



US Army Corps of Engineers ®

# Electronic Technology Systems Center



## On page ...

- 2** Understanding DoD Information Assurance Certification and Accreditation Process
- 3** Energy savings, improving 'noise' immunity by specifying, using switching power supplies
- 4** 2008 Training Courses
- 5** HSPD-12 Implementation Programs and Guidance
- 8** Ask MCX
- 8** Who we are



Visit the U.S. Army Engineering and Support Center, Huntsville at [www.hnd.usace.army.mil](http://www.hnd.usace.army.mil)

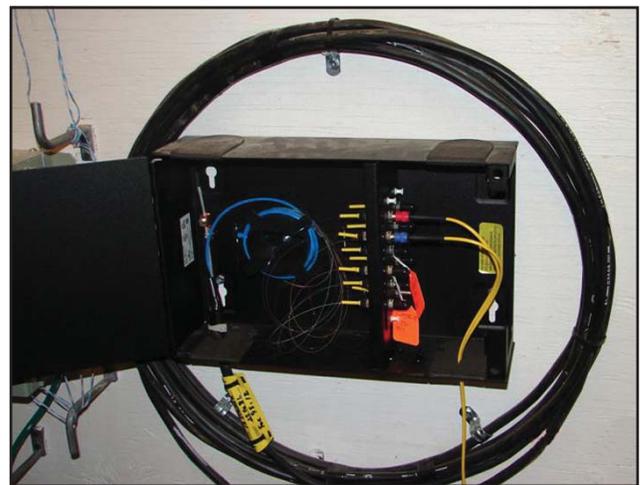
Technical Bulletin

March 2008

# Data connectivity for access control points

By Charles R. Malone

As the Army and the other services continue to enhance security at access control points (ACPs), the need for reliable, high-speed data connectivity at installation perimeters becomes increasingly important. While many installations have been proactive in extending their fiber optic backbone to the perimeter, many ACP security upgrade projects continue to be hampered by the inability to transmit data from ACPs back to security monitoring and administration facilities. Although a dedicated copper phone circuit is generally sufficient for transmitting basic ACP alarm messages (guard duress, door forced, enclosure tamper, etc.), ACP video and access control data demand a much faster connection



Courtesy photo

## Fiber optic patch panel in a gatehouse electrical room

that is best provided by fiber optic cable. To ensure adequate connectivity for an ACP security upgrade, the project team must first confirm the availability of fiber at each ACP and then design and build a network capable of transmitting all required data.

**Issue 1: Fiber optic cable availability.** A detailed site survey should be conducted during the early stages of an ACP

security upgrade project. It is during this survey that each ACP should be visited to document existing conditions, including the availability of fiber optic cable. A representative from the local Directorate of Information Management (DOIM) should accompany the survey team to identify the primary distribution point for the installation-wide fiber optic backbone and

