

**Commonwealth of Virginia Personal
Identity Verification-Interoperable
(PIV-I)
First Responder Authentication
Credential (FRAC) Program**

October 2012

**W. Duane Stafford
Statewide Credentialing Coordinator**



**Governor's Office of Veterans
Affairs and Homeland Security**

Federal Credentialing Standard: HSPD 12

August 2004

- Homeland Security Presidential Directive 12
- Mandatory for all Executive Branches of Government
- Recognized:

“Wide variations in the quality and security of forms of identification used to gain access to secure Federal and other facilities where there is potential for terrorist attacks need to be eliminated.”



**Governor's Office of Veterans
Affairs and Homeland Security**

Federal Credentialing Standard: HSPD 12 (cont.)

Established a mandatory Federal Government-wide interoperable standard for secure and reliable forms of identification that:

- Can verify an individual's identity
- Are strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation
- Can be rapidly authenticated electronically
- Are issued through an official accreditation process
- Standard will include graduated criteria, from least secure to most secure, to ensure flexibility in selecting the appropriate level of security for each application



Federal Credentialing Standard: FIPS 201

February 2005

Federal Information Processing Standards (FIPS) 201:

- National Institute of Standards and Technology (NIST)
- Response to HSPD 12
- Specifies the architecture and technical requirements
- Defines requirements for identity proofing, registration, and issuance of identification cards

Primary Goal:

To achieve appropriate security assurance by efficiently verifying the claimed identity of individuals seeking physical access to federally controlled government facilities and electronic access to government information systems



**Governor's Office of Veterans
Affairs and Homeland Security**

Credentialing and Emergency Responders

In many high profile incidents, the lack of identity trust between jurisdictions resulted in the inability of Emergency Responders to reach incident scenes, and response and recovery activities were significantly delayed because incident scene commanders could not rapidly verify the person's identity



Arlington County 9/11 After Action Report

“Some firefighters said they had never seen so many volunteers, and wondered aloud if a volunteer firefighter tee shirt was the only required identification.”

“The last full activation of the EOC was in preparation for the anticipated problems associated with the arrival of the year 2000 (Y2K). As a result, although many county officials had EOC identification (ID) badges, they had long since expired. A current ID system was not in place.”

“Arlington County should work with neighboring jurisdictions and other emergency response agencies and volunteer organizations to implement a uniform identification system.”



Federal Response to Hurricane Katrina Lessons Learned

“[Complete] the development of a credentialing system ... to allow authorized volunteers and workers restoring critical infrastructure access to relief sites”

“The Federal response should better integrate the contributions of volunteers and nongovernmental organizations into the broader national effort. This integration would be best achieved at the State and local levels, prior to future incidents. In particular, State and local governments must ... credential their personnel, and provide them the necessary resource support for their involvement in a joint response.”



Credentialing Need

During incidents such as natural and man-made disasters, there is a need to expeditiously authenticate and validate Emergency Responders.

- Need to have a standard credential for Emergency Response Officials
- Credential needs to verify the identity and attributes of Emergency Responders at incident scenes
- Credential needs to facilitate access into and out of secured areas and across multi-jurisdictions
- Need a standard process and requirements to obtain the credential (trust model)



Virginia FRAC Program

2006

- The Commonwealth developed a Federal Information Processing Standards 201 (FIPS 201) interoperable FRAC Program using multi-year State Homeland Security Grant (SHSG) funding
- The FRAC is a standards-based smart card that is issued to the Emergency Response Community and recognized as a true representation of identity and other pertinent data
- The FRAC provides an interoperable identity credential platform for all Federal, State, local and private sector Emergency Responders
- Enhances cooperation and efficiency between Federal, state, regional, local, and private sector emergency responders before and during a critical incident



The Northern Virginia FRAC Pilot

- The Commonwealth developed a pilot FRAC using the Virginia portion of a NCR UASI grant in 2006
- Virginia was the first nationally
- Issued over 2,300 FRACs to Arlington County and the City of Alexandria Emergency Response Community
- Credential certificate life cycle ended in March 2010



**Governor's Office of Veterans
Affairs and Homeland Security**

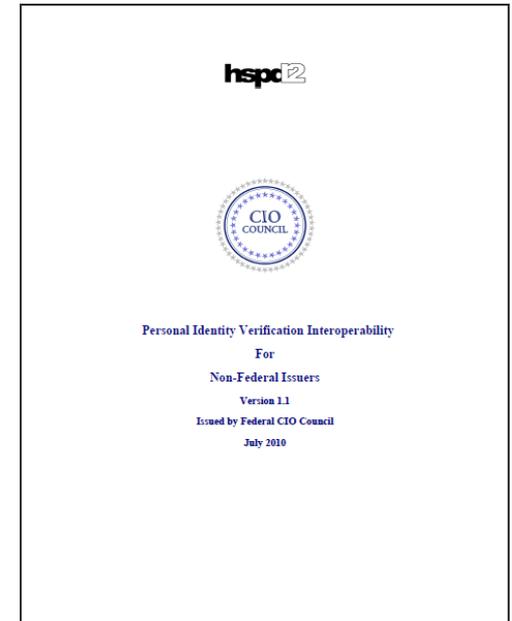
Interoperability Terminology for Identity Cards

