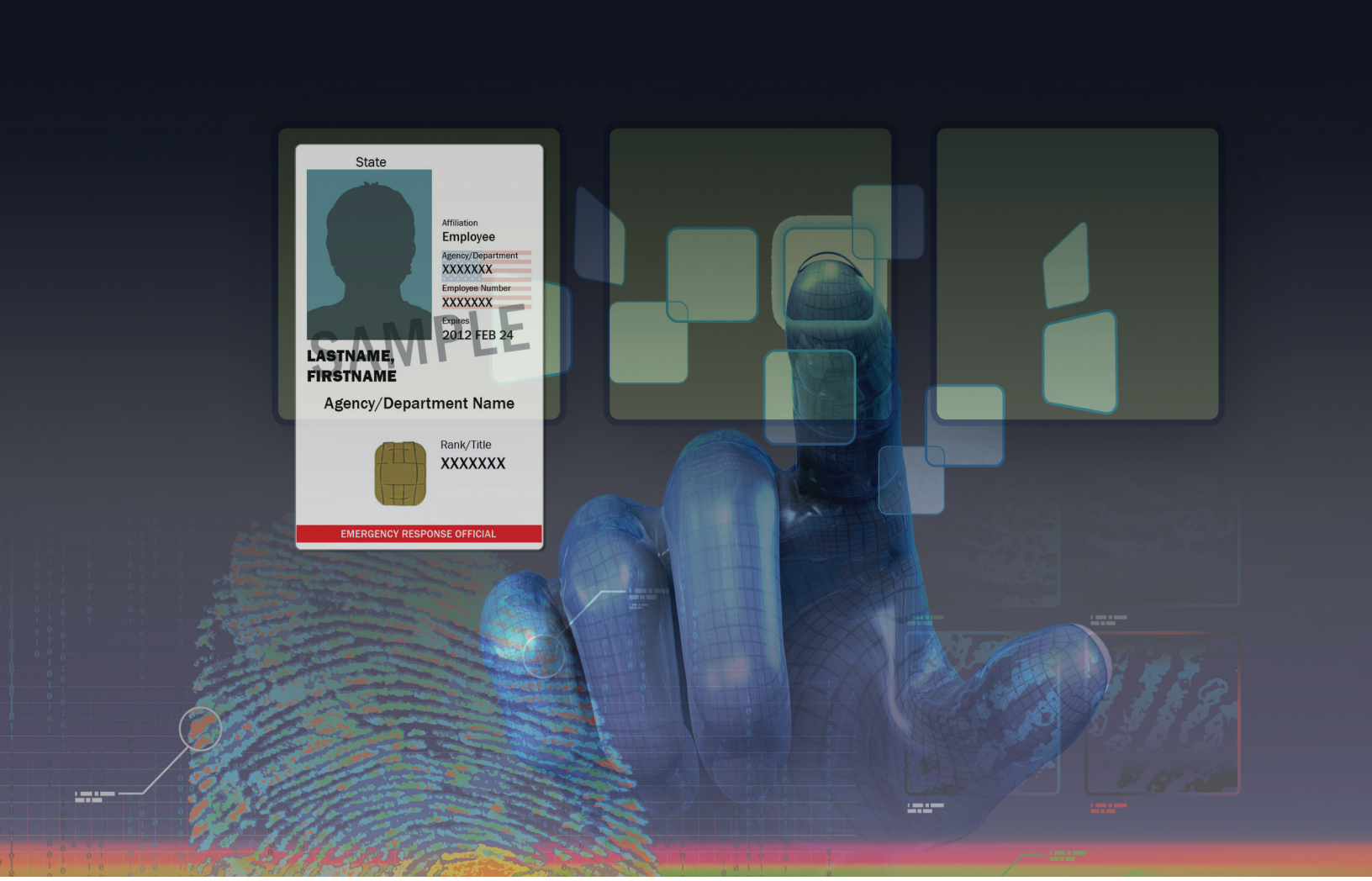



# Moving Towards Credentialing Interoperability

## Case Studies at the State, Local, and Regional Levels

*July 2010*

Homeland Security

# Contents

I. Introduction . . . . . 1

Document Source. 2.

II. Background . . . . . 3

Credentialing and Identity Management Challenges. 3.

Credentialing Solutions. 5.

III. Proven Practices from the PIV-I/FRAC TTWG . . . . . 7

IV. Credentialing Case Studies . . . . . 9

**Southwest Texas:** Too Many Cards in the Deck 9.

**FRAC in the Commonwealth of Virginia:**
One Card for Access at the State and Federal Level 13.

**Comprehensive Training and Skills Attributes in Chester County, PA:**
Empowering Incident Commanders to Make Better Decisions 15.

**Colorado First Responder Authentication Credential Program (COFRAC):**
One State, One Card 18.

**District of Columbia One Card (DC1C) in the District of Columbia:**
Even without SmarTrip, the DC1C Opens More than Just Doors 21.

**West Virginia FRAC:** Wild, Wonderful, and Secure 23.

**Hawaii Emergency Response Official Credentialing Program in Honolulu, Hawaii:**
Trusted Credentials through "H/ERO's" Work 26.

V. Glossary . . . . . 29

# I. Introduction

**The objective of this document is to provide information to non-Federal organizations and their decision makers about the value of strong credentialing practices using Federal standards. Credentialing is a system by which identification cards or other tokens are used to authenticate a person and transmit skills, qualifications, and other attributes associated with that identity. Interoperability, in the credentialing context, provides the capability for a jurisdiction to access information and trust its legitimacy in order to make decisions about granting access and privileges.**

This document also examines the experiences of several non-Federal agencies that have implemented interoperable credentials that leverage the Federal credentialing system. Through a series of case studies, it provides practical solutions, best practices, and lessons learned to assist decision makers in developing credentialing systems in their own jurisdictions. This document serves as an introduction to electronic identity/attribute management and credentialing for those whose purview is emergency management.

Presented within the document are seven case studies on identity/attribute management and credentialing within the emergency response community. Six of the case studies involve state, local, or regional government-led credentialing programs, and one case study documents a hospital system's credentialing program.

The seven case study jurisdictions include:

- The Southwest Texas Regional Advisory Council (STRAC) – San Antonio, Texas
- The Commonwealth of Virginia
- Chester County, Pennsylvania
- The State of Colorado
- The District of Columbia (Washington, D.C.)
- West Virginia, Eastern Panhandle Homeland Security Region 3
- Honolulu, Hawaii

## Document Source

The Command, Control and Interoperability (CCI) Division within the Science and Technology (S&T) Directorate of the U.S. Department of Homeland Security (DHS), the Federal Emergency Management Agency (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 convene the Personal Identity Verification-Interoperable (PIV-I)/First Responder Authentication Credential (FRAC) Technology Transition Working Group (TTWG). The TTWG comprises state, local, and regional emergency management representatives, many of whom have already implemented innovative and secure identity/attribute management solutions in their own jurisdictions.

The mission of the PIV-I/FRAC TTWG is to increase the adoption of interoperable credentials across jurisdictional lines within the emergency response community. The group is working to elevate credentialing from a stove-piped, organization-centric effort to a standardized, interoperable effort. The ultimate goal is to help achieve national credentialing interoperability and trust.

This document incorporates insight from members of the PIV-I/FRAC TTWG and other stakeholders regarding successful state, local, and regional and non-government identity/attribute management projects. This information was obtained through submitted questionnaires, telephone interviews, and PIV-I/FRAC TTWG facilitated meetings. The case studies included in this document do not necessarily reflect the opinions, views, or policies of the U.S. Department of Homeland Security; the Science and Technology Directorate; CCI; nor the U.S. Government.

# II. Background

**How do you really know if they are who they claim to be? While this question may seem simple, people take for granted the subtle and instinctive ways that they identify people. In person, appearance and audio cues are used. Technology has allowed people to increasingly interact with one another remotely, and to rely on various means of identification—such as caller ID, the sound of a voice, passwords, shared knowledge, or a name on a computer screen. These methods rely on familiarity.**

Identity gets more complicated when unfamiliar people interact. In these situations, social cues or context may help determine whether people are who they say they are. Sometimes people accept someone's identity because a trusted acquaintance vouches for them. In other cases, identity is confirmed through visual inspection of common credentials such as driver's licenses.

