



Winter Storm Demonstration

After Action Report

**Mr. Steven E. Calvery
Director, Pentagon Force
Protection Agency (PFPA)**

**Mr. Thomas J. Lockwood
Director, Office of
National Capital Region
Coordination (NCRC)**

WINTER STORM

IDENTITY INTEROPERABILITY DEMONSTRATION

After Action Report

Executive Summary

On February 15, 2007, The Department of Homeland Security Office of National Capital Region Coordination (DHS NCRC) and the Department of Defense Pentagon Force Protection Agency (DoD PFPA) joined public and private sector participants to host Winter Storm, a multi-jurisdictional identity interoperability demonstration to display the advancements of the First Responder Partnership Initiative (FRPI) program.

More than 50 organizations, in over 20 locations across the United States, including the National Capital Region (NCR), simultaneously participated in Winter Storm. The demonstration validated the functionality of the First Responder Authentication Credential (FRAC) and the integration of electronic attributes (qualifications, authorizations, certifications, and privileges) that have been developed and advanced through the credentialing program.

“Winter Storm provided further validation of the technological advancements that will enable the nation to meet the goal of developing a unified credentialing system for first responders,” said Thomas Lockwood, Director of the Office of National Capital Region Coordination. “Such advancements will ensure that emergency personnel are better equipped to respond to incidents across the nation in an expedited fashion. Winter Storm demonstrated that new ground is being broken on this important effort to build a standardized program to improve the methods, capabilities and coordination of emergency responders throughout the nation.”

During Winter Storm, participants and observers viewed details on a commercially available mapping program that gave local, regional, and nationwide emergency operation centers real-time situational awareness of first responders during an all-hazards event.

Winter Storm is a follow on to Winter Fox, a multi-jurisdictional demonstration co-hosted by DHS NCRC and DoD PFPA in February 2006 that validated the capability of the credentialing technology. Winter Fox tested the interoperability and usability of the credential system through simulated emergency incidents at federal, state, and local facilities.

Since September 11th, there has been a critical demand for a common authentication credential first responders can use, not only during an all-hazards event, but also on a day-to-day basis for physical and logical access. NCRC has made great strides to advance this credentialing program. Through the cultivation of interagency and multi-jurisdictional partnerships with multiple federal and non-federal agencies, barriers surrounding information sharing for first responders are being addressed and solved.

Multi-Jurisdictional Standardization

The goal of DHS' First Responder Partnership Initiative is to provide federal and non-federal First Responders with a standardized identity management process and common credential that will enable access to government buildings and incident areas in the event of a terrorist attack or other all hazards events.

The following precepts were agreed upon for Winter Storm:

- 1) All participants had to possess a valid Public Key Infrastructure (PKI) certificate-based smart identity credential.
- 2) DoD participants possessed either a legacy 32K Common Access Card (CAC) with PKI certificates or a Federal Information Processing Standard (FIPS) 201 compliant 64K CAC with PKI certificates and a digital photo imbedded in the integrated circuit chip (ICC)
- 3) Other federal and non-federal participants possessed a FIPS 201 technology-compliant credential with PKI certificates and a digital photo imbedded in the ICC
- 4) Participants who requested routine access into a federal facility in accordance with Homeland Security Presidential Directive (HSPD) 12 were visually verified against printed photo on credential and then were required to insert credential into handheld device for electronic verification
- 5) Participants who requested non-routine access into federal or non-federal facilities had to follow the aforementioned procedure, then were required to electronically validate them to the credentials with Personal Identity Number (PIN) insertion into a handheld device
- 6) All relying parties required credential verification and PIN validation prior to making an informed decision for non-routine access permissions
- 7) All relying parties were pre-positioned at perimeter check points for handheld reader verification
- 8) Emergency Support Function (ESF) participants who forgot their PINs were required to show another form of government-issued photo identification and go through the visitor screening process

Demonstrated Scenarios

Winter Storm included the following three scenarios, which were deemed successful by all participating agencies:

- 1) Routine HSPD 12 / FIPS 201 access to federal facilities
- 2) Regional briefings in response to credible threats to critical infrastructure
- 3) Continuity of Operations (COOP)/Continuation of Government (COG) relocation

Scenario One

DoD PFPA exercised electronic identity management at one of their non-federal leased facilities for routine access permissions in accordance with HSPD 12 / FIPS 201. (Average time for processing individuals was 7 seconds.)

