC) rotation. During the exercises the 4th Infantry Division staff deployed to Piñon Canyon Maneuver Site and exercised mission command of the 3rd Armored Brigade Combat Team's simulation training. SEC coordinated between the 4 ID Mission Command Element and 3/4 ID Brigade Combat Team, the supporting Army Field Support Battalion - Carson, and the Division and Brigade Digital Systems Engineers along with the CECOM field support providers to conduct mission analysis of requirements and to war-game the support request and concept. Field support, which included SEC software support along with system support from Program Executive Office Command Control Communications-Tactical, Aviation and Missile Command, and the CECOM Logistics and Readiness Center, covered 18 separate Command Control Communications Computers Intelligence Surveillance and Reconnaissance systems as the unit prepared for a November NTC rotation and possible future deployment.

Collaboration with the U.S. Army Intelligence Center of Excellence (USAICoE) to provide Soldiers better military Intelligence software support.

SEC kicked off a collaborative effort with the USAICoE's New Systems Training and Integration Division (NSTID) to incorporate military intelligence Soldiers assigned at Fort Huachuca into the software testing process, providing invaluable insight as to how Soldiers navigate the systems when executing their missions, and ensuring software changes and upgrades meet Soldier requirements. SEC's Intelligence Fusion Support Division (IFSD) location on Fort Huachuca allows it to collaborate with the many Army and Joint intelligence organizations located there. The teaming effort with NSTID will provide a user perspective during verification and validation testing, helping to ensure SEC develops and delivers products that meet Soldiers' real-world operational needs. In addition, by participating in tests and gaining access to IFSD's sustainment lab, USAICoE Soldiers will gain an understanding of IFSD's processes and the mission-critical intelligence systems it sustains, facilitating future cooperation and helping

to ensure key personnel have the information they need to keep Soldiers' systems operational. The teaming effort with USAICoE's 35T course gives Soldiers increased situational awareness by having them directly involved in the operational sustainment of intelligence systems, providing the Army improved operational capabilities while enhancing SEC's life cycle system support efficiency.

Tobyhanna Army Depot (TYAD)

Support to the U. S. Navy

TYAD is working with the Rolling Airframe Missile (RAM) In Service Engineering Activity (ISEA), Naval Surface Warfare Center, Port Hueneme California to complete the first RAM Launcher Material Enhancement Program and Refurbishment Turn-Around Program (RTAP). The ISEA is currently providing oversight while TYAD reinstalls a Launcher Switching Multiplexor Unit on an RTAP RAM Guided Missile Launching System asset. The RIM-116 Rolling Airframe Missile is a lightweight, quick-reaction, fire-and-forget missile designed to destroy anti-ship cruise missiles and asymmetric air and surface threats.

Designation as a Depot Source of repair

The Army Maintenance Interservice Support Management Office, Headquarters Army Materiel Command, has designated TYAD as the Depot Source of Repair for the AN/TPQ-50 Light Weight Counter Mortar. This is a lightweight, man-portable weapons location sensor that provides continuous 360-degree surveillance to detect, locate and report enemy mortar, artillery and rocket positions, thereby enabling warfighters to take timely action to neutralize identified threats.

Operation Atlantic Resolve

TYAD is providing one Field Service Representative (FSR) to support Command Post Systems and Integration during Operation Atlantic Resolve, Persistent Presence Land Forces Assurance exercises in Lithuania, Poland, Latvia and Estonia from Oct. 1 through Dec. 31, 2014. The FSR will provide operational support and over-the-shoulder training. Persistent Presence Land Forces Assurance exercises are the first in a series of expanded U.S. land force training activities in the Baltic region taking place during the next few months. The exercises, conducted by U.S. Army Europe Soldiers and host nation forces, are a demonstration of U.S. commitment to the North Atlantic Treaty Organization and to our collective defense responsibilities through increased ground, air, and naval force presence.

(Official U.S. Army photos)

CECOM announces 2014 Safety Award recipients

The Communications-Electronics Command's (CECOM) Safety Award Program provides a mechanism for the Command Group, activity directors and supervisors to recognize actions and accomplishments of CECOM personnel that contribute to the increased safety of CECOM personnel and/or increased effectiveness or efficiency of the CECOM Safety Program. They may be presented to CECOM military and civilian personnel in recognition of suggestions, acts, or other personal efforts that contribute to accident prevention, the improvement of the CECOM Safety Program, or result in the increased safety of CECOM personnel.