Emergency responders such as police officers and firefighters deal with sensitive and dangerous situations and people everyday. Regular encounters with these types of situations enable responders to understand the importance of identity more than the average citizen. Responders' personal safety and the safety of the public may hinge on being able to make informed decisions about the people with whom they interact in the course of their duties. Responders must be sure that the people they are partnering with are who they say they are and are qualified to do what they claim. In this community, absolute confirmation of someone's identity and skill sets (attributes) can mean the difference between life and death.

## Credentialing and Identity Management Challenges

It is easy to take identity for granted within a community of trust. For example, police officers within one jurisdiction work together everyday and recognize the sound of each other's voices over the radio. Their cruisers' emblems are familiar, their uniforms match, and their credentials look the same. However, identity challenges occur when the scale of an incident increases and responders must coordinate across jurisdictions and levels of government. Practices for recognizing identity based on familiarity can break down as responders from other jurisdictions arrive at the scene of the incident.

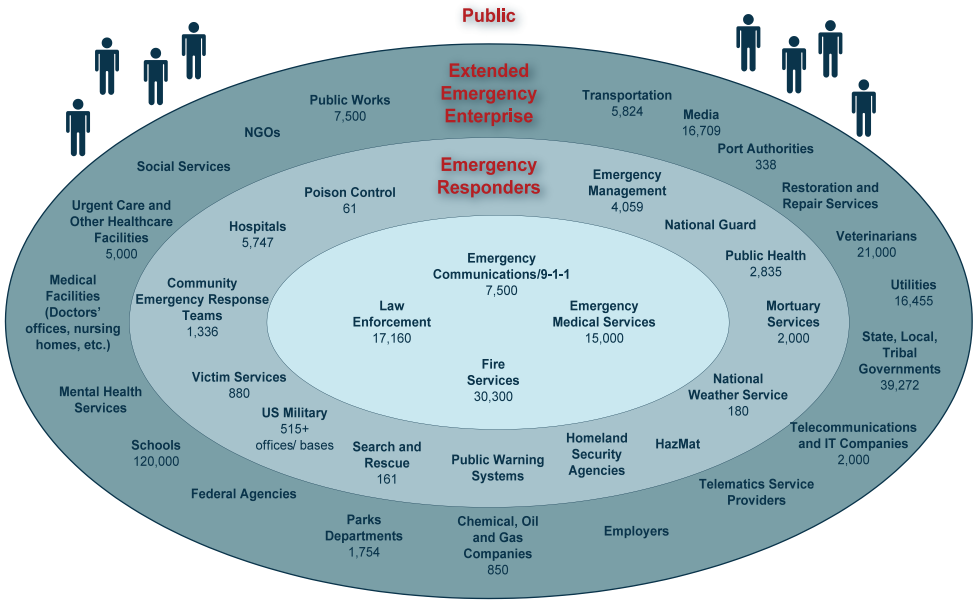
Figure 1 illustrates the concentric circles of emergency response. While small emergencies require only local emergency responders in the innermost circle, larger emergencies require the coordination of multiple stakeholders who do not deal with one another on a daily basis. Emergency responders from one entity may be equipped with credentials that vary widely from those issued by another entity. The

credentials may look different; possess different identity proofing and background checking procedures; and offer varying degrees of counterfeit protection.

- How does one responder know that the other's credentials are valid?
- To what degree can he or she trust and understand the credentials shown by a fellow responder?

Incident Commanders (ICs) and Law Enforcement Officials (LEOs) are acutely aware that most emergency responder credentials lack interoperability across jurisdictions. ICs and LEOs need to make rapid decisions about which emergency responders should be allowed to support response activities to an incident and who should be kept out. While they may know their own firefighters, police officers, and Emergency Medical Technicians (EMTs), multi-jurisdictional deployments require the ICs and LEOs to make decisions about personnel with whom they do not have familiarity in terms of skills and training. Especially in the case of a terrorist attack, ICs must have confidence in the identity of the responding officials.

***Incident Commanders must have confidence in the identity of the responding officials.***




NOTE: Numbers reflect the numbers of entities in the group and all associated offices.

*Figure 1: Emergency Response Stakeholders (Source: COMCARE, 2007)*

Another identity/attribute management and credentialing challenge is controlling physical access to buildings, parking garages, and other locations. Building owners want to enable authorized individuals to enter safely and seamlessly while preventing unauthorized access. Although most buildings require site-specific credentials for entry, the ideal situation would include personnel with credentials issued by other trusted organizations.

Coordinating multiple independent identity/attribute management efforts is a burden for end users, and a challenge for managing identities. For example, emergency responders often carry many credentials, in addition to maintaining dozens of usernames and passwords required for access to applications and Web sites. There are significant and redundant organizational costs and security risks associated with each of these identities, including the costs of maintaining the databases, time spent provisioning users with forgotten passwords, and the time users spend changing and entering passwords.

## Credentialing Solutions

Standardized, secure, interoperable, and trusted credentialing practices can have a tremendous positive impact on multi-jurisdictional response/recovery efforts nationwide. These practices allow an IC or LEO to quickly, securely, and confidently determine:

- Identity – Is the emergency responder the person he or she claims to be?
- Attributes (e.g., knowledge, skills, abilities, training, deployment authorizations) – Is the emergency responder qualified to conduct the needed emergency support functions?

The Executive Branch of the Federal Government is investing considerable resources and labor to establish an interoperable credentialing system for Federal employees and contractors to ensure that government facilities and networks remain protected. Under Homeland Security Presidential Directive 12 (HSPD-12), access to all Federal buildings and computer systems will require secure forms of identification based on smart card technology and identity-proofing procedures. Smart cards are replacing pre-existing Federal credentials and enabling the electronic verification capability that can confirm whether or not a presenter's identity and access privileges are valid and current. These smart cards are known as Personal Identity Verification (PIV) credentials. Federal Information Processing Standard (FIPS) 201 defines the technical specifications for PIV.

Ultimately, Federal employees and contractors will be able to use their PIV credentials to gain access to not only their home agency's physical and logical (i.e., computer-based) infrastructures, but potentially to those of other agencies within the Federal Government. For physical access, a building guard uses an electronic reader to access information on the card and checks it against a database to determine who the person is and whether or not he or she has the proper clearance to enter the building. For logical access, hardware scans the same card to determine whether the person is allowed on a government network, and, ideally, what files and applications the holder can access.

The Federal Chief Information Officer (CIO) Council created the PIV-I Credential for Non-Federal Issuers for those who need to provide identity credentials in a trusted and interoperable manner. The trust and interoperability of a PIV-I Credential is based upon common and consistent standards that have been defined for:

- Determining the proof of identity of a person who needs the credential
- Determining how the issuers of credentials are certified
- Defining how the credentials should be implemented from a technical perspective such that they are usable across jurisdictions

Federal guidance on personnel credentialing can serve as a common blueprint that state, local, and regional creden-

tialing authorities can use to implement an interoperable credentialing system in their area. The PIV-I guidance provides the technical specifications that meet the PIV technical specifications as defined by FIPS 201. An identity credential that meets these guidelines will be interoperable with and trusted by the Federal Government and any partnering jurisdictions. PIV-I credentials have many advantages, including the following:

- **Interoperability across jurisdictions** – Because PIV-I is a national standard, participating state, local, and regional jurisdictions will be interoperable with each other and with the Federal Government.
- **Trust across jurisdictions and levels of government** – Just as an individual sometimes chooses to extend trust to a "friend of a friend," one organization can choose to trust the PIV-I credential of an individual who was issued that credential by a trusted organization.
- **Strong proof of identity** – By following applicant identity proofing procedures as specified by PIV-I guidance, organizations can trust PIV-I credentials issued by other organizations.
- **Ability to electronically authenticate an individual's identity and attributes** – Instead of merely visually inspecting a credential, decision makers can use electronic credential reader devices and/or Physical Access Control Systems (PACS) to rapidly and accurately validate someone's identity and attributes. Electronic validation of attributes can include emergency support function, scope of practice, and level of clearance.
- **Physical access to Federal buildings** – Federal security officers can make authorization and access decisions based on an individual's PIV-I credential presented at an entry point.
- **Logical access to Federal computer systems** – Federal online application owners may configure their applications to be selectively available to non-Federal individuals, based on information electronically retrieved from their PIV-I credentials. This capability requires a computer with a smart card insertion slot or a smart card reader. Conformance with the PIV-I standard will enable non-Federal issuers to provide a credential that provides proof of identity with the highest possible level of assurance (Level 4) as described fully by the Office of Management and Budget Memorandum M-04-04.