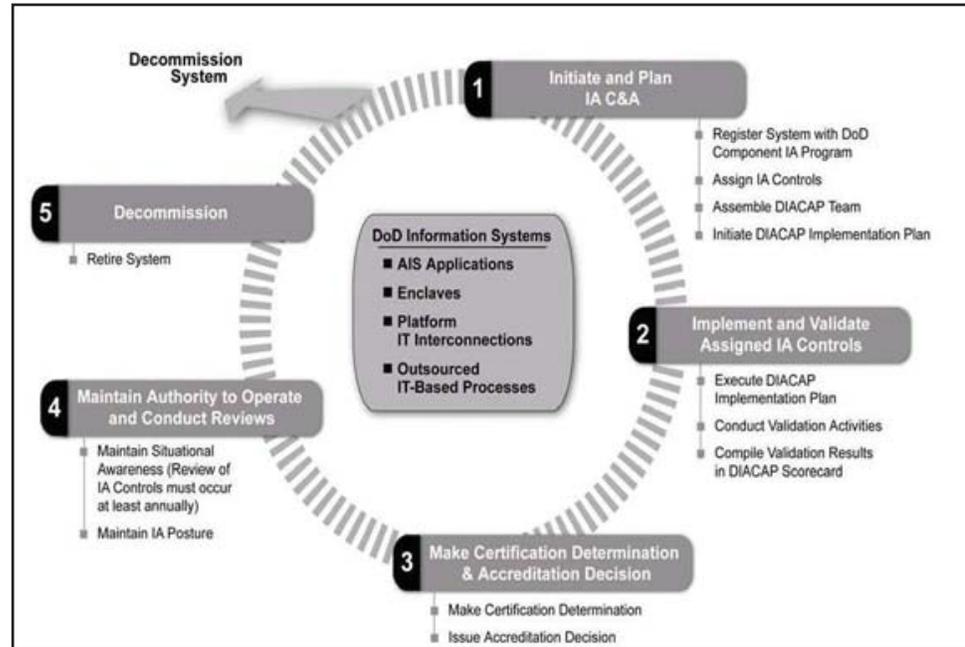
See ACP on page 4

# Understanding Department of Defense, Information Assurance Certification and Accreditation Process

By Buland Mahmood

Using Department of Defense (DoD) networks and systems for Electronic Security Systems (ESS), Utility Monitoring and Control systems (UMCS), Supervisory Control and Data Acquisition (SCADA) Systems, and similar automation systems can be a cost effective solution. However, there are some regulatory and policy requirements which must be met to connect to or interface with such networks.

The data communication technology and the Internet has made available various tools, hardware and software applications which can be used to penetrate networks and steal valuable or classified information. In certain cases adversaries or criminals can destroy, modify or misuse the information stolen from compromised networks. National security interests dictate that information on government networks be accurate, reliable, uncompromised and useful for the purpose it



**The Department of Defense Information Assurance Certification and Accreditation Process (DIACAP)**

is transmitted.

In order to protect the networks and associated information systems DoD had established guidelines and policy, e.g. DoD Instruction (DoDI) 5200.40, Defense Information Technology Systems Certification and Accreditation Process (DITSCAP), which was issued on Dec. 30, 1997. This document was supplemented with manuals and specifics on the process which users needed to follow to implement secure systems and not compromise security features of the

existing DoD systems. The DITSCAP documents provided a structured methodology for DoD network and system users and contractors to obtain the required Certification and Accreditation (C&A).

On Nov. 28, 2007, DoD issued a replacement instruction, DoDI 8510.01, Defense Information Assurance, Certification and Accreditation Process (DIACAP). This new DoDI incorporates requirements to counter threats to DoD networks and systems from

adversaries and criminals resulting from technologies and other factors. The DIACAP process also includes the requirements resulting from the Federal Information Security Management Act (FISMA), which was passed by Congress and signed into law by the president as a part of the E-Government Act of 2002 (Pub. L. No. 107-347).

DIACAP outlines a series of processes and steps users and

See *DIACAP* on page 6

# Energy savings, improving 'noise' immunity by specifying, using switching power supplies

By Buland Mahmood

Power supplies are one of the crucial building blocks of a modern society, converting high-voltage alternating current (AC) into low-voltage direct current (DC) for use by the electronic circuits in office equipment, telecommunications and consumer electronics. Over 2.5 billion AC/DC power supplies are currently in use in the U.S. alone. About 6 to 10 billion are in use worldwide. Power supplies sold and used in equipment are generally of two types, linear and switched. Most power supplies, as well as chargers and adapters which are built around a linear power supply are plugged into an AC wall socket and are left there indefinitely, even when not in use. Commercial linear power supplies are built around the low-tech iron core transformers using copper wires. These power supplies, chargers and adapters typically waste more than a watt, even when they are disconnected from the device they power.

Most electronic devices,

including newer high definition televisions and video and audio equipment are configured such that their power supplies are in the "on" state, even though the device itself is turned off. In non-consumer-related areas, the electronic equipment such as electronic security system (ESS) equipment panels, data communication equipment, video equipment, utility monitoring and control system (UMCS) electronic panels and electronic controllers, as well as supervisory control and data acquisition (SCADA) system electronic equipment panels have built-in power supplies. These power supplies serve the processors, communication and instrumentation cards.