The 2014 Safety Award recipients are:

Outstanding Safety Program 2014

- **Julia A. Leister,** Information Systems Engineering Command (ISEC), Fort Detrick, Maryland

- **Todd M. Rust,** ISEC, Fort Detrick

Star Notes recognize individuals for their contributions to the CECOM Safety and Occupational Health Program. Each year, the CECOM Directorate for Safety recognizes individuals for outstanding safety program initiatives.

Because of the exemplary safety programs and outstanding safety initiatives by the CECOM workforce, a Star Note from the CECOM Commanding General is well deserved.

Star Note

- **Ms. Margaret L. Brown,** Software Engineering Center, Aberdeen Proving Ground, Maryland

- **Mr. Forrest Garrett,** SEC, APG

- **Mr. Oscar Martinez,** SEC, Fort Lee, Virginia

- **Mr. Fred Orr,** G4, APG

HAIL & farewell

The Communications-Electronics Command (CECOM) welcomes its new military service members:

Capt. Jeremy L. Hutchinson
Information Systems
Engineering Command (ISEC)

CECOM congratulates the following employees on their departure:

Command Sgt. Maj. Kennis J. Dent
Headquarters CECOM, APG

Robert DiMichele,
Public Affairs & Communications
Media, APG

Awards ★★★

CECOM congratulates the following employees on their achievement:

Superior Civilian Service Awards:

Robert DiMichele,
Public Affairs & Communications Media, APG

Commander's Award for Civilian Service:

Bronwyn P. Areta, ISEC
Alan Cannon, G4
Carl Y. Edwards, G4
Levi B. May, G4
Ariel Nieves (retired), Software Engineering Center
Corrine M. Rao, G4

Are you a pioneer?

Lt. Col. Young D. Kim,
CECOM Command Chaplain

One of my favorite books is *The Nuremberg Chronicle*. It was written in Latin by Hartmann Schedel, with a version in German and translated by Georg Alt. It was published in the early 1490's. *The Nuremberg Chronicle* is an illustrated biblical paraphrase and world history that follows the story of human history related in the Bible. It includes the histories of a number of important Western cities. and predicts the end of the Earth coming within the year of its publication by quoting Bible verses and providing historical evidences. It shocked and dismayed people in Germany and all of Europe.

About four months after the book came out, a small sailing ship left the port of Palos in Spain. The ship journeyed westward toward the unknown world, fighting the wind and waves of the Atlantic Ocean.

On the bow of the ship, a man stood staring into the horizon. While everyone else was fearing the end of the world, this man believed there must be a new, better world at the end of the sea.

One month after the departure, he discovered a new land on Oct. 12, 1492. This man's name was Christopher Columbus. The new land he saw was part of the Bahama Islands and he named the island "San Salvador," which means "the savior." He believed he could reach there because the Lord gave him hope, vision, and courage. Greek philosopher Anon said, "Hope sees the invisible, feels the intangible, and achieves the impossible."

Are you a pioneer, who attempts to discover new things, or a follower who only travels in the footsteps of others? Listen to the Creator who says, "Be strong and very courageous. Do not be terrified; do not be discouraged, for the Lord, your God, will be with you wherever you go" (Joshua 1:9).

Blessings!

Breast Cancer Awareness

Republished from the Army Materiel Command's Wellness Newsletter

Most breast cancers are found in women who are 50 years of age or older, but about 9,000 women who are younger than 40 are diagnosed with breast cancer each year in the United States. In this younger group, breast cancer is generally more aggressive, found at a later stage, and has lower survival rates.

Two genes influence risk for breast cancer: BRCA1 and BRCA2. All men and women have these genes. Normally, they help protect you from getting cancer. But when one or both of them have a mutation (change), they increase your breast and ovarian cancer risk. Without treatment, women with a BRCA gene mutation are seven times more likely to get breast cancer and 30 times more likely to get ovarian cancer before age 70 than other women.

How do I know if I have a higher risk for a BRCA gene mutation?

Learn your family history of cancer.
Talk to your doctor if you have:

- Multiple relatives with breast cancer.
- Any relatives with ovarian cancer.
- Relatives who were diagnosed with breast or ovarian cancer before age 50.

What should I do if I am at increased risk?

The only way to know for sure if you have a BRCA1 or BRCA2 gene mutation is to get a genetic test. You should meet with a genetic counselor before getting a genetic test. Your doctor can refer you to one. Most people do not need genetic counseling and testing. A genetic test helps only the small number of people with a higher risk for having a mutation.

If you learn that you have a BRCA gene mutation, you can take important steps to reduce your cancer risk.

