Don't Miss The NEWEST Training For Security & Identity Professionals…
Packed with the latest plans, solutions, and requirements for identity credentials to help you move to an integrated system and achieve results!

IDENTITY MANAGEMENT FOR GOVERNMENT

Planning For The Operational Use, Implementation And Interoperability Of Identity Credentials

September 13-15, 2010 • Washington, DC

Rave Review from a Past Identity Conference Attendee:

"Good opportunity for receiving information on HSPD-12. It was interesting to hear the ideas and processes of other agencies. I have a better idea of requirement challenges and GSA approvals for systems and smartcards."
Visitor Control Lead
NATIONAL NUCLEAR SECURITY ADMINISTRATION

★★★★★ Register by July 15th To Save $400! ★★★★★
Register 3 and send a 4th for FREE!
To Register, Call (888) 362-7400 -or- (773) 695-9400

REGISTER TODAY!
www.aliconferences.com
Call TOLL FREE: (888) 362-7400 • Phone: (773) 695-9400 • Fax: (773) 695-9403
Mail to: Advanced Learning Institute, 8600 W. Bryn Mawr Ave., Suite 920-N, Chicago, IL 60631

KEY TAKE AWAYS:

Attend this conference to learn how to develop an effective identity management strategy and roadmap -- from policy to implementation -- along with helpful solutions, tools, tips and guidance to get started, including:

- **Understanding** the key technologies – how they work, costs and benefits, strengths and weaknesses – through various identity credential case study examples
- **Overcoming** the common obstacles of deploying the various credentials: Personal Identity Verification (PIV), Personal Identity Verification – Interoperable (PIV-I), Personal Identity Verification – Compatible (PIV-C), Transportation Worker Identification Credential (TWIC), Common Access Card (CAC), First Responder Authentication Credential (FRAC), etc.
- **Achieving** interoperability at the user level
- **Planning** for implementation and getting buy-in across the organization
- **Using** identity credentials for more than just flash passes - - to maximize investments in identity programs

SPEAKING ORGANIZATIONS:

Join your colleagues for this must-attend industry summit featuring best-practice examples and case studies from government experts who have successfully developed identity management systems and solutions, including:

U.S. General Services Administration

National Aeronautics and Space Administration

U.S. Department of Education

Transportation Security Administration

Defense Manpower Data Center

Federal Emergency Management Agency

Commonwealth of Virginia

Deloitte & Touche, LLP

Federal Bureau of Investigation

U.S. Department of Homeland Security

- **Implementing** identity credentials for federal, state and local government employees and contractors
- **Demonstrating** the ROI of standardized identity management credentials
- **Executing** Identity, Credential, and Access Management (ICAM) – an identity and access management solution in your agency
- **Transforming** identity and access management into a more centralized activity to ensure security
- **Considerations** for PIV in a physical access control system
- **Incorporating** Public Key Infrastructure (PKI) to build trust in a federated system of identity
- **Establishing** policies, procedures and technology to support HSPD-12
- **Credentialing** not just individuals, but entire responder units
- **Practical uses** in the first responder world – going beyond implementation for just non-emergency events
- **Differentiating** between PIV, PIV-I, PIV-C
- **Deploying** identity management credentials on a shoestring budget
- **Building** the business case for the construction of unified and standardized identity management infrastructures
- **Integrating** and developing compliant credentialing systems for large and small populations
- **Achieving** compliance with Federal laws, regulations, standards and governance related to ICAM
- **Reducing** costs and increasing efficiency with ICAM to yield big payoffs
- **Developing** performance goals for identity systems
- **Incorporating** biometric information into your identity management system
- **Partnering** with other government and non-government agencies and organizations to determine standards and enable interoperability
- **Understanding** and using identity management standards to ensure interoperability and trust

International Biometric Group

Pentagon Force Protection Agency

State of West Virginia

Daon

CertiPath LLC

American Trucking Associations

ActivIdentity

Microsoft

Adobe Systems Incorporated

Verizon

Supporting Organizations:

IBIA
The International Biometrics & Identification Association

pipeline
global security

BioAPI™

POLICE LINE DO NOT CROSS
Terrorism, Crime, Natural Disaster and Accidents...
Contingency Today

HomelandSecurityToday™
HOMELAND SECURITY INSIGHT & ANALYSIS

Presented by:

Advanced Learning Institute

Your Government & Security Training Partner Since 1997

***** Register by July 15th To Save $400! *****
Register 3 and send a 4th for FREE!
To Register, Call (888) 362-7400 -or- (773) 695-9400

MAXIMIZE YOUR TRAINING!
Choose From Two Workshops For Ultimate Value And Learning!
Sign up for your choice of these highly-interactive workshops:

- **Pre-Conference Morning Workshop –**

  Monday, September 13, 2010, 8:30 a.m. – 11:30 a.m.:
  Understanding And Using Identity Management Standards To Ensure Interoperability And Trust

- **Pre-Conference Afternoon Workshop –**

  Monday, September 13, 2010, 1:00 p.m. – 4:00 p.m.:
  How To Integrate Biometric Technologies Into Your Identity Credentialing Program:
  Strategies For Deploying Successful Identity Management Systems

WHO WILL ATTEND:

This conference has been researched with and designed for Federal, State and Local Government Managers, Directors, Program Managers, Analysts, Leaders, Officers, Administrators, CIOs, Specialists, Advisors, Coordinators, Staff, Consultants and Contractors involved in:

- Information Technology
- Access Control
- Physical Security
- Enterprise Security
- Operations
- Information Security
- Network Communications Security
- Identity Management
- Biometrics
- Security and Safety

… and all other End Users, Consultants, Contractors, Designers & Developers of Security & Identification Technologies who are interested in the latest identity management developments & how it can benefit their organizations.

Don't miss out on this excellent networking opportunity!