Federal CIO Council releases *Personal Identity Verification (PIV) Standard for Non-Federal Issuers* in July 2010:

PIV Card (PIV) – an identity card that is fully conformant with federal PIV standards (i.e., Federal Information Processing Standard (FIPS) 201 and related documentation). Only cards issued by federal entities can be fully conformant. Federal standards ensure that PIV Cards are interoperable with and trusted by all Federal government relying parties.

PIV Interoperable Card (PIV-I) – an identity card that meets the PIV technical specifications to work with PIV infrastructure elements such as card readers, and is issued in a manner that allows Federal government relying parties to trust the card. **The FRAC is a PIV-I card.**

PIV Compatible Card (PIV-C) – an identity card that meets the PIV technical specifications so that PIV infrastructure elements such as card readers are capable of working with the card, but the card itself has not necessarily been issued in a manner that assures it is trustworthy by Federal government relying parties.



*As defined by the *Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guide* and the *Personal Identity Verification Interoperability for Non-Federal Issuers* document.



**Governor's Office of Veterans
Affairs and Homeland Security**

Credentialing Case Study

July 2010

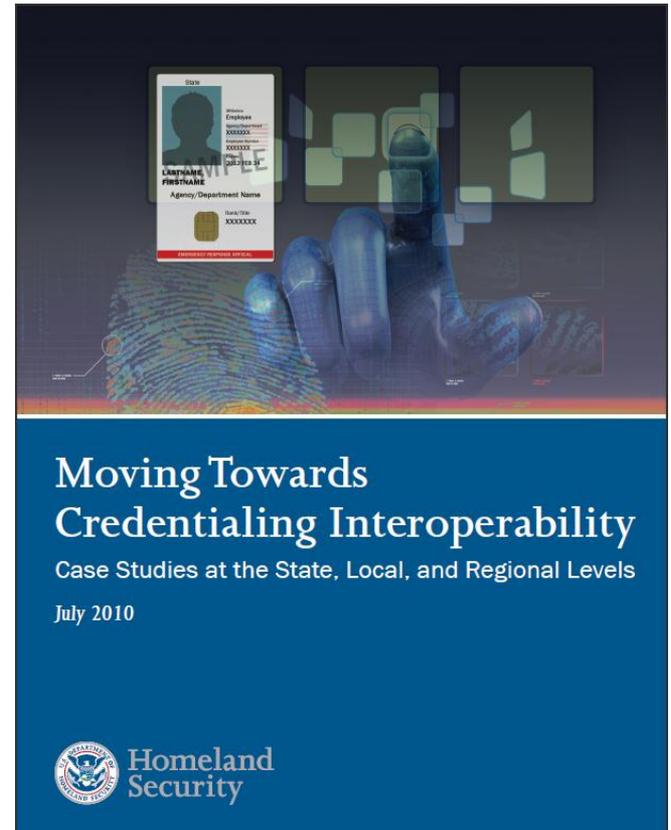
- Provides information to non-Federal organizations and their decision makers about the value of strong credentialing practices using Federal Standards
- Serves as an introduction to electronic identity/attribute management and credentialing for those whose purview is emergency management