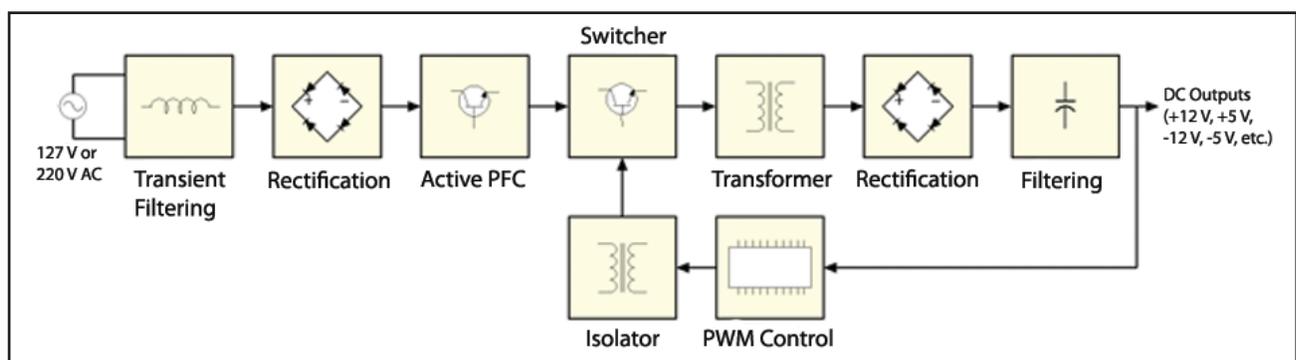
The California Energy Commission (CEC) issued an amendment to CEC regulations Dec. 15, 2004, to improve the efficiency of power supplies. This amendment forbids the use of energy wasting linear power supplies after July 2008. In 2006 the U.S. Department of Energy under the Energy Policy and Conservation Act (EPCA) and the

Energy Policy Act of 2005 (EPACT 2005) issued appliance energy efficiency standards.

The emergence of inexpensive, high-speed switching power transistors, low-loss ferrites for inductor cores and low-cost large scale integrated circuits containing all necessary control circuitry has significantly expanded the range of switching regulator in power supply application where lower heat dissipation and high energy efficiency are design requirements.

One advantage of the switching regulator over the more conventional linear regulator is greater efficiency, since cutoff and saturation modes are the two most efficient modes of operation. In the cutoff mode, there is a large voltage across the transistor but little current through it; in the saturation mode, the transistor has little voltage across it but a large amount of current. In either case, little power is wasted; most of the input power is transferred to the output and efficiency is high. Regulation is achieved by varying

See Power Supplies on page 7



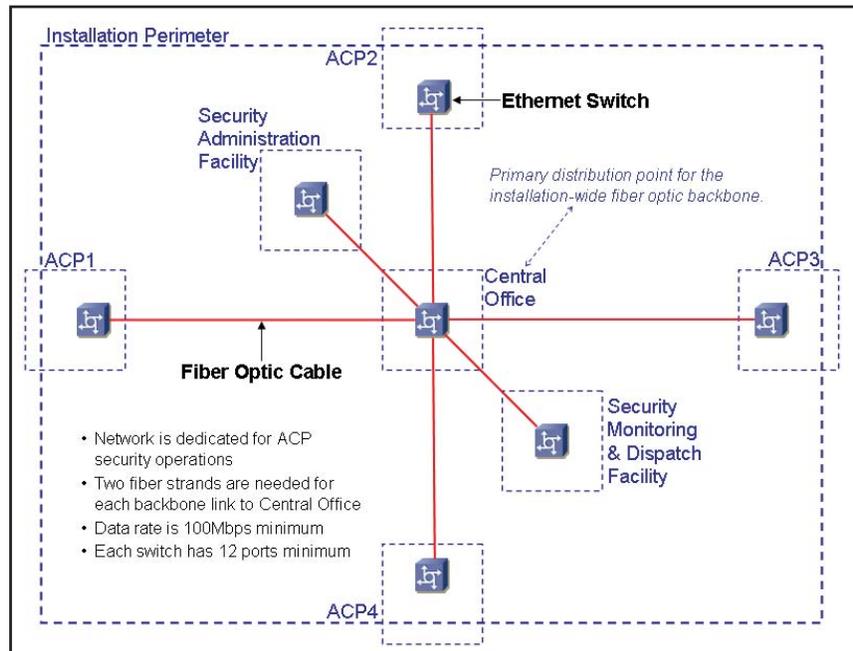
Block diagram of a switching power supply

# ACP

continued from page 1

then locate fiber termination points at ACPs. If fiber extends to an ACP it will often be terminated somewhere in the gatehouse or another nearby building. Detailed field notes and photographs should be taken for each ACP fiber termination describing the specific location and type of fiber optic cable. The number of fiber strands (total and unused) in the cable should be noted along with any DOIM labels on cables or patch panels. If backbone fiber is not available at an ACP, then the nearest point of connection should be determined and a fiber extension project initiated as soon as possible. It may be possible to employ ongoing DOIM initiatives such as the Installation Information Infrastructure Modernization Program (I3MP) to address ACP fiber connectivity deficiencies. The site survey report should contain enough information about fiber optic infrastructure, both existing cables and required upgrades, to design a network capable of supporting ACP security upgrades.