PAST ATTENDEES Include Representatives From:

The Metro-Herald • NIST • Lucent • Defense Manpower Data Center • Social Security Administration • U.S. Department of Defense • Privaris, Inc. • Ingersoll Rand Security Technologies • FAA • Pacific NW National Labs • CoreStreet • ActivIdentity • CTC • Perot System/BWXT-Y12 • IBIA • BearingPoint • Oberthur • The Higgins-Hermansen Group • U.S. Small Business Administration • Identification Technology Partners • Nuclear Regulatory Commission • Identix, Inc. • Merkatum • International Biometric Group • PricewaterhouseCoopers • Bioscrypt • National Biometric Security Project • DSCI • Nortel Government Solutions • Dreifus Associates • Pearson Government Solutions • ImageWare Systems, Inc. • U.S. Coast

Guard • Mitretek Systems, Inc. • U.S. General Services Administration • SPAWAR Systems Center • Federal Reserve Board • Daon • Bureau of Economic Analysis • Department of the Treasury, FMS • IBM Global Business Services • Bamboo Technologies

BENEFITS OF ATTENDING THIS CRITICAL EVENT:

- **29 innovative speakers** at your disposal to share their strategies and experiences in identity credentialing fundamentals that are already proven to work
- **Over 18 hours of intense, interactive learning** - we guarantee you will recoup your money spent by implementing just a few of the strategies shared during the conference
- **The opportunity to customize your learning** by participating in the unique and interactive workshop sessions that will enable you to practice and apply your skills in peer groups -- you will walk away with strategies and tactics that you can begin to implement in your own organization
- **An abundance of networking opportunities** - be sure to bring plenty of business cards to exchange with your fellow attendees
- **A comprehensive overview of identity management strategies and processes** from leading practitioners like the **U.S. General Services Administration, National Aeronautics and Space Administration, Defense Manpower Data Center,** and many more
- **Acquiring new knowledge** to lead your organization through the imperative, yet sometimes extremely difficult, responsibility of ensuring that your physical and logical security systems are secure
- **A complimentary packet of research materials** that will serve as a helpful resource long after you have attended this conference
- **A formal Certificate of Completion** which documents your training achievement and commitment to continuing professional development
- **Optional networking lunches** that will give you the opportunity to brainstorm and benchmark solutions with your fellow attendees
- **Participating in instructional sessions** that will share real-world examples, tactics and lessons learned from leading identity management and security initiatives that will ground you in advancing your own strategy

A LETTER FROM THE CONFERENCE CHAIRPERSON:

Deloitte.

Dear Government Executive:

Identity management is becoming increasingly important to the business operations of every organization. Whether you are part of a Federal agency, state or local government or private industry, moving forward means rethinking how you do business in every area, helping to make sure that the right people have access to information and facilities while protecting and preventing access to those that shouldn't. This is no longer limited to just people in your own organization. The effective use of identity and trust makes this possible. Because of HSPD-12, Federal employees and contractors now have PIV cards. But is this the end or the beginning? As Winston Churchill pointed out, perhaps this is the end of the beginning.

Progress requires innovation and/or transformation. That requires looking at what we do and seeking to make use of new and effective tools to help us do our jobs better. Not sure how to do it? Then this conference is for you. You will hear from those who are already making progress. Everything from making use of the PIV, operating in emergency conditions, outreach to the private sector to interactions with citizens will be covered. The tools of identity aren't the end; they are enablers to help you do your job better.

YOU CAN'T AFFORD TO NOT ATTEND!

Attend the **Identity Management for Government Conference** on September 13-15, 2010 in Washington, DC and learn how to take advantage of new capabilities, help move the government forward, better serve the nation, and increase capability while still promoting security and privacy. You will hear insights, backed up by experience, in an engaging environment, on how identity management tools have been brought to bear to make government agencies more effective, including how:

- **U.S. General Services Administration** implemented a logical access credential management project at a low cost
- **Defense Manpower Data Center** has been aggressively working to accommodate federated credentials, without sacrificing the security of the U.S. Department of Defense, despite its unique working situations
- **Commonwealth of Virginia** used its FRAC Program to expedite response and recovery efforts in emergency situations by facilitating an efficient verification of identity and attributes/skill sets and protecting responders from unauthorized access
- **U.S. Department of Homeland Security** has begun shaping the national security landscape by encouraging State and local government organizations to engage private sector partners in focusing on mutual interests that include planning, protective measures and strategic response/recovery efforts

The time is now. In recent history, there has never been a better time for innovation and transformation. Strong initiatives for transparency, reinforced by penalties for non-performing programs, make business as usual unacceptable. Inclusion of identity management into the Federal Enterprise Architecture means you will have to do more toward this end. Most importantly, being able to serve your customers better, more effectively and more efficiently, is the right thing to do.

This conference is the ideal forum for you to share successes and challenges, get ideas and suggestions, learn proven methods, processes and approaches for identity management. Call, toll-free, 888-362-7400 or visit www.aliconferences.com to register yourself and your colleagues, today!

I look forward to seeing you this September!

Sincerely,

James D. McCartney, Identity Management and Privacy Consultant
Deloitte & Touche, LLP
Conference Chairperson

RAVE REVIEWS FROM PAST SECURITY CONFERENCE ATTENDEES:

“Very interesting topics presented – will definitely consider attending again! Nice mix of backgrounds/industries; the speakers were good at addressing all of them.”
K. Davis, IT Specialist
U.S. DEPARTMENT OF COMMERCE

"As a first time attendee, this was a great way to see the various issues and successes…”
R. Carson, Technical Manager
PEC SOLUTIONS, INC.

"Well organized, great presenters with timely and pertinent information."
N. Blacker, Major
U.S. ARMY

"Overall, an excellent selection of speakers.”
S. McCallum, System Analyst
PINELLAS COUNTY SHERIFF’S OFFICE

"The conference provided information that will now enable me and my colleagues to make an informed decision."
G. Williams, Program Manager
U.S. DEPARTMENT OF HOMELAND SECURITY

"I really appreciate hearing about real world projects from both the user/customer and integrator/vendor perspectives."
C. Tilton, VP, Standards & Emerging Technology
DAON

PRE-CONFERENCE WORKSHOPS: Monday, September 13, 2010

Take identity management from complexity to clarity through these interactive workshops guaranteed to jumpstart your conference experience. These information-packed sessions are a great opportunity to network with fellow attendees while taking a hands-on, common-sense approach to mastering identity management that will enhance your understanding of the informative, case study presentations throughout the entire conference.

8:30 a.m. to 11:30 a.m.

PRE-CONFERENCE MORNING WORKSHOP

Registration will begin at 8:00 a.m. Refreshments will be served.

Understanding And Using Identity Management Standards To Ensure Interoperability And Trust

Standards provide the underpinning for many successful systems, initiatives, and their underlying components and technologies. This is also true for the area of identity management, particularly in a federated context where interoperability and trust are essential. This session will identify and describe the technical and process standards that apply in the area of identity management. Participants will learn what standards exist, who developed them, what they contain, where to find them, and how they apply.