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



**Governor's Office of Veterans
Affairs and Homeland Security**

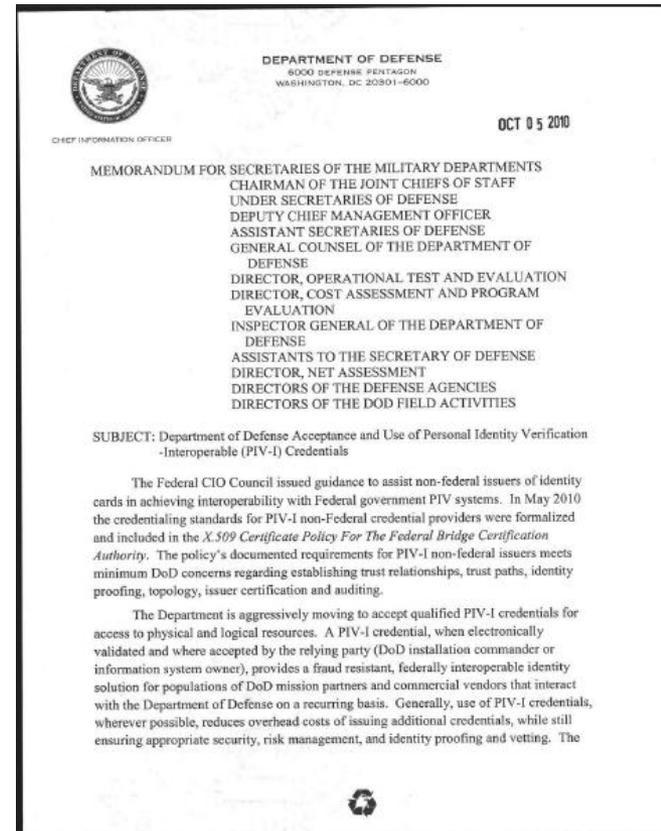


Department of Defense and PIV-I

October 2010

“The Department [DoD] is aggressively moving to accept qualified PIV-I credentials for access to physical and logical resources.”

“In those cases where DoD relying parties, installation commanders, and facility coordinators determine that granting access is appropriate and that appropriate vetting requirements are met, they should begin accepting DoD-approved PIV-I credentials for authentication and access.”



Governor's Office of Veterans
Affairs and Homeland Security

Hampton Roads Region FRAC Program

- Secured additional DHS grant funding for FRAC implementation in the Hampton Roads region
- Hampton Roads Regional Credentialing Working Group
- Public and Private participation



Hampton Roads Credentialing Roll Out

- Set up and configuration of the solution infrastructure (hardware, software, support and services)
- Deployment of the **8 enrollment and issuance stations** hosted and operated by localities.
- **39 handhelds** for on-scene credential validations
- **12,900 FRACs**
- \$3.2 M (over three FY grant cycles)

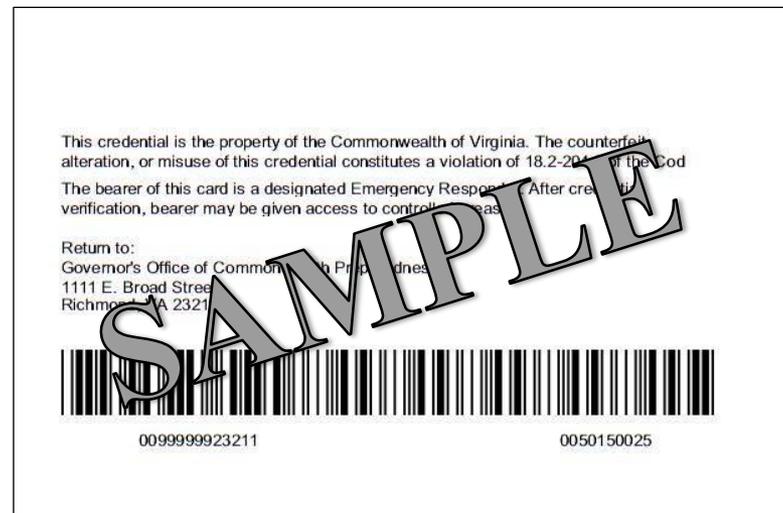


Hampton Roads Region FRAC Progress

- Distributed equipment to and trained
 - Newport News
 - Norfolk
 - Chesapeake
 - James City
 - Hampton
 - York County
 - Williamsburg
 - Virginia Beach
- Coordinating equipment, training and issuance to additional jurisdictions



Hampton Roads FRAC Topography



NIMS Credentialing Guidelines: State, Local and Tribal

July 2011 (released September 2nd)

“DHS strongly encourages state, local, and tribal authorities to use FIPS 201 and the PIV-I guidance in developing their credentialing systems.”

“A strong national preparedness and response system should be based on interoperability, commonality, and consistency. Therefore, DHS strongly recommends and requests that our partner governments build and implement a credentialing system consistent with these guidelines. DHS strongly recommends that the credentialing system developed incorporates the elements described herein to the maximum degree possible, should partner governments choose not to build a system completely compliant with the guideline.”



NIMS Guideline for the Credentialing of Personnel

July 2011



Homeland
Security



**Governor's Office of Veterans
Affairs and Homeland Security**

NIMS Credentialing Guidelines: Private Sector and Critical Infrastructure

“...DHS/FEMA encourages [Private Sector and Critical Infrastructure] to consider using FIPS 201 and the PIV-I guidance in developing their credentialing system.”

“Private sector organizations and CI owners and operators are encouraged to utilize PIV-I/FIPS 201 for badging their personnel.”