These standards combine to provide organizations with the ability to accept the credentials of visitors so their jurisdiction can be assured that the visitor's credential was issued in the same manner as their own (if they are also PIV-I issuers) and that the same level of confidence in the identity of the credential holder can be extended to the visitor. This in turn eases the burden (both financial and procedural) of establishing bi-lateral trust mechanisms with other jurisdictions.

While state, local, regional, public, and private credential issuers may choose to issue other types of credentials, PIV-I is the only credentialing standard endorsed at level 4 by the Federal Government to ensure interoperability and a high level of trust among participants. With the support and collaboration of partners from different levels of government, PIV-I will result in our Nation adopting better identity/attribute management and credentialing practices. This document addresses many of the challenges surrounding PIV-I issuance and provides guidance on how state, local, and regional governments can be interoperable with Federal Government identity management practices.

# III. Proven Practices from the PIV-I/FRAC TTWG

**More than a dozen state, local, and regional jurisdictions participate in the PIV-I/FRAC TTWG and are working toward issuing PIV-I credentials. While these participating members are at different stages in fully achieving the PIV-I standard, they are considered the "early adopters" of a national identity credentialing standard. Their collaboration and lessons learned will benefit other agencies that choose to adopt the PIV-I standard.**

While a full analysis of the seven credentialing case studies is presented in Section IV, below are key themes from across all case studies. These lessons learned focus on the processes surrounding the implementation of a credentialing program rather than the procedures for actually distributing the credentials to individuals. The themes below are intended to serve as guidance to other potential PIV-I credential issuers from the members of the PIV-I/FRAC TTWG based on their collective experiences.

## Participant Adoption and Usage

- A credentialing solution must show value for the participating agencies.
  - It is necessary to garner executive sponsorship and endorsement.
  - Cost savings, enhanced response and recovery efforts, security, and risk mitigation.
- A standardized credentialing solution must show value for the end users.
  - Widespread adoption is more likely if end users perceive that the solution:
    - Meets their needs.
    - Enhances their capabilities.
    - Is a useful tool that can be used to effectively address specific common access control issues.
  - One measure of the success of a PIV-I deployment is the level of end-user adoption (e.g. usage is embedded into the culture and work environment).
- Credentials should provide the ability to access multiple resources, which allows them to be used every day, on a routine basis:
  - This provides the opportunity to consolidate credentials and reduce the number of credentials a person must carry.
  - It enables agencies to validate against, streamline, and consolidate legacy identity databases.
  - Agencies that have already issued credentials must agree to migrate to the new credential.
  - If individuals use the credential every day for routine purposes, they will have it at all times—including when an unexpected emergency occurs.

## Governance and Coordination

- A governance structure with representation from all participating organizations or jurisdictions allows stakeholders and decisions makers to address challenges efficiently and gain consensus.
- Identify key stakeholders (see Figure 1 on page 4), including:
  - Critical Infrastructure and Key Resources (CIKR)
    - There are 18 CIKR sectors within the National Infrastructure Protection Plan (NIPP).

- Public-private partnerships
  - Non-Governmental Organizations (NGOs), faith-based, recovery mode, retail, community-related.
- Industry organizations (e.g., bankers associations, trade associations, chambers of commerce, large contractors).
- Public-public partnerships (e.g., counties, cities, agency chiefs' organizations, regional councils of government, interstate/regional partnerships).

- Employing a federated model helps with buy-in.

## Standards

- The standard is PIV-I.
  - Provides a common specification for an interoperable identity credential
  - The credential is issued in a trusted manner
  - Interoperable and trusted across domain boundaries
- Attribute management – PIV-I in combination with an Attribute Management capability enables a decision-maker to determine a responder's roles, skills, qualifications, and licensures.
- An identity credential that meets the PIV technical specification (FIPS 201).
- Initial adherence to PIV-I specifications avoids the additional work that would be required later to integrate new organizations into the framework.
  - Alignment with PIV-I specifications should be the defined end-state
  - Alignment with the standards may make buy-in more difficult from organizations that have already invested in legacy systems

## Funding

- Complete a cost-benefit analysis.
  - This essential step can enable cost savings and enhanced risk mitigation.
- Develop a sustainment strategy at the beginning.
  - Grant funding is helpful to initiate the effort, but sustainability comes from demonstrating business value to participating agencies and end users.
- Work to influence DHS Grants & Training to establish FIPS 201-dependent grants.
- Identify opportunities to leverage interest from the private sector.
- Join with other jurisdictions to achieve economies of scale:
  - For smart card implementation/sustainment procurements.
  - For "group" credential issuance by forming a PIV-I Managed Service Office (MSO).

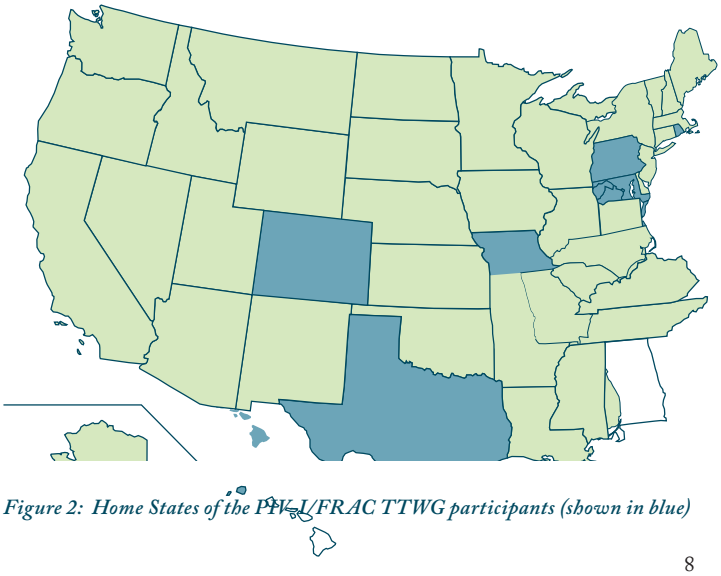


*Figure 2: Home States of the PIV-I/FRAC TTWG participants (shown in blue)*

# IV. Credentialing Case Studies

**Below are seven case studies of non-Federal entities implementing PIV-I based credentialing solutions in their jurisdictions. Several of the projects are still in the pilot phase, and most have not reached the stage of issuing PIV-I credentials, although each of the leaders of the projects understands the value in working towards the Federal standard of PIV-I credentials. While some of them are exemplary, the purpose in telling these stories is mainly to enable visibility into the work that others have already accomplished so that future states, localities, and regions issuing credentials can consider those lessons learned. For more information about any of the case studies, please contact FEMA-FRACSupport@dhs.gov.**

## **Southwest Texas:** Too Many Cards in the Deck

### Background

Controlling access is a big concern for hospitals. Busy, open-access facilities can increase health risks to patients. Hospitals focus on ensuring that the right medical personnel are in the right areas, delivering the right medical care to the right patients. Keypads are placed next to emergency room doors to control entry, and computer systems used for medical record-keeping require usernames and frequent password changes. The Joint Commission, a national health care accreditation body, requires hospitals to issue identification credentials to all doctors.

While these security precautions are necessary, they are a nuisance to doctors and other hospital staff. Doctors and other hospital staff serving in the Texas Trauma Service Area – P (TSA-P), a group of hospitals located in the greater San Antonio/Southwest Texas region, previously carried six or more identification credentials for various purposes, from accessing parking garages and staff lounges to entering trauma units. Additionally, they needed to remember multiple usernames and passwords for the different computer systems that they logged onto at each hospital.