In particular, five areas of standardization will be addressed:

1. Identity management
2. Smart cards
3. Biometrics
4. Public Key Infrastructure (PKI) technologies
5. Credentialing

Don't miss this opportunity to learn what you need to know to utilize these standards effectively in your identity management programs.

WORKSHOP LEADERS: Catherine J. Tilton, VP for Standards & Emerging Technologies at Daon, has over 25 years of engineering and management experience, including over 15 years in the biometrics industry. She has led the design, development, and deployment of numerous biometric systems in both the commercial and government domains, many of which involved smartcards. Cathy is also very active in the development of national and international biometric standards, currently serving as the US head of delegation to ISO/IEC JTC1 SC37 subcommittee on biometrics and chair of the Biometric Identity Assurance Services (BIAS) Integration technical committee at OASIS.

Andrew Webb, Principal Technical Consultant at Daon, has worked on the TWIC (GSC-IS 2.1 and PIV versions), and Registered Traveler (Verification station HSM) smart card projects. In 1995, Andrew started working with Smart Cards in 1995 with Cybermark (MPCOS), and also worked for Giesecke Devrient (Visacash, Starcos,Javacard), Motorola (Javacard), Litronic (CAC), and Saflink. He holds a BS from Carnegie Mellon in Applied Mathematics and a MBA from Imperial College.

Testimonials From Past Cathy Tilton Sessions:

"Cathy brings outstanding knowledge and energy to her presentations!"

"Very knowledgeable about subject. Excellent speaker!"

"Cathy was a wealth of knowledge and a captivating speaker."

11:30 a.m. to 1:00 p.m.

Lunch on your own

1:00 p.m. to 4:00 p.m.

PRE-CONFERENCE AFTERNOON WORKSHOP

How To Integrate Biometric Technologies Into Your Identity Credentialing Program: Strategies For Deploying Successful Identity Management Systems

This session will focus on best practices for deploying biometric-enabled identity management systems in large scale government and commercial programs. It will focus on the impact of biometrics on your identity system architecture, considerations for purchasing biometric hardware and software, proper collection methods, and common deployment pitfalls. The discussion will also include interoperability considerations, as well as case studies illustrating the usage of various biometric modalities for credentialing and identity management.

Attend this workshop and learn how to overcome the pitfalls and challenges that can develop during the deployment of biometric-enabled identity management systems. Specifically, you will:

- Learn from real-world examples of identity management systems that successfully utilized biometrics
- Identify the positive and negative impacts biometrics will have on your credentialing program
- Compare and contrast high quality enrollments with low quality enrollments – and learn how to obtain high quality enrollments consistently
- Discuss solutions to common problems of deploying biometrics, such as lack of interoperability between systems and end user privacy concerns

WORKSHOP LEADER: Joy Kasaaian is a Sr. Consultant with International Biometric Group. Joy provides strategic consulting services to biometric and non-biometric firms. Prior to IBG, Joy worked in GlaxoSmithKline's Scientific Computing and Mathematical Modeling Group and received a Bachelor of Science in Biomedical Engineering from the University of North Carolina at Chapel Hill.

Testimonials From Past Joy Kasaaian Sessions:

“I appreciated how Joy engaged the audience and asked for participation.”

“Well presented.”

“Very effective. Engaging presenter.”

AGENDA - DAY 1: Tuesday, September 14, 2010

8:00 a.m.

Registration, Continental Breakfast & Exhibits

8:30 a.m.

CHAIRPERSON'S WELCOME

Chairperson's Welcome & Opening Remarks

James D. McCartney, Identity Management and Privacy Consultant
DELOITTE & TOUCHE, LLP

8:45 a.m.

KEYNOTE PRESENTATION

An In-Depth Look At Identity, Credential And Access Management (ICAM): A Roadmap And Implementation Guidance For Success

The Federal Government has built government-wide infrastructure for common and secure identity, credential and access management (ICAM) through four principal components – the Federal Public Key Infrastructure (PKI), Homeland Security Presidential Directive 12 (HSPD 12), Open Identity for Open Government, and the Federal e-Authentication initiative.

This session will examine each of these infrastructure components, how they are inter-related, and the status of deployment across government as well as other non-federal user communities. Attendees will leave with a greater understanding of the U.S. Federal Government's processes for Trusted Identity Federation and for certifying non-federal identity federation trust providers. You'll also learn about the U.S Federal Government's trust model for federated identity and the requirements and testing for interoperability across organizations, systems and components.

Don't miss this opportunity for increased insight on the Federal Identity and Access Management Infrastructure, including:

- The Federal ICAM components
- The Federal Identity Trust model
- The basis for interoperability
- Interoperability and conformance testing for products, components, and systems

David Temoshok, Director, Federal Identity Management
Office of Governmentwide Policy
U.S. GENERAL SERVICES ADMINISTRATION

9:45 a.m.

Speed Networking

Become acquainted with your fellow attendees in this fun and fast-paced forum!

10:15 a.m.

Morning Networking Break & Exhibits

10:45 a.m.

CASE STUDY

Federating Identity In The U.S. Department Of Defense: How To Integrate Multiple Identity Management Efforts Into A Single System While Maintaining Security

As the Federal Government moves toward a more integrated approach to identity, harmonizing existing efforts with new directions offers significant challenges to Federal agencies. It isn't enough to just create new capabilities; efforts must be an answer to existing requirements within the organization and must be able to meet those needs sufficiently to gain the trust of the people in the Department.

The U.S. Department of Defense (DoD) has some of the most challenging environments to work in and any identity management solution must be able to function in those unique situations. Whether it's operating at remote bases in Afghanistan, on a ship, or in an office, employees must be able to access their workspaces and computers. DoD also deals with a wide variety of people who do not receive credentials for the Department that must be accommodated. DoD is aggressively working to accommodate federated credentials, without sacrificing security.

In this session, you will learn:

- What does Rapid Electronic Authentication really mean?
- PIV-I: Who should be doing it?
- Attribute exchange - enabling trust through information
- Integrating multiple efforts into a single approach
- How to avoid breaking your systems

Irving R. (Bob) Gilson, Program Office Branch Chief
Personal Identity Protection Solutions (PIPS) Division
DEFENSE MANPOWER DATA CENTER

11:30 a.m.