NIMS Guideline for the Credentialing of Personnel

July 2011



Homeland
Security



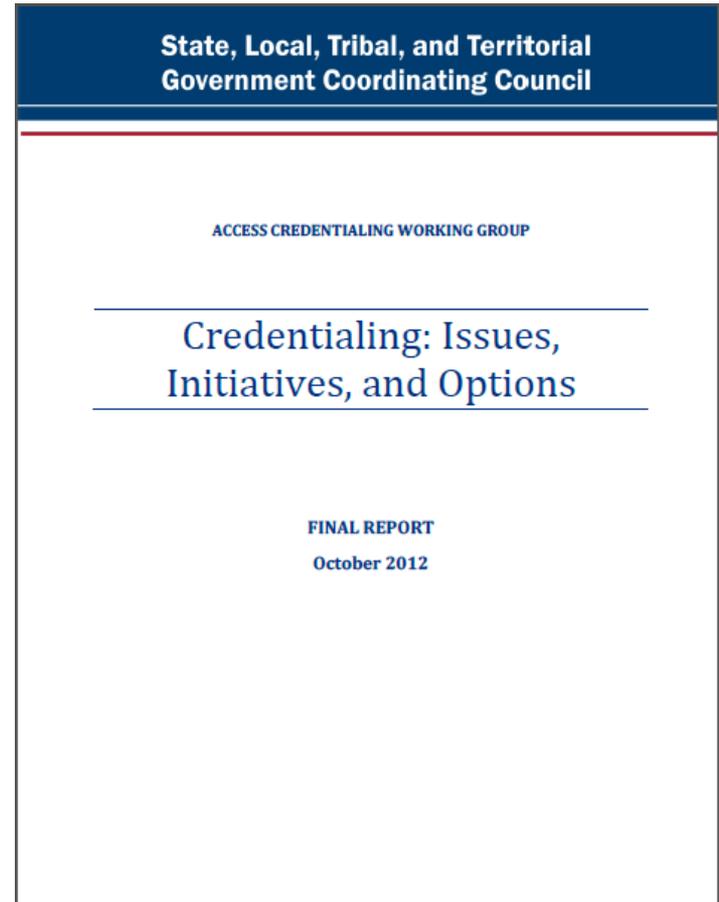
**Governor's Office of Veterans
Affairs and Homeland Security**

State, Local, Tribal, and Territorial Government Coordinating Council

“SLTT officials and critical infrastructure owners and operators typically carry several different identification credentials in order to perform their routine duties as well as operate effectively during emergencies.”

“The demands for credentialing are increasing in complexity and delayed access is becoming a critical issue.”

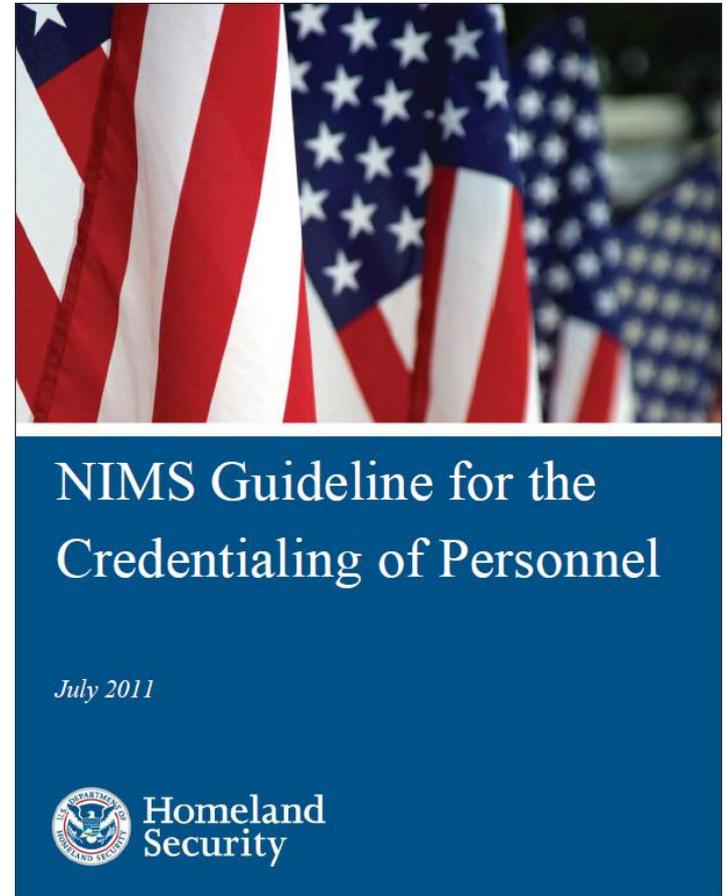
“PIV-I is the recommended model to follow for SLTT governments that are interested in adopting a federated credentialing model and/or a federally interoperable credentialing system.”



**Governor's Office of Veterans
Affairs and Homeland Security**

Next Steps

- Credential issuance using PIV-I standard
- Emergency Responders and CIKR Responders (public & private)
- Implement logical and physical access control
- Re-engage in Northern Virginia
- Issuance planning for the remainder of Virginia



Contact Information

W. Duane Stafford

duane.stafford@governor.virginia.gov

Office: (804) 225-4502



**Governor's Office of Veterans
Affairs and Homeland Security**