AROUND *the* COMMAND

Tobyhanna Army Depot, Pennsylvania – Production Management's Anthony Ceccacci and Chris Hunsinger prepare to serve their Smooooth Heat chili during the Combined Federal Campaign (CFC) Chili Cook-Off on Oct. 6. Smooooth Heat was voted Best Chili while Emerald City chili won Best Booth and Death Sentence chili was named the Firefighter's Choice. (Photo by Steve Grzezdzski, Tobyhanna Army Depot)

Aberdeen Proving Ground, Maryland – Installation Commander Col. Gregory McClinton (left) and Communications-Electronics Command Commanding General and Aberdeen Proving Ground (APG) Senior Mission Commander Maj. Gen. Bruce Crawford (center), answer APG- related questions from Harford Cable Network host Ed Hopkins during a live taping for "Inside Harford County" on Oct. 9, 2014. (Photo by Greg Mahall, CECOM Public Affairs)

Fort Huachuaca, Arizona – (Third from front) Col. Patrick L. Kerr, commander of CECOM's Information Systems Engineering Command (ISEC), with his team of directors and advisors participate in a team building hike on Bear Canyon Trail in Tucson, Arizona. The hike was part of a week long leadership development and organizational planning event held at ISEC. (Photo by Robert Lorentsen, Information Systems Engineering Command)

Enterovirus confirmed in Maryland

From the Maryland Department of Health and Mental Hygiene

On Sept. 24, 2014, the Maryland Department of Health and Mental Hygiene (DHMH) confirmed the presence of enterovirus D68(EV-D68) in Maryland. The virus, which has been associated with respiratory infections in children across the country, was identified in a specimen collected from a hospitalized child in suburban Maryland and was sent to the Centers for Disease Control and Prevention (CDC) for confirmation.*

"Now that this virus is known to be in Maryland, it is important that we all take reasonable steps to limit its spread and control its impact," said DHMH Secretary Dr. Joshua M. Sharfstein.

DHMH is recommending that families adhere to the following measures:

- Practice preventive steps, as with other ailments, by regularly washing hands with soap and water.
- Provide special attention to children with asthma.
- Be alert to wheezing and other respiratory ailments in children.
- Keep sick children at home.
- Avoid touching eyes, nose and mouth.
- Cough and sneeze into sleeve or a tissue.
- Avoid kissing, hugging and sharing cups, eating utensils, etc. with people who are sick.
- Disinfect frequently touched surfaces, such as toys and doorknobs, especially if someone is sick.
- Stay up-to-date on vaccinations, especially influenza vaccine, to reduce respiratory illness.

DHMH has been working with healthcare facilities to prepare for the expected arrival of enterovirus D68. Since there is no EV-D68-specific treatment, identifying EV-D68 doesn't change the treatment of the patient: If a patient is wheezing, the wheezing symptoms can be treated; if a patient is having difficulty breathing, respiratory support and oxygen can be given.

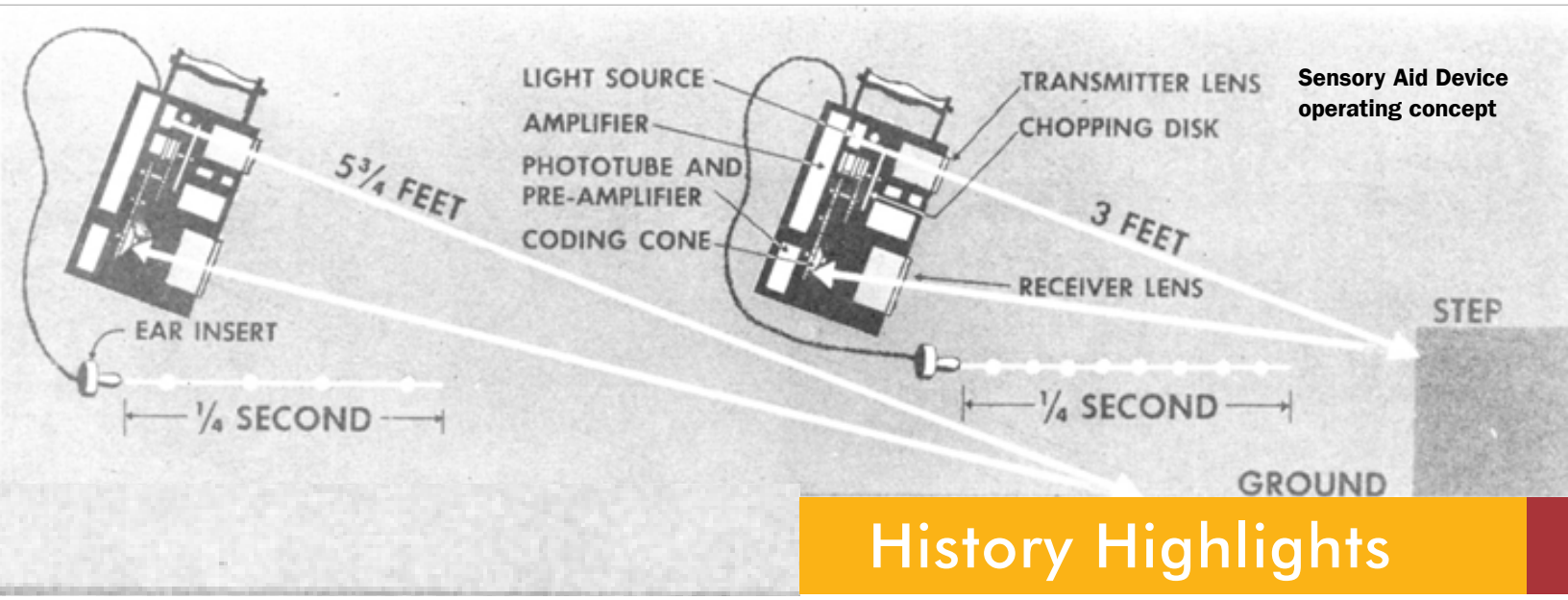
Healthcare providers, as recommended by the CDC should:

- Consider EV-D68 as a possible cause of acute, unexplained severe respiratory illness, even if the patient does not have fever.
- Consider laboratory testing of respiratory specimens for enteroviruses when the cause of respiratory illness in severely ill patients is unclear.
- DHMH also will continue to work with school officials and other institutions that monitor student health and activity, for updates on absenteeism and other indicators of respiratory illness activity. The department will continue to conduct surveillance on the spread and impact of this virus.

Enterovirus is one of many viruses that can cause respiratory illness, and there are more than 100 types of enteroviruses that affect humans, causing between 10 million and 15 million illnesses per year. Most people with enteroviruses have no symptoms or only mild symptoms, but some infections can be serious. EV-D68 infections are believed to occur less often than other enterovirus infections.

The CDC is providing updates on nationwide D68 infections at

http://www.cdc.gov/non-polio-enterovirus/about/EV-D68.html



Sensory Aid Device operating concept

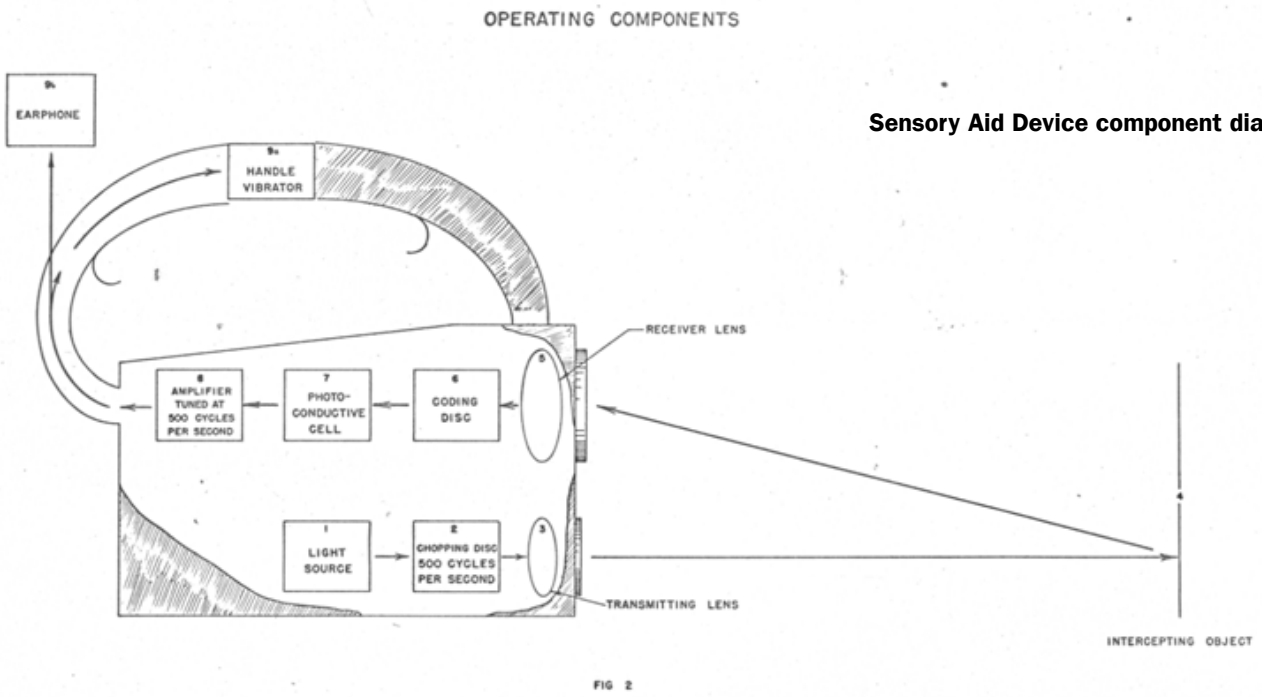
Signal Corps technology assisted visually impaired