CASE STUDY

Next Generation Identification:
The Future Of National-Scale Multimodal Biometric Systems

Driven by advances in technology, customer requirements, and growing demand for Integrated Automated Fingerprint Identification System (IAFIS) services, the FBI has initiated the Next Generation Identification (NGI) program. The NGI system is being developed over a multi-year timeframe and will be an incremental replacement of the IAFIS that provides new functionality and improves upon existing capabilities. This technology upgrade will accommodate increased information processing and fuse together information sharing from local, state, federal, and international agencies. The NGI system will offer state-of-the-art biometric identification services and provide a flexible framework of core capabilities that will serve as a platform for multimodal functionality.

Don’t miss the latest update on the FBI’s Next Generation Identification program and considerations for your own identity management systems.

Robert Holman, Management & Program Analyst, NGI
FEDERAL BUREAU OF INVESTIGATION

12:15 p.m.

Lunch On Your Own -- But Not Alone!

Join a small group of your colleagues for lunch with an informal discussion facilitated by one of our expert speakers. Take this opportunity to join others in an interactive group setting to network and brainstorm solutions to your most pressing identity management concerns.

1:45 p.m.

INTERACTIVE SESSION

Panel Discussion: An Inside Look At Establishing Interoperability Between Federal, State And Local Emergency Response Officials

The Command, Control and Interoperability (CCI) Division within the Science & Technology (S&T) Directorate, the FEMA Office of National Capital Region Coordination (NCRC), the FEMA Office of the Chief Security Officer (OCSO), and the FEMA Office of the Chief Information Officer (OCIO) have partnered to create the PIV-I/FRAC Technology Transition Working Group (TTWG). The TTWG is composed of State and Local government emergency management representatives, many of whom have already implemented innovative and secure identity-management solutions in their own jurisdictions.

The goal of the working group is to:

- Provide Federal policy makers with a unified State emergency manager perspective on Federal/Emergency Response Official (F/ERO) attributes
- Baseline current identity infrastructure and best practices to share with stakeholders
- Identify technological gaps where CCI can provide test bed research and development support
- Share information: State-to-State, State-to-Federal, and Federal-to-State

The working group is focused on exploring PIV-I credentials as the standard that enables interoperability between local and State emergency response officials. PIV-I is a trusted identity and credentialing standard developed by the Federal Government for non-Federal issuers. Non-Federal entities that elect to conform to the PIV-I standard will be trusted by and interoperable with Federal agencies at assurance level 4. These authentication assurance levels are described fully by OMB M-04-04.

Through the efforts of the TTWG, your state and local emergency response partners will be equipped to provide seamless and secure interactions that ensure public safety.

Learn from the experiences of this innovative Federal, state and local government partnership how you can incorporate best practices to help transform your own identity management efforts.
Moderated By:
Craig Wilson, Sr. Consultant, NCRC
FEDERAL EMERGENCY MANAGEMENT AGENCY

Panelists:
Karyn Higa-Smith, Program Manager, Science & Technology (S&T) Directorate, Command, Control and Interoperability (CCI) Division
U.S. DEPARTMENT OF HOMELAND SECURITY

Charles Luddeke, Chief of Physical Security, Office of the Chief Security Officer
FEDERAL EMERGENCY MANAGEMENT AGENCY

Elisa Cruz, Chief Information Security Officer, Office of the Chief Information Officer
FEDERAL EMERGENCY MANAGEMENT AGENCY

Mike McAllister, Deputy Assistant to the Governor for Commonwealth Preparedness
COMMONWEALTH OF VIRGINIA

Pamela Holstein-Wallace, West Virginia Region III Coordinator
STATE OF WEST VIRGINIA

2:45 p.m.

CASE STUDY

FIPS 201 Standards-Based Interoperable Credentialing Of First Responders: Enhancing Cooperation And Efficiency Across Multiple Jurisdictions

The First Responder Authentication Credential (FRAC) is an interoperable standards-based (Federal Information Processing Standards 201 [FIPS 201]) identification smart card designed to provide federal, state, local and private sector emergency responders with the ability to quickly and easily gain access to an all-hazards event across multiple jurisdictions. The Virginia FRAC Program serves as a model for other regions to enhance cooperation and efficiency between emergency responders before and during a critical incident. It expedites response and recovery efforts by facilitating a more efficient verification of identity and attributes/skill sets and enhancing the protection of emergency responders and Critical Infrastructure / Key Resources (CI/KR) from unauthorized access during an event.

To date, the Commonwealth of Virginia has issued over 2,300 FRACs and participated in multiple “proof of implementation” and COOP/COG DHS multi-state exercises. Through participation, the Commonwealth of Virginia has demonstrated that its FRACs are interoperable with other FIPS 201 compliant and interoperable federal, state and private industry credentials. In 2010, the Commonwealth will issue an additional 12,900 FRACs in the Hampton Roads and other regions.

This session will provide you with insight on the Commonwealth of Virginia's experience with the implementation of an interoperable FIPS 201 standards-based credentialing program, including:

- An overview of the FIPS 201 interoperable credentialing standard
- Enhanced capabilities provided by an interoperable and trusted credentialing program
- Stakeholders (public and private sector)
- Credentialing strategies
- Funding

Mike McAllister, Deputy Assistant to the Governor for Commonwealth Preparedness
COMMONWEALTH OF VIRGINIA

3:30 p.m.

Afternoon Networking Break & Exhibits

3:45 p.m.

CASE STUDY

How To Leverage Public-Private Partnerships In Security Management, Access Control And Credentialing

The U.S. Department of Homeland Security, Office of Infrastructure Protection implemented the Critical Infrastructure Key Resources (CIKR) Partnership Framework as the foundation for collaboration between Federal government and CIKR Private Sector Partners. Focusing on mutual interests that include national planning, protective measures and strategic response/recovery efforts, these coordinating council partnerships assist to shape the national security landscape.

State and local government organizations are now leveraging similar frameworks as models to engage private sector partners in identifying priorities that include incident management and processes for access control and credentialing.

This session will share the critical success factors of successful partnerships, including:

- Identifying Key Partners
- Cultivating the Purpose
- Measurements for Success

You will leave this session equipped with new strategies to help you establish your own partnership model.

Renee Murphy, Section Chief, Partnership Programs, Partnerships and Outreach Division
Office of Infrastructure Protection
U.S. DEPARTMENT OF HOMELAND SECURITY

4:30 p.m.