**Issue 2: Network architecture.** Once the issue of fiber optic infrastructure is addressed, the next



**Simple network architecture to support ACP security upgrades**

step in achieving ACP connectivity is designing a high-speed network. A standalone ACP network, physically separated from the existing DOIM network, is preferred due to the criticality and sensitivity of the data being transferred. This network must provide multiple connections at each ACP and at security administration, monitoring and dispatch facilities. For example, the network switch at a single ACP could require local ports/connections for a digital video recorder (DVR), video workstation computer, automated installation

entry (AIE) file server and an AIE workstation computer. The port configuration of the ACP switch should include a fiber-optic uplink to the backbone switch and enough local spares to accommodate new equipment in the future. The network should support Ethernet and TCP/IP protocols, and the data rate should be no less than 100 Mbps. A properly designed ACP network will support “plug-and-play” connectivity for a wide range of security equipment and ultimately enhance the force protection posture at the installation perimeter.

## 2008 Training Courses

### Electronic Security Systems (ESS) Design Course

- April 7 – 11                      Huntsville, Ala.
- April 28 – May 2                Bernkastel-Keus, Germany
- June 2 – 6                        Huntsville, Ala.
- Aug. 18 – 22                      Destin, Fla.

### Integrated Commercial Intrusion Detection System (ICIDS) System Administrator Course

- April 14 – 18                      Huntsville, AL
- July 14 – 18                        Huntsville, AL
- For more information, please call 256-895-1740.

## HSPD-12 Implementation Programs and Guidance

### December 2007

Federal Identity Credentialing Committee (FICC), URL: <http://www.cio.gov/ficc/>

GSA's FIPS 201 Evaluation Program, URL: <http://fips201ep.cio.gov/>

FIPS PUB 201-1, Personal Identity Verification (PIV) of Federal Employees and Contractors (March 2006), URL: <http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf>

NIST Special Publication 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems (May 2004), URL: <http://csrc.nist.gov/publications/nistpubs/800-37/SP800-37-final.pdf>

NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems (December 2006), URL: <http://csrc.nist.gov/publications/nistpubs/800-53-Rev1/800-53-rev1-final-clean-sz.pdf>

NIST Special Publication 800-73-1, Interfaces for Personal Identity Verification (March 2006), URL: <http://csrc.nist.gov/publications/nistpubs/800-73-1/sp800-73-1v7-April20-2006.pdf>

NIST Special Publication 800-76-1, Biometric Data Specification for Personal Identity Verification (January 2007), URL: [http://csrc.nist.gov/publications/nistpubs/800-76-1/SP800-76-1\\_012407.pdf](http://csrc.nist.gov/publications/nistpubs/800-76-1/SP800-76-1_012407.pdf)

NIST Special Publication 800-78-1, Cryptographic Algorithms and Key Sizes for Personal Identity Verification (August 2007), URL: [http://csrc.nist.gov/publications/nistpubs/800-78-1/SP-800-78-1\\_final2.pdf](http://csrc.nist.gov/publications/nistpubs/800-78-1/SP-800-78-1_final2.pdf)

NIST Special Publication 800-79, Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations (July 2005), URL: <http://csrc.nist.gov/publications/nistpubs/800-79/sp800-79.pdf>

NIST Special Publication 800-85A, PIV Card Application & Middleware Interface Test Guidelines (April 2006), URL: <http://csrc.nist.gov/publications/nistpubs/800-85A/SP800-85A.pdf>

NIST Special Publication 800-85B, PIV Data Model Testing Specification (July 2006), URL: <http://csrc.nist.gov/publications/nistpubs/800-85B/SP800-85b-072406-final.pdf>

NIST Special Publication 800-96, PIV Card to Reader Interoperability Guidelines (September 2006), URL: <http://csrc.nist.gov/publications/nistpubs/800-96/SP800-96-091106.pdf>

NIST Special Publication 800-104, A Scheme for PIV Visual Card Topography (June 2007), URL: [http://csrc.nist.gov/publications/nistpubs/800-104/SP800-104-June29\\_2007-final.pdf](http://csrc.nist.gov/publications/nistpubs/800-104/SP800-104-June29_2007-final.pdf)

# DIACAP

continued from page 2

administrators need to implement to test software and systems which conform to policy and protect the information content and the network operations.