By Susan Thompson, CECOM Command Historian

October is National Disability Employment Awareness Month, and the month is focused the contributions Americans with disabilities makes to our Army. But did you know that CECOM's mission and the Signal Corps can be traced back to one man's attempt to improve life for the deaf population?

Albert J. Myer received a medical degree from the University of Buffalo in 1851, with his medical dissertation, " A New Sign Language for Deaf Mutes." Myer had worked in a telegraph office while studying for his degree, and transformed the Bain telegraph code into a means of personal communication by spelling out words with taps on a person's hand or nearby object. After joining the Army in 1854 as an assistant surgeon, Myer converted his sign language system into the flag and torch system which became known as "wigwag." This system, unlike semaphore signaling, relied on a single flag, which was easily transportable and used a limited number of personnel. In 1860, the bill authorizing the creation of the Signal Corps was signed, and Myer, promoted to Major, was placed in charge. From communicating with the deaf to communicating across distances, Myer's work significantly contributed to the development of Army communications.

Moving forward almost one hundred years, the well-established Signal Corps was on the cutting-edge of communications equipment research and development, with most of this research taking place at the Signal Corps Engineering Laboratories at Fort Monmouth,



Sensory Aid Device component diagram

New Jersey. In 1945, Signal Corps Electronics Laboratory Physicist Lawrence Cranberg developed what was called the Sensory Aid Device, AN/PVQ-2. An outgrowth of personal radar sensory aid AN/PPQ-1 (Operational radar, personnel detection), meant for nighttime use for Soldiers on patrol, the sensory aid device was considered to have potential for civilian use. About 25 of the devices were built for the Veterans Administration, which submitted them for further testing.

The AN/PVQ-2 used a pulsed beam of light which, when reflected from an object, impinged upon a photoelectric cell. This cell in turn would set off either an audio signal or a vibration, which the user detected in an earphone or through the handle of the device. The aid was unaffected by non-pulsed light, such as sunlight and ordinary electric light. The intent was to allow the user to "sense" the physical environment, including straight lines (curbs, buildings), steps, and doorways, to assist the user in navigating common obstacles. The hand-held device weighed about 9 pounds and was equipped with an ear piece. Though it was never developed commercially, the device lead to further experimentation on devices to assist with non-visual navigation.

These examples help illustrate the basic idea of National Disability Employment Awareness month – that good ideas and contributions can come from anywhere and anyone. In the quest to improve communications technologies, the Signal Corps has benefitted from the contributions of wide range of individuals – Army doctors, scientists, engineers, Soldiers and civilians. The Army draws from the technologies being developed by industry, and in turn, produces unique military equipment that ends up being broadly adopted by society at large.

CECOM DOTS and DASHES

“-.-. -.-- -... . .-. ... . -.-. ..- .-. .. - -.-- .. ..- . .-. -.-- --- -. . .----. ... .-. . ... .--. --- -. ... .. -... .. .-.. .. - -.--”

The answer to “What’s in the box?” is:

Morse code for - “Cybersecurity is everyone's responsibility!”

DISCLAIMER: Dots and Dashes is an authorized CECOM publication for the CECOM workforce. This publication focuses on awards, achievements, people and events internal to CECOM as well as topical and policy updates from staff. Contents of Dots and Dashes are not necessarily the official views of, or endorsed by, the U.S. Government, the Department of the Army, or CECOM. The content of the publication is the responsibility of the U.S. Army CECOM Chief of Public Affairs, Robert DiMichele. The newsletter is published monthly and distributed electronically via email. It is posted to the CECOM SharePoint site at: **https://sp4.kc.army.mil/cecom/home**

Send questions, comments to:
marissa.l.anderson.civ@mail.mil, 443-861-6714 (DSN 848-6714) or
pamela.a.leigh.civ@mail.mil, 443-861-6626 (DSN 848-6626)