CASE STUDY

The Transportation Worker Identification Credential (TWIC) Program: An Update On One Of The Largest Government-Sponsored Biometric Identity Programs

This presentation will provide you with an overview of the (TWIC) program that is jointly managed by the Transportation Security Administration (TSA) and the U.S. Coast Guard. TSA has enrolled 1.5 million civilian maritime workers in the TWIC program and has issued a smart card credential with biometric and other security features to each worker who passes a security threat assessment and background screening process. Possession of a TWIC card is required for unescorted access to restricted areas of maritime facilities and vessels regulated under the Maritime Transportation Security Act (MTSA).

Attendees will learn the background and legal authority for the TWIC program, its current status, and lessons learned in deploying the first massive government-led secure credentialing program to a civilian population. In particular, this session will share:

- An overview of the TWIC program – including objectives, legislative authority and current operational status
- The status of the field pilot test of TWIC reader products
- A review of the technology behind TWIC and how it is aligned with HSPD-12 directive and FIPS 201 standards
- The outlook for future rule making that will lead to regulatory requirements for the deployment of TWIC reader devices

John Schwartz, Deputy Program Director – TWIC

TRANSPORTATION SECURITY ADMINISTRATION

Gerry Smith, Subject Matter Expert (SME) Support Contractor to TSA
IDENTIFICATION TECHNOLOGY PARTNERS

5:15 p.m.

End Of Day One

5:30 p.m.

Networking Reception: Please Join Us!

We invite you to join us for a drink as you relax with your peers. All conference attendees, speakers and exhibitors are welcome to join us for this special opportunity to continue networking. Don't miss this chance to benchmark new ideas over complimentary drinks!

7:00 p.m.

Dine Around

Sign up during the day for dinner with a group. Take advantage of Washington, D.C.'s fine dining while you continue to network with your colleagues.

AGENDA - DAY 2: Wednesday, September 15, 2010

8:00 a.m.

Continental Breakfast & Exhibits

8:30 a.m.

CHAIRPERSON'S ADDRESS

Chairperson's Opening Of Day Two & Presentation: Why Identity Management – It's Not Just About Security

Making identity management important to the average person means making it personal. There are few things in today's world that represent a more clear and visceral threat to individuals than identity theft. If the problem was, as many people think, limited to credit cards, it wouldn't be much of an issue. The fact is that anything that you can do in your name… so can someone else.

Your whole life may crumble when someone uses your name to get healthcare (how many million people are without coverage?) and you are denied coverage because of what they did. What happens when an illegal immigrant uses your SSN to get work (an unintended consequence of eVerify) and you don't report their income to the IRS? Perhaps it is that when you retire and find that someone is already collecting your Social Security benefits that it becomes important.

The fact is, many of the issues relating to identity theft do or will come back to the government to solve. In this session, we will discuss:

- What identity theft really is and why it matters
- The importance of how the government responds

- What happens when things go wrong
- Ways to move forward based on effectiveness, not perfection

James D. McCartney, Identity Management and Privacy Consultant
DELOITTE & TOUCHE, LLP

9:40 a.m.

CASE STUDY

Implementing HSPD-12 Provisions On A Shoestring Budget

The U.S. General Services Administration started their credential management program using an Access database with scripts to import required data from its HR system. The little Access database grew into a web application that required the Personal Identification Verification Credential (PIV Card) for login. The CIO Council's Logical Access Working Group assisted many small agencies in getting their systems ready for mandatory usage of the PIV Card in Federal Information Security Management Act (FISMA) reporting. What these and other projects have in common is that they were all implemented without costly third-party packages.

Attend this session and learn how your agency can implement a credential management project at a low cost. Specifically, you will learn:

- Pre-implementation planning requirements
- How networks can implement smartcard login without costly add-on packages
- How web applications can use client certificates for identity verification using only what is built into the web server operating system
- Which pieces of an entire solution can be implemented separately – it doesn't have to all happen at once

William Erwin, Program Manager
Identity, Credential & Access Management Office
U.S. GENERAL SERVICES ADMINISTRATION

10:25 a.m.

Morning Networking Break & Exhibits

10:45 a.m.

CASE STUDY

Identity Assurance Using Smart-Card Access Control And Multi-Modal Biometrics

The Pentagon Force Protection Agency (PFPA) is responsible for the physical security needs of the Pentagon reservation, Mark Center (under construction) and National Capital Region (NCR) facilities. The Concept of Operations was developed with a goal to transition to a FIPS 201-1 compliant Physical Access Control System (PACS). The existing PACS at the Pentagon reservation itself has over 7,000 card readers, 2,100 control panels and 90,000 active cardholder records. The future PACS will support the required identity assurance levels using smart card-based access control and multi-modal biometrics.

The goal of the PFPA HSPD-12 program is to leverage best practices and technology to ensure all personnel are correctly identified and authorized to access the resources of the Pentagon, including:

- Leveraging the mechanisms provided by the CAC to increase security
- Assigning a single identity per person for all activity in Pentagon
- Biometrically binding people to their identity
- Automating processes and reducing paperwork through the use of digital signatures
- Electronic accountability of all personnel – no more “flash” pass

This session will discuss the particular processes PFPA followed to prepare for HSPD-12 FICAM implementation, including:

- Developing requirements
- RFI’s to industry
- Developing a roadmap for implementation
- Product testing
- Concept of Operations, Standard Operating Procedures, lessons learned
- Education & Awareness
- Creating a training plan
- Budgeting

Lemar Jones, Director, Antiterrorism/Force Protection Directorate
PENTAGON FORCE PROTECTION AGENCY

11:30 a.m.

CASE STUDY

How To Leverage Cross-Agency Investments And Achieve Multiple Security Functions Using An External IT Vendor

The U.S. Department of Education’s Office of Management (OM) along with the Office of the Chief Information Officer (OCIO) jointly formed an Integrated Process Team (IPT) to develop, design and field a two-factor credential/token based on the already developed and fielded HSPD-12 / FIPS 201 compliant PIV credential. After OM initially addressed the physical access control (PACS) requirements of the standard, the OCIO reached out to leverage the PIV credential for the development of Logical Access control (LACS) capabilities. Adding an additional layer of complexity to the challenge, was that the Department’s IT infrastructure and environment was owned and operated by an external IT vendor. Key to the successful implementation of the LAC’s program, as well as the Enterprise Identity Management architecture, was the ability to develop the relationships necessary to leverage the Department’s Windows Active Directory platform, as the source for PIV authentication and end-user verification.