Like many regions around the country, hospitals in San Antonio evaluated their security protocols and found several opportunities for improvement. For example, the emergency room access keypad had wear and tear from Emergency Medical Services (EMS) personnel entering the same code over and over, which made the code apparent to any observant intruder. Emergency "lockdown" situations pose a particular problem, as hospital leadership and local emergency management need to ensure that appropriate doctors and hospital staff have authorized access to the facilities but prohibit unauthorized access as well.

## Solution and Implementation Approach

The Southwest Texas Regional Advisory Council (STRAC) is responsible for design and implementation of the regional Trauma/Emergency Healthcare System in TSA-P, including disaster response. STRAC is a 501(c)(3) non-profit, tax-exempt organization that has affiliation with 53 hospitals and 70 EMS agencies in the region. It facilitates and helps broker agreements among the hospitals in the area.

STRAC evaluated the need for better identity and access management controls to help solve the security concerns for their hospitals. STRAC is the designated agency for the Hospital Preparedness Funding from the U.S. Department of Health and Human Services' (HHS) Health Resources and Services Administration (HRSA) and Office of the Assistant Secretary for Preparedness and Response (ASPR). This funding is designed to make hospitals more prepared for homeland security and disaster response/recovery.

With the ASPR Hospital Preparedness Program (HPP) funds, STRAC started building a system to replace the complex web of credentials, usernames, and passwords. Unlike other credentialing programs around the country, STRAC chose to build its solution in-house rather than hiring a third-party integrator. This approach took into account the high cost associated with large national contractors. As a result, STRAC was able to leverage in-house subject matter expertise and information technology (IT) capabilities that other regions did not have.

The initial "STRAC-ID" credential provided a convenient single card that gives doctors, paramedics, and other hospital staff access to all participating hospitals, including parking garages, lounges, and secure areas. Approximately 12,000 STRAC-ID credentials have been distributed to date, including:

- 4,000 to hospital-based doctors.
- 7,000 to paramedics and firefighters who regularly need access to hospitals.
- 1,000 to mid-level responders.

Since 2008, STRAC has been migrating from the original card that was integrated to all the hospitals' PACS, to a more robust "smart card" using FIPS 201 standards to guide the implementation. The resulting STRAC-ID "smart card" will not only provide the backwards compatibility for PACS access, but also computer login procedures that use FIPS 201 processes. Secure electronic capability is critical because as healthcare systems migrate to include more and more electronic health records, they need to be carefully protected. FIPS 201-standardized credentials provide the needed high level of identity assurance and trust.

The cost to produce each PIV-I STRAC-ID smart card is roughly $25-$30. As more hospitals adopt the new system, other hospital regions are following suit. Hospitals sponsor their staff and STRAC issues them STRAC-IDs based on specific business rules. This standardized process ensures that all stakeholders trust the credentials, the asserted identity of the individual is correct, and the system is credible. In all of this, STRAC plays a critical coordination role among the disparate healthcare systems.

## Benefits

- The STRAC-ID credential system is comprised of a single system in which all 35 acute care hospitals within STRAC agreed to participate.
- The second version of the STRAC-ID credential is PIV-I.
  - These credentials contain the individuals' identity and physical access information only for those hospitals with which they have affiliations. The credential will not work in hospitals where the indivdual is not affiliated, based on the their need for access.
  - The credential still has backward functionality through its barcode and magnetic stripe. This allows previous access control systems to be migrated to FIPS 201 readers using a phased approach. The credential will perform with both legacy and FIPS 201 architectures in a manner transparent to the credential holder.
- The single STRAC-ID credential replaces the need to carry multiple credentials.
  - Authorized personnel are allowed quick access to secure yet frequently accessed areas such as emergency rooms.
- The credentials enhance accountability (e.g., in the event of a large-scale disaster) through physical access control and Personnel Accountability Systems.
- The system's Web-based portal allows new individuals to be added or removed to the PACS by affiliation. This process is controlled exclusively by the building/ PACS owner, not STRAC.

***Authorized personnel are allowed quick access to secure yet frequently accessed areas such as emergency rooms.***

## Factors Contributing to Success

- A governance structure through STRAC has allowed the stakeholder decision makers to address challenges (e.g., technical and political hurdles) with hospitals and the vendor community.
- Gaining buy-in and implementation support through conversations with emergency management personnel and hospital CIOs was essential.
  - Initially, when doctors and hospitals were asked about the likelihood of adopting this type of system, each group felt that the other would not be interested, but buy-in from both groups was achieved through mediated communication by STRAC and the demonstration of a sustainable business model.
- STRAC established the STRAC-ID credential as the parking pass for hospital staff to ensure that it would be used everyday. This routine functionality was crucial because the STRAC-ID will most likely be with an individual whenever they are reporting for duty regardless of the time of response or location.

## Lessons Learned

- Financial value should be demonstrated to decision-makers.
- Benefits should be demonstrated to end users.
  - Doctors and other staff who work at multiple hospitals only need to remember one password for access to multiple hospital data systems.
  - More secure access to facilities while increasing physical access control and decreasing the number of access cards being carried by doctors and hospital staff.
  - The greater the number of hospitals that can be accessed through a single credential, the more likely it would be carried.
- Value should be demonstrated to the emergency response community.
  - Hospitals are much safer during "lockdown" situations.
- By building the system themselves, rather than relying on the vendor community, STRAC created a more affordable and sustainable system that still met their requirements and FIPS 201 standards.
  - The solution would have been cost prohibitive if STRAC had used a private sector vendor.
- Pay attention to tipping point effects.
  - Once several hospitals participated, the others followed suit.
- Meet two requirements through a single solution.
  - Satisfied a public safety need and a commercial need.

## Next Steps

- Complete the implementation of the Logical Access Control System (LACS) deployment for secure computer access in hospitals.
- Deploy the STRAC-ID credential to public safety command and specialty team personnel.
- Deploy the STRAC-ID credential to other healthcare and civilian personnel.

# FRAC in the Commonwealth of Virginia:
## One Card for Access at the State and Federal Level

## Background

Working in the National Capital Region (NCR) requires interoperability across multiple jurisdictions to enable emergency responders to successfully fulfill their jobs. The majority of emergency responders already have some form of identification cards; however those ID cards often vary by discipline or specialty and may not be uniformly recognized across all levels of government or by different jurisdictions. Because the Commonwealth of Virginia did not have an identity/attribute management and authentication process with standards-based credentialing and issuance protocol, they were vulnerable to interoperability challenges in the NCR.

In the past, incident commanders had to assume that people were who they said they were, or may have had to deny access until it was possible to validate their identity and/or attributes. As a result of the additional time needed to authenticate unknown cards, these significant delays could prevent doctors and nurses from accessing incident scenes for extended periods of time.

***Virginia embraced HSPD-12/FIPS 201 as the credentialing standard for emergency responders and coordinated with DHS and the NCR to develop and implement FIPS 201 as part of its Emergency Response Initiative.***

## Solution and Implementation Approach

Beginning in 2005, Virginia allocated a portion of its Urban Area Security Initiative (UASI) grant funding to fund a pilot implementation of the First Responder Authentication Credentialing (FRAC) Program, which meets the PIV-I standard. The program, lead by the Governor's Office of Commonwealth Preparedness (OCP), primarily focused on providing credentials to jurisdictions responsible for incident response to Federal Government facilities, such as the Pentagon. The Commonwealth issued more than 2,400 FRACs to Arlington County and the City of Alexandria, which are due to expire by March 2010—when the pilot is concluded. Since 2005, Virginia has funded the program with State Homeland Security Grants.

Virginia embraced HSPD-12/FIPS 201 as the credentialing standard for emergency responders (e.g., state, local, Federal, private, and volunteer groups) and coordinated with DHS and the NCR to develop and implement FIPS 201 as part of its Emergency Response Initiative. FRAC holders still retained their legacy access cards and systems because the FRAC, at the time, was only a pilot program.