An unwritten part of this process is that all personnel responsible for interfacing or connecting to any DoD system needs to take into account the time and associated cost implication of the certification and accreditation (C&A) process. Planners need to include in their schedule a window of 18 months to two years for C&A, from the start to completion of the process. This time frame is based on the assumption that at least two dedicated individuals, who are fully cognizant of the C&A process, with full authority of management to take all actions related to the C&A process, will be dedicated to obtaining the certification. In addition, the planners should be confident that there will be no major or complex issues related to the systems which are to be certified and accredited.

The certification process tests and certifies all software, including protocols, code, database applications, custom applications and graphics software to be installed on the new subsystems. Simply put all software and hardware is tested and certified for use on the shared network. Only after a contractor or agency has obtained the certification, via the DIACAP process, can the system hardware

and software be installed. This would include interfaces, communication software and application programs for ESS, UMCS, and SCADA system interfaced to the DoD network.

It is preferred that electronic security systems, and their sub-systems, i.e., intrusion detection systems and access control systems, are installed, operated and maintained as dedicated and independent systems. However, under various scenarios, such as distance, cost or user needs, connectivity of the ESS, UMCS or SCADA systems may require the use of DoD communication networks, or sharing sub-networks which are connected to DoD networks. Under such conditions it would be prudent to follow the DIACAP requirements so that the ESS, UMCS and SCADA systems conform to regulations and policy requirements of DoD, and AR 25-2.

## DIACAP process

To implement DIACAP for any system requires dedication, time and perseverance. The C&A process for most systems is lengthy and continues throughout the useful life of the systems. DIACAP generally includes the following steps:

a. Initiate and Plan Information Assurance (IA) – Certification and Accreditation Requirements

1. Register ‘System’ with DoD Component Information

Assurance Program

2. Assign IA Controls
3. Assemble DIACAP Team
4. Initiate DIACAP Implementation Plan

b. Implement and Validate Assigned IA Controls

1. Execute DIACAP Implementation plan
2. Conduct validation activities
3. Complete validation results in DIACAP scorecard

c. Make Certification Determination and Accreditation

1. Make certification determination
2. Issue accreditation decision

d. Maintain Authority to Operate and Conduct Reviews

1. Maintain situational awareness (Review of IA Controls must occur at least annually)
2. Maintain posture

e. Decommission

1. Retire system

An indepth understanding of the DIACAP methodology leads to successful installation of secure, regulation-compliant ESS, UMCS and SCADA systems.

Implementing DIACAP enables users to use the available DoD networks and data communication resources, when permitted by policy, and reduces overall system cost.

## You can learn more about Huntsville Center and its many programs by accessing online fact sheets.



Find fact sheets on:

*Access Control Points*

*Electronic Security Systems*

*Utility Monitoring and Control Systems*

*... and many more!*

Check them out at [www.hnd.usace.army.mil/pao/factshts.aspx](http://www.hnd.usace.army.mil/pao/factshts.aspx)