This presentation will address key steps and strategies that can lead to a successful implementation of your organization’s Identity Management program and HSPD-12 / PIV solution, including:

- Formalization of departmental interagency roles and responsibilities
- The importance of a pre-issuance specification
- Obtaining senior leadership buy in
- Negotiations - union participation and acceptance
- Choosing the right service provider – one that is committed to your success and not just sales
- Developing a wide ranging and often repeated communication plan
- Policy development at the same pace as the development and fielding of the technology

- Limited duplication of work between physical and logical activities - true capitalization and maximization of our investment

Winona Varnon, Principal Deputy Assistant Secretary, Office of Management
Phillip Loranger, Chief Information Security Officer and Acting Director for Information Assurance, Office of the Chief Information Officer
U.S. DEPARTMENT OF EDUCATION

12:15 p.m.

Lunch On Your Own -- But Not Alone!

Join a small group of your colleagues for lunch with an informal discussion facilitated by one of our expert speakers. Take this opportunity to join others in a small, interactive group setting to network and brainstorm solutions to your most pressing identity management concerns.

1:45 p.m.

INTERACTIVE SESSION

Panel Discussion: The IT Industry's Perspective On Identity Credentialing

Hear expert representatives from leading companies in the IT industry discuss and share their perspective on identity credentialing, including:

- Identity management standards put in place for Federal employees
- Establishing interoperability with external communities
- How their companies have incorporated those standards into their product line and strategy

Moderated By:
Tim Baldridge, Computer Scientist
NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

Panelists:
Dominic Fedronic, CTO
ACTIVIDENTITY

John Biccum, Security Strategist
MICROSOFT

John Landwehr, Director, Product Management
ADOBE SYSTEMS INCORPORATED

Tom Greco, Director, Vertical Solutions
VERIZON

2:45 p.m.

Afternoon Networking Break & Exhibits

3:00 p.m.

CASE STUDY

Program And Architectural Perspectives In The Evolution Of ICAM: A NASA Case Study Of A Post HSPD-12, Second Generation Framework

Attend this session and receive the inside story on NASA's experience with HSPD-12 compliance from the Federal ICAM Architecture Working Group's Co-Chair. You'll hear about what NASA has accomplished thus far, what they hope to do in the future, and plans to improve their efforts the second time around.

Key takeaways will include:

- Identity Life Cycle Management (Independent of Credential and Access)
- Credential Life Cycle Management (including PIV and non-PIV, with plans to accept other Agency PIV, PIV-I and other credentials)
- Access Management (provisioning and de-provisioning of access, continuous risk based access management determination)
- Access Control Enforcement (Where is the policy decision point of enforcement? Is it in or beyond the scope of ICAM?)

Tim Baldridge, Computer Scientist
NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

3:45 p.m.

CASE STUDY

Redundant Security Credentials: How Interoperability Can Reduce Costs And Improve Efficiency

Various mandates in the Patriot Act, the Maritime Transportation Security Act, and other relevant pieces of post-9/11 legislation have demonstrated that background vetting will play a significant role in the transportation of goods by air, ocean, truck and rail for the foreseeable future. Utilizing sundry legislative mandates, agencies have created a balkanized security credentialing regime—sometimes even for multiple vetting programs operated out of a single agency.

This session will focus on the various security credentialing programs in the transportation industry, the similarities between their vetting requirements, and how their lack of integration has dealt harm to the U.S. economy. Multiple credentials will be examined, but the presentation will focus upon two specific credentials issued by the Transportation Security Administration: the Hazardous Materials Endorsement for the Commercial Drivers License and the Transportation Worker Identification Credential (TWIC) and one issued by the U.S. Customs and Border Protection: the Free and Secure Trade card.

Specifically, you will learn:

- The similarities in vetting requirements and physical/machine readable zone(MRZ)/biometric qualities embedded in each credential
- Processing multiple credentials for one employee
- Opportunities to save federal funds and manpower by instituting interoperability between the various credentials

Boyd Stephenson, Manager, Security & Cross Border Operations
AMERICAN TRUCKING ASSOCIATIONS

4:30 p.m.

Chairperson's Recap:
Key Takeaways And What To Do When You Get Back To The Office

We'll recap the highlights of the past two days and ask you to share key insights and next steps with the group.

4:45 p.m.

Close Of General Sessions

ABOUT OUR CONFERENCE SUPPORTERS:

Founded in 1998 as a non-profit trade association in Washington, DC, the **International Biometric Industry Association (IBIA)** promotes using technology effectively and appropriately to determine personal identity and enhance the security, privacy, productivity, and convenience for individuals, organizations, and governments worldwide. With biometric and other identification technologies as the core focus, the IBIA brings key stakeholders together in a dialogue center for discussion, education, advocacy, and public policy. For more information, please go to http://www.ibia.org/.

Homeland Security Today, the leading monthly magazine on homeland security, looks beyond other media to reveal and analyze what is really going on behind the scenes. From top national decision-makers to first responders on the front lines, Homeland Security Today covers the entire homeland security community. Its global network of correspondents delivers original insight and analysis through its magazine, website, podcasts, videos and daily e-newsletters. Homeland Security Today is a proud recipient of multiple awards from the American Society of Business Publication Editors. Homeland Security Today is free to qualified homeland security professionals. Register for your complimentary subscription at http://www.hstoday.us/.

The BioAPI Consortium is a group of over 120 organizations that have a common interest in promoting the growth of the biometrics market through standardization. The Consortium has developed a specification for a standardized Application Programming Interface (API) that is compatible with a wide range of biometric applications programs and a broad spectrum of biometrics technologies. The BioAPI Specification was approved as an ANSI standard in 2002 and an ISO standard in 2006. The organization now focuses on promoting its adoption and disseminating information and resources. For more information, go to http://www.bioapi.org/.

VB/Research is a leading global source of research and deal intelligence on venture capital and private equity funds and their investments, M&A and the public capital markets in the Global Security and Defense sector.

By focusing on fundraisings currently marketed, acquisition targets, M&A opportunities and upcoming IPOs they deliver actionable intelligence that provides insight into tomorrow's industry leading companies. In addition, VBR's research platform offers the most accurate and comprehensive database, tracking deals and investors in all asset classes including private placements, buyouts, PIPEs, M&A and IPOs since 2002.

Members of their research service range from governments and multinational companies to investment banks, venture capitalists, private equity funds, hedge funds and law firms in over 55 countries. Venture Business

Research was founded in 2005 and employs 20 analysts and journalists in various locations around the globe.