## Benefits

- Increases cooperation between local, state, Federal, private, and volunteer sector emergency responders before and during a critical incident.
- Meets the control, identity proofing, registration, and technical objectives of HSPD-12 and FIPS 201/PIV-I as allowed by a non-Federal entity.
- Allows emergency responders to have authorized physical access to identified critical incident areas.
- Accurately and efficiently identifies a person's qualifications and status within his or her respective agency or organization.

## Factors Leading to Success

- Marketing materials on the FRAC program and FIPS 201/PIV-I standard helped educate credential holders.
- Buy-in was gained though meetings with local emergency managers on FIPS 201 and the FRAC.
- Funding was provided through grants and was therefore not a financial burden on the localities.
- Localities sponsored and scheduled appointments for the applicants.
- The FRAC program was influenced by both top-down and bottom-up approaches, as well as stakeholder outreach methods used to gain input and consensus. The program was shaped by Executive Order 44 (Establishing Preparedness Initiatives in State Government), lessons learned from natural and man-made disasters, and working groups in the public sector.

## Lessons Learned

- FIPS 201 standards, especially for non-Federal entities, were still being developed while the project was ongoing and resulted in additional changes.
- The FRAC was not integrated with existing access points and was not used everyday.
- Regional mobile credential readers provide for more optimal usage.
- Performance of registration and issuance processes by localities would provide FRAC holders with more ownership of the program.

## Next Steps

- Perform additional planning around the actual use of the credential, with specific attention paid to the possibility of reducing the number of credentials that an individual would carry.
- Identify funding for program sustainability efforts and FRAC reissuance after March 2010.

# Comprehensive Training and Skills Attributes in Chester County, PA: Empowering Incident Commanders to Make Better Decisions

## Background

Incident commanders frequently confront challenges that make it difficult to make informed decisions about resource allocation in mutual aid situations. This is partially due to the diversity of titles, training curriculum, and resource roles across political jurisdictions in the United States. Each jurisdiction designs its emergency responder training curriculum to meet the needs of its population. For example, an EMT from Pennsylvania may have completed different training than an EMT from New Jersey.

*Incident commanders are faced with allocating resources with different training programs, types, and titles across jurisdictions. They have to quickly make decisions that are based upon currently available resource information.*

As a result, incident commanders are faced with allocating resources with different training programs, types, and titles across jurisdictions. They have to quickly make decisions that are based upon currently available resource information. Chester County, Pennsylvania, needed a way to help incident commanders make informed decisions and also provide them with an easy method to compare curriculums, protocols, and scopes of responsibility, and to identify the differences to those requesting mutual aid.

Chester County's solution, the "Comprehensive Training and Skills Attributes System," allows for input regarding various training curriculums, protocols, and scopes of responsibility. This provides the on-scene incident commander, other command and control entities, and multi-agency coordinating entities with a comprehensive identification of the differences between their jurisdiction and others. The system enables incident commanders to make informed decisions regarding the allocation of mutual aid.

## Solution and Implementation Approach

Chester County's credentialing effort began in May 2006, and focused on the following disciplines: fire, police, EMS, emergency management, 911 call centers, and public works officials. The credential system provides incident commanders with an accurate understanding of the training completed by emergency responders, with the added benefit of reducing the number of access cards that responders carry to a single credential. The program was funded by various sources, including three-year performance grants from the U.S. Department of Justice Community Oriented Policing Services technology grants and DHS State Homeland Security grants.

Unable to force state-level (top-down) standardization of training and certification, Chester County accepted the fact that different jurisdictions would continue to have different training curriculums and position titles. As a result, the county compared and contrasted its training

curriculum and those of the surrounding jurisdictions. This process enabled Chester County to understand how its emergency responder skills and titles corresponded with those of their counterparts in the surrounding jurisdictions.

An individual's information would be stored on a single access PIV-I credential, and would reduce the number of credentials that the user would normally carry. By linking programs and information that the user would access on a normal basis—such as the Justice Network (JNET) and the Law Enforcement Justice Information Sharing Project (LEJIS) systems in the law enforcement community—the user would be more likely to keep this credential on his/her person at all times.

## Benefits

- Incident commanders are now able to almost instantly assess the level of training and scope of practice of the emergency responders arriving at the scene. The commanders can decide whether or not the mutual aid they received on the scene is adequate for their needs. The PIV-I credential reader electronically reads the responders' attribute dataset and presents the information to the user in local terminology.
  - An instant comparison can be made between the individual's knowledge and task statements and the receiving jurisdiction's requirements, thus identifying critical discrepancies. Examples:
    - After analyzing the table of pharmacology for Paramedics in Pennsylvania, it was determined that a Paramedic on a helicopter received the necessary training and was given the legal ability to administer medication to perform Rapid Sequence Intubation (RSI) as part of the scope of care. A paramedic on a ground unit could not have delivered that degree of care.
    - Jurisdictions with firefighters who are trained only within their own department and not by the state may not be certified to enter a burning structure, unlike jurisdictions that mandate firefighters complete state-sponsored training.

## Factors Leading to Success

- All potential uses and standards were developed in the early stages of the program, and this helped obtain buy-in from the many stakeholders who would use the credential.
  - Interoperability is an important aspect to leverage buy-in. This is only achieved by adhering to the same standards.
  - The best standard to use, which ensures interoperability with not only surrounding jurisdictions but also the Federal Government and the Department of Defense, is the PIV-I standard including equipment from the U.S. General Services Administration (GSA) FIPS 201 Approved Products List (APL).
    - Ask vendors to see their Certification & Accreditation (C&A) Report.
    - Ask vendors to provide the certification information from the APL (proof that they have passed the National Institute of Standards and Technology [NIST] Test Tool for compliance).
    - Visit www.idmanagement.gov to determine whether a vendor/Public Key Infrastructure (PKI) provider is on the approved PIV-I list. Do not rely on vendor "assurances."
    - Ask for help and guidance until you clearly understand the process.
- To replace existing access credentials, certain aspects of legacy credentials had to be incorporated into the solution.
  - The Commonwealth of Pennsylvania issues credentials with information contained in barcodes, so the PIV-I credentials also contained barcodes to interoperate with the state system.
- A credential issuance process was designed to make it easy for recipients to receive their credentials.
  - The applicants' training and certification information was collected within their own

agencies and submitted into the system prior to credential issuance.

  - Credential-issuing kiosks were set up in multiple locations and kept open for several time allotments, giving individuals ample opportunity to receive a credential.

- Because many emergency responders are volunteers, issuing them a recognizable, government-issued PIV-I credential provides a valuable sense of belonging within a larger community.

- Program sustainability comes from widespread use, which results when end users consider the program to have high value.

  - Individuals use the credentials for many everyday purposes and see them as a part of their job.
  - Widespread use reinforces the need for the system and provides increased confidence that the initiative will continue through state-allocated funding if grant funding diminished.
  - Implementation should include everyday emergency uses, such as an on-scene accountability system.

## Lessons Learned

- Educating jurisdictions on how their information will be used and how sharing it will benefit them is essential to expedite collection of personal information.

  - Organizations are hesitant to give up their information without completely understanding the purpose and benefits of sharing it.

- Changing requirements and standards in the midst of solution development can cause the project to change direction.

## Next Steps

- Distribute additional credentials and continue incorporating surrounding jurisdictions, both inside and outside Pennsylvania.

- Continue collecting training curriculums, especially from agencies that have been unwilling to submit to date.

- Use the credentials to enable logical access to electronic information sharing systems.

- Develop electronic links between the certification agencies and entities and their systems.

  - A newly trained or recently transferred individual could have his/her training information automatically entered into the system from the training agent or previous jurisdiction.

# Colorado First Responder Authentication Credential Program (COFRAC): One State, One Card

## Background

Emergency responders need to move and communicate easily across multiple jurisdictions in the event of a terrorist or other all-hazards incident. Too many agencies within the State of Colorado were branching out and developing their own credentialing processes, which resulted in stove-piped information and redundant, inefficient processes. Prior to the establishment of the FIPS 201 standard, the Colorado North Central Region had already developed, and was ready to deploy, a machine readable emergency responder credential to allow electronic enrollment and tracking of responders at an incident site. These issues, combined with differences in training across jurisdictions, made interoperability a challenge and resulted in more difficult decision making for incident commanders.