## Power Supplies

continued from page 3

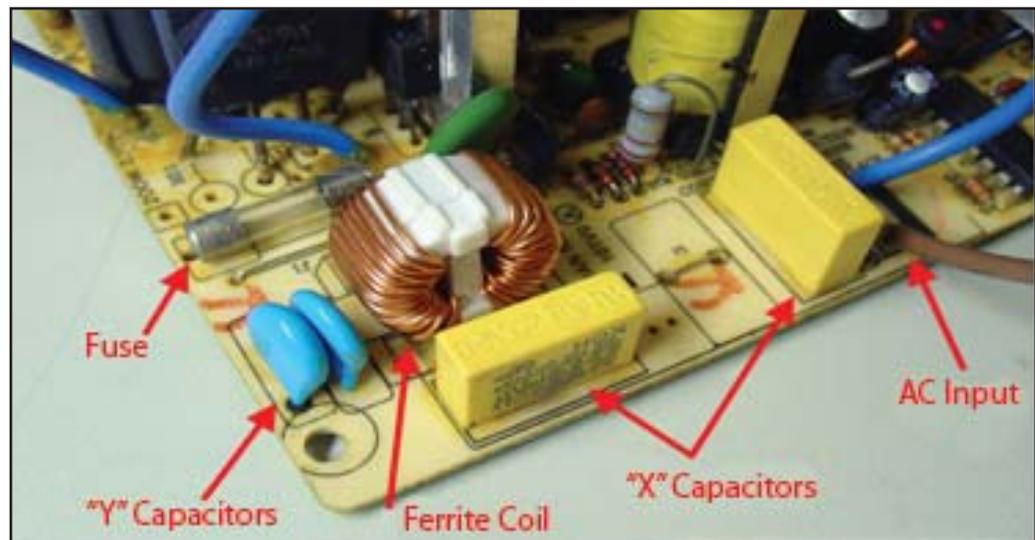
the duty cycle that controls the average current transferred to the load. As long as this average current is equal to the current required by the load, regulation is maintained. Besides high efficiency operation, another advantage of the switching regulator is the increased application flexibility offered by output voltages that are less than, greater than, or of opposite polarity to the input voltage.

Sound energy conservation in combination with good engineering

practices will result in having lower power consumption and smaller power supplies. A word of caution is to locate power supplies especially in tight enclosures with adequate separation from communication circuits for data and video.

Electromagnetic interference (EMI) from adjacent power consuming devices and radio frequency interference (RFI) generated devices can result in communication data packet loss and bit error in digital signals.

Use of filters and shielding of power supplies from communication or data processing chips and circuits would be necessary to maintain reliable alarm and data communication transmission.



A switching power supply with components identified

U.S. Army Engineering and Support Center, Huntsville  
4820 University Square  
Huntsville, AL 35816-1822

Phone: 256-895-1740  
DSN: 760-1740  
Fax: 256-895-1519

---

**Check us out online:**

## ESC

[www.hnd.usace.army.mil/esc](http://www.hnd.usace.army.mil/esc)

- **History of the ESC**
- **Why choose the ESC?**
- **List of clients**
- **Services offered**

## UMCS

[www.hnd.usace.army.mil/umcs](http://www.hnd.usace.army.mil/umcs)

- **What does UMCS offer?**
- **Why choose UMCS?**

---

## Useful Acronyms:

**ACP:** Access Control Point

**ESC:** Electronic Security Center

**ESS:** Electronic Security Systems

**ETSC:** Electronic Technology Systems Center

**MCX:** Mandatory Center of Expertise

**UMCS:** Utility Monitoring and Controls Systems

# ASK MCX!

**Q: I am looking for updated information on acquisition and use of electronic access control equipment for facilities and compliance with HSPD-12 and FIPS 201. Do you have any information or know of any Army guidance?**

**A:** Unfortunately, there is no simple Army guidance for fielding of physical access control systems that comply with HSPD-12 and FIPS-201. For new access control systems, we recommend they support both the new contactless CAC (common access card) as well as standard proximity cards. The list of other guidance that may be helpful is on page 5.

---

## Who We Are

The Electronic Technology Systems Center (ETSC) is a team within the U.S. Army Corps of Engineers that provides unmatched experience and technical expertise in the specialized fields of Utility Monitoring and Control Systems (UMCS) and Electronic Security Systems (ESS).

Located in Huntsville, Ala., the ETSC supports the Corps of Engineers, the Army, other services and various defense and federal agencies. ETSC has hundreds of active projects around the world.

In its technical consulting role, the ETSC performs engineering surveys, develops criteria, reviews designs and conducts special studies and training for a wide variety of customers. For those customers needing “turn-key” project execution, the ETSC provides indefinite delivery, indefinite quantity (ID/IQ) contracts for system engineering, procurement and installation through a seamless, expedited task order process.

Each year the ETSC participates in numerous conferences, symposia, working groups and trade shows to build relationships and influence future development and application of UMCS and ESS technology.

---

---

## Point of Contact

**contact-esc@usace.army.mil**  
**256-895-1740**