For more information, go to: http://www.vbresearch.com/.

ContingencyToday.com and CT Review magazine (print) are dedicated to the challenges and opportunities provided by the broad spectrum of critical infrastructure protection and civilian homeland security. For more information, please go to: http://www.contingencytoday.com/.

Sign-up today for a free newsletter and receive CT Review!
Online: http://www.contingencytoday.com/subscribe-free (UK mailing addresses only)
Email: freemagazine@contingencytoday.com (outside the UK)

VENUE AND LODGING:

ALL CONFERENCE SESSIONS WILL BE HELD AT THE:

The Melrose Hotel
2430 Pennsylvania Avenue, NW
Washington, DC 20037
Phone: (202) 955-6400
Toll Free: (800) MELROSE (635-7673)
http://melrosehoteldc.com

Please contact the hotel directly when making your reservation. **For the conference, a limited number of rooms have been set aside at the government per diem rate of $229/night.** Please be sure to call the hotel no later than **Thursday, August 12, 2010** to help ensure this rate. Guests should mention the group name Identity Management for Government or group code IDEN091210. **Reservations can be made by calling 1-800-635-7673 or 202-955-6400 between the hours of 8:00AM – 6:00PM EST, Monday through Friday or online** <https://gc.synxis.com/rez.aspx?Hotel=15333&Chain=5388&group=IDEN091210> . We recommend that reservations be made early, as the number of rooms at our rate is limited.

In the heart of one of DC's most notable neighborhoods is its newest luxury, upscale hotel, The Melrose Hotel, Washington, D.C. Just one block from Georgetown and the Foggy Bottom Metro station (Blue & Orange Lines), The Melrose Hotel Washington, D.C. offers discerning business travelers and leisure visitors to the District a luxurious oasis in the heart of one of the world's fastest-paced cities. It is only 10 minutes from Reagan National Airport (DCA), 30 minutes from Washington Dulles International Airport (IAD), and 45 minutes from Baltimore Washington International Airport (BWI).

Photo courtesy of WCTC

For more information on your visit to Washington, DC, go to www.washington.org.

REGISTRATION FEES:

The following are included in your conference registration: attendance, continental breakfasts, refreshments, evening networking reception, a detailed conference workbook and any additional meeting materials - - including access to the conference wiki.

Group Discount: **Register 3 colleagues and the 4th is FREE!**	**Earlybird Pricing:** **Register with payment by July 15th**	**Regular Pricing:** **Register with payment after July 15th**
Conference Only (September 14th & 15th)	$1,299	$1,699
Conference Plus One Workshop	$1,699	$2,099
Conference Plus Two Workshops	$1,999	$2,399
Conference Workbook Only	$199.00* + $20.00 S&H	
*IL residents will be charged 9.25% sales tax on workbook orders.		

Payment is due two weeks prior to the conference. If payment has not been received two weeks before the conference, a credit-card hold, training form or purchase order will be taken to ensure your space.

SPONSORSHIP & EXHIBIT OPPORTUNITIES ARE AVAILABLE:

This conference provides an excellent opportunity to market your products and services to a targeted executive audience interested in identity management. Space is limited, so please call Amy at (773) 695-9400 x20, for more information.

TEAM DISCOUNTS: REGISTER 3 & THE 4TH IS FREE!

Four or more attendees, registering together, enjoy a savings of at least $1,299! That’s a 25% savings off each registration. Note to small departments — register together with your colleagues from another organization and receive the same group discount. The free registrant must be of equal or lesser value.

A.L.I. FREQUENT ATTENDEE DISCOUNT:

Earn conference attendance bonuses as you benchmark with other organizations. For every A.L.I. conference attended, receive a $200 discount off your next A.L.I. conference. Also, you will receive special bonuses and perks reserved only for A.L.I. frequent attendees.

PROGRAM CHANGES:

A.L.I. reserves the right to make changes in programs and speakers, or to cancel programs if enrollment criteria are not met or when conditions beyond its control prevail. Every effort will be made to contact each enrollee if a program is canceled. If a program is not held for any reason, A.L.I.'s liability is limited to the refund of the program fee only.

CANCELLATION POLICY:

You may make substitutions at any time; please notify us as soon as possible. If you cancel (in writing) more than two weeks prior to the conference (before August 30th), a $150 service fee will be charged and a credit memo will be sent reflective of that amount, which can be used for a future A.L.I. conference. Registered delegates who do not attend or who cancel two weeks prior to the conference or less (on or after August 30th) are liable for the entire fee. A credit memo will be issued which can be used for a future A.L.I. conference by anyone in your organization.

ABOUT THE ADVANCED LEARNING INSTITUTE:

The Advanced Learning Institute's mission is to help executives build strong personal relationships, expand their business knowledge of cutting-edge trends, and find proven solutions to a wide range of strategic management problems.

Our forums bring together industry leaders and experts to share valuable, real-world experiences, and best practices on how to meet tomorrow's management challenges.

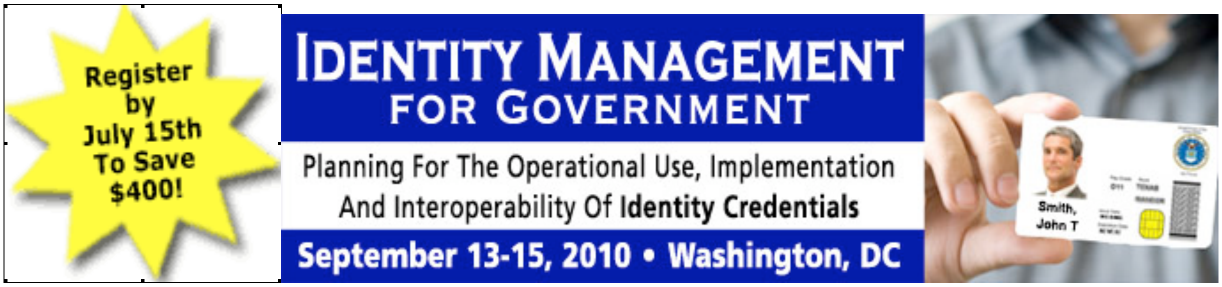
The Advanced Learning Institute's focus is on delivering high-quality programs, which consistently meet the needs of our customers. Our conferences serve a broad range of specialized industries and functions, including:

Biometrics… Information Technology… Government… Technology…
Marketing… Human Resources… Communications… Strategic Planning…
Brand Management... Performance Measurement… e-Commerce

WE GUARANTEE RESULTS:

The Advanced Learning Institute has been successfully providing senior executives with forums to share practical experiences and solutions to a variety of organizational challenges. We are so confident you'll benefit from the innovative strategies shared during this conference that we'll guarantee it! If you follow the advice of our speakers, and you don't improve efficiency valued at the cost of your registration fee, then we'll send you a full credit to be used for another event.