The State of Colorado wanted to provide incident commanders with the ability to verify and validate the identity, qualifications, knowledge, skills, and abilities of the emergency responders with a high degree of assurance and trust, on the scene of an incident. A statewide credentialing working group determined that issuing credentials based on national standards to emergency responders across the state would facilitate movement across jurisdictional boundaries and enable more rapid response to catastrophic events. Compliance with Federal standards would enable interoperability among local, state, and Federal entities, which is particularly important in Colorado because a number of Federal agencies and military bases are located there.

## Solution and Implementation Approach

To address these needs, Colorado created the Colorado First Responder Authentication Credential Program (COFRAC), a statewide program to issue credentials to all emergency responders. These credentials are Tier I (PIV-I Smart Chip Encoded) or Tier II (barcoded) credentials that can be issued through fixed and mobile issuing stations. COFRAC began in the North Central Region of Colorado (Denver Area) in 2007, and was funded through several grant programs, including the State Homeland Security Grant Program, the UASI Grant Program, the Metropolitan Medical Response System (MMRS) Grant Program, and the Court Security Grant Program. COFRAC quickly grew into a state-driven initiative, which allowed for the creation of state-wide standards and state-managed training curriculums. The Colorado North Central Region abandoned its pre-PIV project, and reprogrammed all credentialing funding to the FIPS 201 architecture.

***A statewide credentialing working group determined that issuing credentials based on national standards to emergency responders across the state would facilitate movement across jurisdictional boundaries and enable more rapid response to catastrophic events.***

In Phase 1 of COFRAC, the Governor's Office of Information Technology (OIT) developed the "state bridge." This bridge contains the identity and privilege (attribute) database and the PKI infrastructure, which stores responder information and provides the Federal Public Key Infrastructure (FPKI) Common Policy, and is cross-certified to the Federal Bridge Certificate Authority (FBCA) at a medium hardware assurance level. Phase 1 also included the Colorado North Central Region's issuance of 800 credentials to law enforcement, fire, EMS, and emergency management personnel across to five pilot agencies. The program paid for the initial issuance to an agency ($60 per credential) and the first year's user fee. The agency funds the annual $20 fee per user for ongoing system maintenance.

Phase 2 of COFRAC calls for Colorado to continue issuing Tier I and Tier II credentials to these emergency responders, but now also includes the Governor's Office of Homeland Security, which will issue COFRAC credentials for other groups including doctors, registered nurses, EMS, and deployable emergency management stakeholders. The Program Managers of the remaining Regions are developing implementation plans based on grant guidance from the State of Colorado, and will begin implementing COFRAC in the current grant cycle.

COFRAC's value to organizations in the private sector, such as utility or repair companies, could eventually have a positive impact on the production costs of the credentials. It could also enable an external source of revenue that would offset credential production and system maintenance costs that are currently paid by the states and state agencies. Pre-credentialing employees who report to the site of an incident or to Federal buildings on a regular basis could save time and resources. These private sector credentialed individuals would still be processed through the state and would require the same information as any other state-credentialed individual.

## Benefits

- End user agencies will have improved interoperability with neighboring jurisdictions and will have statewide—and in some cases (e.g., Tier I credentials)—national interoperability.
- Physical and logical access can be standardized across the state, saving infrastructure costs.
- Consistency in training across the whole state enables better incident management.
  - Resources can be allocated by specific training and technical abilities.
- COFRAC can be used for everyday activities, such as checking in for shifts, issuing equipment to credential holders, releasing equipment on the scene, and incident management component tracking.
- COFRAC makes volunteer emergency responder training easier to track and provides individuals with reminders of training certificate expiration dates.

## Factors Leading to Success

- Development of compelling use cases, including:
  - Integrated incident management systems and responder accountability products.
  - Real-time incident views and post-incident reconstruction.
  - Links between responders' skills and abilities and authoritative regulatory databases, allowing positive trust in those abilities.
  - Automation and tracking of training records.
- State adoption of COFRAC by the State Department of Public Safety (State Patrol, Bureau of Investigation, Intelligence Center).
  - Shows real state commitment to the system.
  - Blunts perception as another "flash in the pan" state program.
- Further phases of this program will allow for strategically positioned mobile issuing stations in all

nine homeland security regions of the state allowing users to be easily credentialed close to where they live.

- Only minimal training on the COFRAC system is needed for users and agencies.
- COFRAC demonstrated and publicized the following benefits of the program to end users:
  - FIPS 201/PIV-I interoperable.
  - Standardized training.
  - Improved credential resource tracking and situational awareness is attractive to agencies that look to remain technologically current.
  - Software updates are funded by COFRAC and participating agencies can spare the related expenses.

## Lessons Learned

- Consistency in standards from the start avoids rework later in integrating new agencies.
- State-level buy-in on such an initiative is useful for local government and agency support.
- Local executive buy-in is crucial.
  - One key to COFRAC's success was that local chief executives had (pre-FIPS) already supported a credentialing solution.
- Existence of standards protects investment and eases buy-in.
  - The ability to point to an open-source standard (FIPS 201) made chief executives more accepting of the system and less concerned about long-term viability of their investment.
- It is important to find a sustainable business model.
  - Colorado is looking into multiple long term funding streams for this program.
  - Sustainment is built into per-user costs. COFRAC is not dependent on grant funds to continue functioning.
- Jurisdictions with legacy credentialing investments are hesitant to migrate without demonstrated savings or a state mandate.
  - Buy-in is easier to obtain from jurisdictions that do not currently have a credentialing system.
  - State agency adoption of COFRAC and continued rollout by large local agencies helps ensure protection of investment (i.e., no one wants to be the "first").

## Next Steps

- Continue to issue PIV-I/FRAC credentials.
  - COFRAC will have issued approximately 3,500 PIV-I/FRAC credentials to emergency responders across the state by the end of 2010.
- Encourage multiple independent jurisdictions to abandon legacy systems and utilize COFRAC for a broader statewide solution.
  - Today, some agencies add COFRAC as an additional credential, rather than rely upon it as a replacement of several credentials that they normally carry.
  - Continue roll-out of COFRAC within state agencies, replacing legacy state ID credentials.
- Continue the rollout of PIV-based physical access control systems:
  - Clear Creek County, Colorado Sheriff's Office, jail, and county offices.
  - Colorado Bureau of Investigation headquarters, State Crime Lab, Intelligence Center, and high-security criminal IT server rooms.
- Develop the ability to incorporate real-time training records, and the ability to validate state licensures and certifications into the state bridge.
- Achieve 100-percent credentialing of the public sector and include relevant segments of the private sector.
- Begin to develop policy and procedure guidelines for the statewide COFRAC program deployment through the state-designated agency.

- Build interfaces with definitive licensing databases, such as driver's license information, EMT and paramedic licensure databases, and doctors' and nurses' regulatory databases.
- Develop framework at the state level to leverage the infrastructure for logical network access to improve the security posture of the state's information systems and promote trusted identities across the governmental ecosystem (Federal-state-local).

# **District of Columbia One Card (DC1C) in the District of Columbia:** Even without SmarTrip, the DC1C Opens More than Just Doors

## Background

The District of Columbia (D.C.) offers a wealth of government-based resources to its residents and each agency had its own method of credentialing residents to allow them access. Having multiple agencies each issue a single-purpose credential was inefficient, since each agency was expending resources creating individual identification cards. A D.C. resident could potentially possess over a dozen cards, including a library card, a recreation center ID, a driver's license, a school ID, a Medicaid card, a D.C. government employee ID, and a number of other credentials provided by the city government. All 72 D.C. public secondary schools were each responsible for printing student IDs with their own resources and at their own expense. In addition, these disparate systems of managing resources prevented the identification of opportunities for residents to use one of their credentials for multiple purposes.

*With so many cards and so many disparate systems, the District focused on streamlining the systems and making data interoperable between agencies to increase accountability and benefit the residents.*

## Solution and Implementation Approach

With so many cards and so many disparate systems, the District focused on streamlining the systems and making data interoperable between agencies to increase accountability and benefit the residents. By identifying a way to link one card to many of the residents' everyday resources, such as linking it to the Washington Metro Area Transit Authority's (WMATA) SmarTrip system for public transportation, agencies would see the value of becoming affiliated with the program.

This incremental, phased approach of incorporating one agency at a time into the system began in April 2008. The District of Columbia One Card (DC1C) Program was developed by the Office of the Chief Technology Officer (OCTO) as a way to improve efficiency and reduce duplicative processes across government agencies. After conducting a pilot where information was successfully exchanged between the D.C. public library system and recreational centers, the District began issuing DC1C credentials to partici-

pants in the Summer Youth Employment Program. The DC1C Program implemented a supporting Identity Management System in January 2009 to manage information more efficiently through a consolidated system. To date, approximately 50,000 out of possible 600,000 D.C. residents have received a DC1C.

Currently, the District has the operational capability to issue Citizen DC1Cs to specific programs (e.g., D.C. Public Schools, Summer Youth Employment Program) and to the general public. Operational capacity to maintain ongoing service at the D.C. One Card Customer Service Center, as well as the ability to provide periodic rapid issuance capabilities (e.g., when traffic increases as the school year begins) is required. Since the program's inception, the OCTO has issued more than 50,000 DC1Cs to citizens primarily out of the one central Customer Service Center.

## Benefits

- District employees and residents will receive a single consolidated, multi-platform credential that can be used across all participating D.C. agencies.
- The program will increase efficiency, reduce cost to the government, and provide much-improved convenience for users and savings for participating agencies.
- The program is shifting its focus to begin implementing high-tech credentials that can help bridge the logical and physical worlds, assure the identities of users, and improve security.
- Members of the emergency response community can use this credential to access local, regional, and national incidents if produced with technology that allows PIV-I/FRAC capabilities.
- The centralized DC1C Identity Management System (IDMS) allows for centrally managed credential access (e.g., issuance, revocation, replacement) at participating agencies.
- Scanning credentials for attendance in schools prevents unauthorized students from entering during special events (e.g., sports or social events).

## Factors Leading to Success

- Users will be able to add new access points easily once they are in the IDMS.
  - Users can do this online through an online DC1C Activation Services or by visiting participating agencies.
- D.C. public schools were able to take advantage of economies of scale by consolidating their student ID production operations through the DC1C.
  - Student DC1Cs are standardized and easily read across schools, thus providing improved security.
  - Each school spends less time and effort enrolling and issuing IDs, spends less on printing equipment and consumables, and avoids delays due to local equipment failures.
- Making DC1Cs affordable for agencies and users (free for standard credential, $5 per SmarTrip-enabled card) contributes to widespread use.

## Lessons Learned

- An incremental, flexible approach has its advantages and disadvantages.
  - The program was able to be implemented quickly and meet the needs of the early adopters.
  - However, as new agencies were on-boarded into the program and demanded different services from the credentials, the program recognized the need for a central Identity Management System (IDMS). As the IDMS was implemented, significant time and resources were spent reworking aspects of the original solution.
- Agreeing on and adhering to standards from the beginning make scalability easier and saves re-work in the long run. However, it may make getting off the ground difficult in the first place.

- Agencies are happy to offload credentialing services if they can save money without jeopardizing service.
  - Credentialing is a non-core part of their business process.
- Linking the solution to widely used services, such as the Metrorail, will likely help increase adoption.
- A government that invests in high-tech (PIV-I/FRAC) credentialing technologies will need to see a return on investment.
- Card production costs would increase if they had PIV-I/FRAC technology.
- Increased outreach and marketing to end users and agencies would drive demand, but may overload the current capabilities for credential issuance and production based on the current resource level of the OCTO for this project.

## Next Steps

- Continue issuing DC1Cs to residents and gaining agency participants to the extent possible, given current resources.
- Develop and deploy its first PIV-I/FRAC credentials in early summer 2010.
- Link OCTO employees' PIV-I DC1Cs to network logins as a pilot for testing District employees' access potential.
- Distribute PIV-I compatible DC1Cs to emergency responders.

# **West Virginia FRAC:** Wild, Wonderful, and Secure

## Background

West Virginia lies immediately west of the National Capitol Region, and holds significant strategic value for the Federal Government Continuity program implementation. Additionally, significant mass-migration planning has occurred across state borders—from inside and outside the National Capital Region—which will potentially direct tens of thousands of people in the direction of West Virginia.

***As a result of the additional time needed to authenticate unknown credentials, these significant delays could prevent Federal officials from accessing Continuity sites and could keep doctors, nurses, and other emergency responders from accessing critical facilities or incident scenes for extended periods of time.***

With the exception of the City of Martinsburg (Berkeley County), the Eastern Panhandle fire departments are volunteer organizations. There is a mix of paid and volunteer EMS providers, although the vast majority of departments are fully-volunteer. There are numerous law enforcement agencies in each of the seven Counties, with many small local departments having only a two- or three-person squad. In the past, traffic-control point supervisors and incident commanders were left to assume that people were who they said they were, or else potentially deny them access until it was possible to validate their identity and/or qualifications. The additional time

needed to authenticate unknown credentials could cause significant delays, preventing Federal officials from accessing Continuity sites and could keep doctors, nurses, and other emergency responders from accessing critical facilities or incident scenes for extended periods of time.

For the routine-use case, there are few (if any) integrated physical or logical access systems in the Eastern Panhandle. Most personnel carry multiple access cards, pin numbers, and keys. Although the routine use case will become more important in coming years, the emergency use case has been the primary focus during initial planning stages of the "West Virginia FRAC: Wild, Wonderful, and Secure" program.

## Solution and Implementation Approach

West Virginia has embraced the intent of HSPD-12 and recognizes the value of FIPS 201 as the credentialing standard for Federal officials and emergency responders across the state. To that end, it is important to note that West Virginia is not part of the UASI, and therefore not eligible for the large blocks of funding typically associated with UASI jurisdictions. The State Homeland Security Grant Program (SHSG) will be used to fund the initial investment in system hardware and training for the Eastern Panhandle Counties, with additional grant opportunities explored for additional expense items.

West Virginia adopted the 2010 West Virginia Homeland Security Strategy, with Strategic Goal 4 addressing an interoperable credentialing system (Strategic Goal #4, Objective 4.3 – Develop a Credential Program). West Virginia's approach has been slow and deliberate, with a reverse implementation focus as compared to the other case studies. Protection of the Eastern Panhandle corridor is paramount for not only the nation's political establishment, but also for the traveling public and the State of West Virginia as a whole.

The corridor protection will only happen with a combination of reliable information sharing, staffing, identification credentials, and credential readers that are readily available to staff key traffic management locations. The Eastern Panhandle Region 3 grant committee recently approved a regional grant submission, written to facilitate the purchase of two readers and one management station for each of the seven Counties (Berkeley, Grant, Jefferson, Hampshire, Hardy, Mineral, Morgan) in Region 3. The regions linear mountain and valley topography, combined with limited wired-broadband access, necessitates the use of a higher number of management stations designed to maximize use of wireless networks for management control.

The seven County Emergency Managers make up the Eastern Panhandle Office of Emergency Management (OEM) Coordinating Council (EPOCC). Through a regional mutual aid agreement, EPOCC has agreed to assist each other with credential reader deployment, should additional readers be needed in any particular location. EPOCC recently appointed a regional credentialing coordinator and prioritized the list for physical and logical access system deployment, in the following phases:

- Phase 1: 911 and Emergency Operation Centers (to include the state EOC).
- Phase 2: Law enforcement facilities (including court facilities).
- Phase 3: Fire, EMS, and Health facilities.
- Phase 4: Other critical infrastructure (Government and Non-government).

Within each phase are two objectives (Objective A-physical access, and Objective B-logical access). It is the program's intent to fully implement Objective A within each phase before moving to Objective B needs. Though it is yet to be determined, it may be necessary to complete all Objective As across phases, before moving on to Objective B.