Thousands of satisfied alumni can't be wrong - register today for the opportunity to learn from our platform of proven experts!



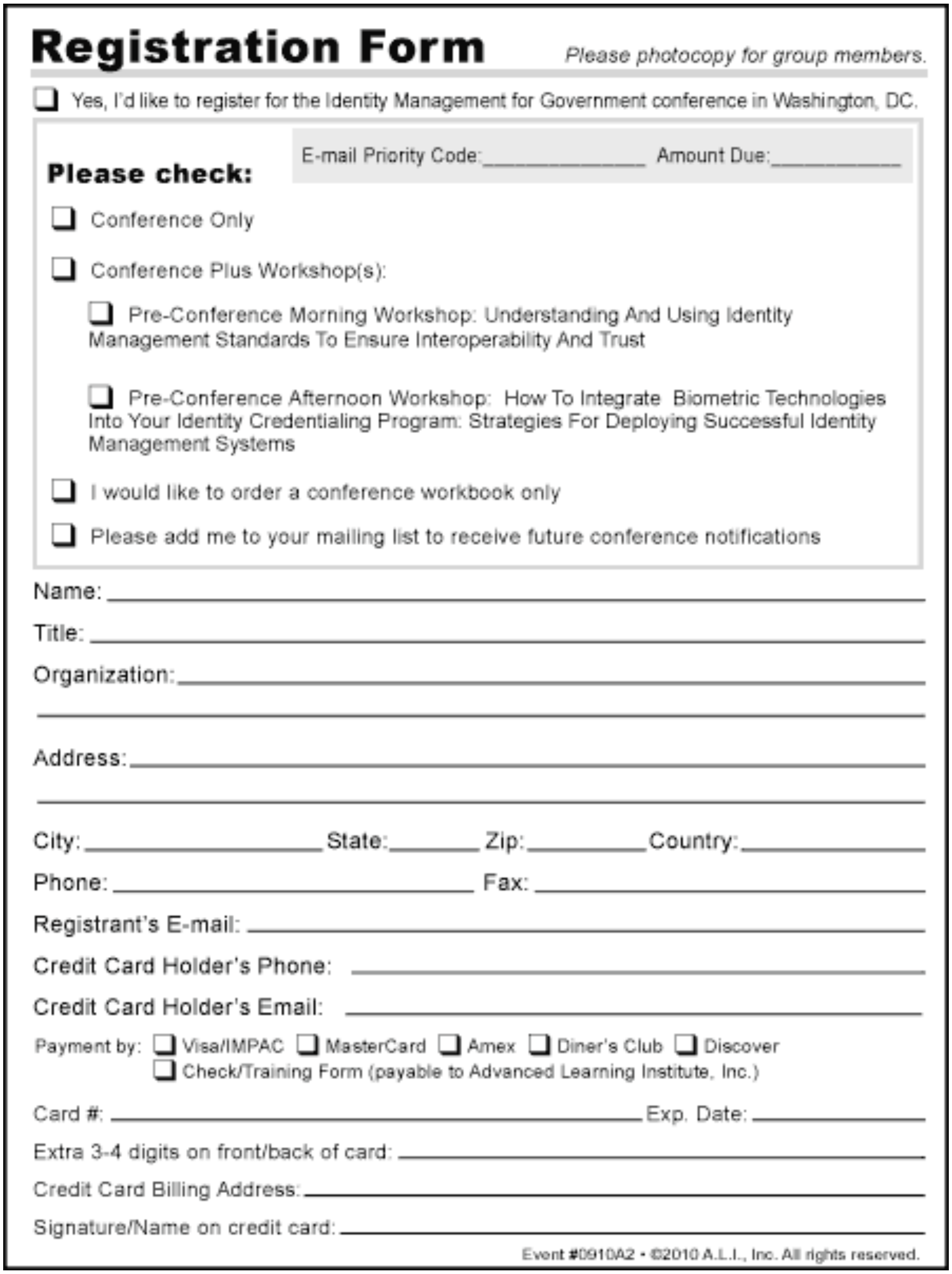
Register by July 15th To Save $400!

IDENTITY MANAGEMENT FOR GOVERNMENT

Planning For The Operational Use, Implementation And Interoperability Of **Identity Credentials**

September 13-15, 2010 • Washington, DC

REGISTER TODAY!
www.aliconferences.com
Call TOLL FREE: (888) 362-7400 • Phone: (773) 695-9400 • Fax: (773) 695-9403
Mail to: Advanced Learning Institute, 8600 W. Bryn Mawr Ave., Suite 920-N, Chicago, IL 60631



Registration Form

Please photocopy for group members.

□ Yes, I'd like to register for the Identity Management for Government conference in Washington, DC.

Please check:

E-mail Priority Code:______________ Amount Due:___________

□ Conference Only

□ Conference Plus Workshop(s):

□ Pre-Conference Morning Workshop: Understanding And Using Identity Management Standards To Ensure Interoperability And Trust

□ Pre-Conference Afternoon Workshop: How To Integrate Biometric Technologies Into Your Identity Credentialing Program: Strategies For Deploying Successful Identity Management Systems

□ I would like to order a conference workbook only

□ Please add me to your mailing list to receive future conference notifications

Name: ____

Title: ____

Organization: ______________________________________

____

Address: ____

____

City: __________________ State: ________ Zip: ________ Country: ____________

Phone: ______________________________ Fax: ______________________

Registrant's E-mail: ________________________________

Credit Card Holder's Phone: __________________________

Credit Card Holder's Email: __________________________

Payment by: □ Visa/IMPAC □ MasterCard □ Amex □ Diner's Club □ Discover
□ Check/Training Form (payable to Advanced Learning Institute, Inc.)

Card #: ______________________________ Exp. Date: ____________

Extra 3-4 digits on front/back of card: ____________________

Credit Card Billing Address: ______________________________

Signature/Name on credit card: ____________________________

Event #0910A2 • ©2010 A.L.I., Inc. All rights reserved.