## Benefits

- Increases cooperation between local, state, Federal, private and volunteer sector emergency responders before and during a critical incident.
- Meets the control, identity proofing, registration, and technical objectives of HSPD-12 and FIPS 201 as allowed by a non-Federal entity.
- Allows emergency responders to have authorized physical access to identified critical incident areas.
- Accurately and efficiently identifies a person's qualifications and status within his or her respective agency or organization.

***Routine use will be critical to successful implementation of the FRAC system—not only limited to door/computer use scenarios, but also local meetings, fairs, and conferences.***

## Factors Leading to Success

- Including the FRAC program and FIPS 201 standards-based scenarios in exercise deliveries helped educate decision makers, state officials, local elected official, local emergency managers, and other emergency responders.
- Full no-match grant funding was not a financial burden on the localities.
- EPOCC and Region 3 Coordinator provided an integrated regional approach.
- Adoption of the State Homeland Security Strategy, "Strategic Goal 4: Facilitate Interoperability, Objective 4.3: Develop a Credentialing Program."

## Lessons Learned

- FIPS 201 standards and credentialing concepts continue to evolve—which has resulted in and will result in—additional changes.
- Routine use will be critical to successful implementation of the FRAC system—not only limited to door/computer use scenarios, but also local meetings, fairs, and conferences.
- Depending on specific jurisdictional challenges, credential issuance may not necessarily be the right way to "start."
- Regional mobile credential readers provide for more optimal usage.
- Inclusion and demonstration of FRACs, readers, and third-party software during local and regional exercises provides a tremendous visual for local elected officials who may otherwise be unintentionally disengaged from the program discussion.

## Next Steps

- Appoint a statewide credentialing coordinator.
- Establish stronger relationship with Federal relocation efforts.
- Evaluate all Phase 1 facilities for Objective A (Physical Access) needs.
- Identify multi-year funding for each phase and objective of implementation.
- Identify program governance and training needs—including issuance mechanisms.
- Identify additional short-term funding for program sustainability efforts and FRAC reissuance during 2010.

# Hawaii Emergency Response Official Credentialing Program in Honolulu, Hawaii: Trusted Credentials through "H/ERO's" Work

*Honolulu is in the early pilot phase of interoperable credentialing implementation but is committed to the PIV-I standard as the solution.*

## Background, Benefits, Solution, and Implementation Approach

Hawaii's emergency responder community did not have trusted credentials that aligned with FIPS 201 standards. They needed a solution that was PIV-Interoperable and compatible with the City and County of Honolulu enterprise Access Control and Monitoring System (ACAMS) as well as the City and County of Honolulu's Information Technology guidelines. Their solution, the Hawaii Emergency Response Official Credentialing Program (H/ERO), included PIV-I enrollment, credential creation, credential issuance with Federal Bridge interoperability, and City and County of Honolulu (CCHNL) ACAMS compatibility. To become enrolled in the system and receive a PIV-I credential, end users were required to provide two forms of personal identification in accordance with Schedule I-9.

H/ERO is funded by a UASI grant and has completed its beta testing stage. Phase 1 is scheduled to begin in Q3 2010 and will deliver approximately 2,000 credentials to CCHNL Government emergency responders, such as members of the fire department, police department, and EMS. Initial implementation will span across 2010-2011, with completion slated for 2011.

To date, the success of H/ERO can be attributed to its consistent operating procedures for end users and ongoing communication around the initiative. This is particularly true in terms of notifying enrollees as to the two forms of identification that are required for enrollment and scheduling of enrollment appointments. Key stakeholders including the Mayor's Office, the Information Technology Department and Emergency Management Department Heads; and the Honolulu Fire Department Administrative Chiefs were also active in the project.

## Lessons Learned

- Users will forget their Personal Identification Number (PIN) if they don't use it frequently.
  - If PIN authentication is enforced for the ACAMS system, it will promote daily use and increase the likelihood of remembering the PIN.
- Identification, compilation, categorization, and typing of attributes needed to be completed prior to the end user's enrollment.

***The Hawaii Emergency Response Official Credentialing Program (H/ERO), included PIV-I enrollment, credential creation, credential issuance with Federal Bridge interoperability, and City and County of Honolulu (CCHNL) ACAMS compatibility.***

## Next Steps

- End user working groups need to be established to confirm which attributes are considered credentials.
- Deployment of a system to support the incoming Asia Pacific Economic Cooperation (APEC) Federally credentialed responders and responder support staff.
- Train the Hawaii-based emergency response community to authenticate visiting emergency responders through the system when they arrive in Hawaii.
- Acquire the necessary hardware and software and add it to the existing ACAMS system (infrastructure is already in place).
- Develop exercises and test how systems will be used not only during APEC but afterwards.

## Notes:

# V. Glossary

**ACAMS –** Access Control and Monitoring System

**APEC –** Asia Pacific Economic Cooperation

**APL –** Approved Products List

**ASPR –** Office of the Assistant Secretary for Preparedness and Response

**C&A –** Certification and Accreditation

**CCHNL –** City and County of Honolulu

**CCI –** Command, Control and Interoperability

**CIKR –** Critical Infrastructure and Key Resources

**CIO –** Chief Information Officer

**COFRAC –** Colorado First Responder Authentication Credential Program

**D.C. –** District of Columbia

**DC1C –** District of Columbia One Card

**DHS –** U.S. Department of Homeland Security

**EMS –** Emergency Medical Service

**EMT –** Emergency Medical Technician

**EOC –** Emergency Operations Center

**EPOCC –** Eastern Panhandle OEM Coordinating Council

**ESF –** Emergency Support Function

**FBCA –** Federal Bridge Certificate Authority

**FEMA –** Federal Emergency Management Agency

**FICAM –** Federal Identity, Credential, and Access Management

**FIPS –** Federal Information Processing Standard

**FPKI –** Federal Public Key Infrastructure

**FRAC –** First Responder Authentication Credential

**GSA –** U.S. General Services Administration

**H/ERO –** Hawaii Emergency Response Official

**HHS –** U.S. Department of Health and Human Services

**HPP –** Hospital Preparedness Program

**HRSA –** Health Resources and Services Administration

**HSPD –** Homeland Security Presidential Directive

**IC –** Incident Commander

**IDMS –** Identity Management System

**IT –** Information Technology

**JNET –** Justice Network

**LACS –** Logical Access Control System

**LEJIS –** Law Enforcement Justice Information Sharing Project

**LEO –** Law Enforcement Official

**MMRS –** Metropolitan Medical Response System

**MSO –** Managed Service Office

**NCR –** National Capital Region

**NCRC –** Office of National Capital Region Coordination

**NGO –** Non-governmental Organization

**NIPP –** National Infrastructure Protection Plan

**NIST –** National Institute of Standards and Technology

**OCIO –** Office of the Chief Information Officer

**OCP –** Office of Commonwealth Preparedness

**OCSO –** Office of the Chief Security Officer

**OCTO –** Office of the Chief Technology Officer

**OEM –** Office of Emergency Management

**OIT –** Office of Information Technology

**PACS –** Physical Access Control System

**PIN –** Personal Identification Number

**PIV –** Personal Identity Verification

**PIV-I –** Personal Identity Verification - Interoperable

**PKI –** Public Key Infrastructure

**RSI –** Rapid Sequence Intubation

**S&T –** Science and Technology

**SHSG –** State Homeland Security Grant Program

**STRAC –** Southwest Texas Regional Advisory Council

**TSA-P –** Trauma Service Area - P

**TTWG –** Technology Transition Working Group

**UASI –** Urban Area Security Initiative

**WMATA –** Washington Metro Area Transit Authority

## Notes:

## Notes:

*Through a practitioner-driven approach, the DHS Science and Technology Directorate's Command, Control and Interoperability Division (CCI) creates and deploys information resources—standards, frameworks, tools, and technologies—to enable seamless and secure interactions among homeland security stakeholders. With its Federal partners, CCI is working to strengthen capabilities to communicate, share, visualize, analyze, and protect information.*

Homeland Security