Scenario Two

A credible threat was received against National Critical Infrastructure sites in five different geographic regions. Officials in those regions assembled to receive regional threat briefings and discuss coordinate preparedness and response activities. Special perimeters and non-routine access permissions were established as follows:

Two perimeter checks were completed to enforce anti-terrorism/force protection security measures for authorized attendees.

- 1) The first perimeter check electronically verified identities using a handheld device, smart credential contact technology, and PIN insertion in accordance with HSPD 12 / FIPS 201 for personal identity verification
- 2) The second perimeter check electronically verified the sponsor-assigned ESF attribute or CAC DoD affiliation by smart credential insertion into handheld. The handheld device displayed the attribute information of Emergency Response Officials who were from ESF categories 1, 4, 5, 8, 9, and 13 in accordance with the National Response Plan (NRP) / National Incident Management System (NIMS) (See Appendix A.3)
- 3) All personnel repeated step ii when exiting the controlled area for an electronic capture of departure
(Average time for processing individuals through both perimeters was 55 seconds.)

Scenario Three

DoD PFPA and Central Intelligence Agency (CIA) Emergency Response Group (ERG) personnel dispersed advanced COOP/COG teams to a predetermined site in order to exercise relocation procedures which included HSPD 12 / FIPS 201 electronic identity management as a performance measure. (Average time for processing individuals through both perimeters was 55 seconds.)

Situational Awareness

In all scenarios, an electronic roster of onsite personnel was displayed on a commercially available mapping program that gave local, regional, and nationwide emergency operation centers real-time situational awareness of all first responders during the demonstration.

Validated Metrics

The Winter Storm demonstration validated the functionality of the FRAC and the capability to integrate HSPD 12 / FIPS 201 electronic identities with electronic attributes (qualifications, authorizations, certifications, and privileges). This process enables the integration of NRP/ NIMS resource typing skill sets. Winter Storm also validated the following key capabilities:

- 1) 100% validation of PKI identities using handheld devices and smart credentials
- 2) 100% verification of Emergency Response Officials with targeted ESFs as determined by participating agencies/jurisdictions
- 3) 100% validation of ESF attribute information exchange as agreed upon by participating agencies/jurisdictions
- 4) Statistics:
 - a) More than 50 organizations participated simultaneously in over 20 locations across the United States
 - b) Total electronic ID scans: 720
 1. PKI credentials: 665
 - i. Successful PIN entries for non-routine access: 479
 - ii. Incorrect PIN entries for non-routine access: 119
 - iii. Scan with no PIN entries for routine access: 64
 - iv. Revoked scans (intentional): 3
 2. Other government issued photo identification scans (driver's license barcodes): 55

Next Steps

The next steps for continued progress are:

- 1) Work with federal government to streamline electronic ID integration into established COOP/COG relocation processes
- 2) Work with federal and non-federal partners for NRP / NIMS resource typing skill set integration
- 3) Work with federal and non-federal partnership members for implementation in all of the NCR as incubator for national implementation

- 4) Work with partners to integrate usage into daily functionality for physical and network access permissions
- 5) Work with the public/private sector practitioner communities for critical infrastructure protection implementation and integration
- 6) Standardize products, services, and practitioner community application development
- 7) Include FRAC interoperability as a performance measure in all future exercises (federal, state, regional/private)
- 8) Integrate FRAC into Homeland Security Information Network (HSIN)
- 9) Provide lessons learned to federal agencies responsible for development of the Transportation Workers Identification Credential (TWIC) recommendations due to be published for Notice of Proposed Rule Making (NPRM)

APPENDIX A:

First Responder Partnership Initiative Business Rules

Expected Outcomes:

- 1) 100% electronic validation of identity and ESF category by all relying parties
- 2) Standardized disaster recovery identity and attribute processes incorporated into daily business practices

First Responder Authentication Credential (FRAC) Requirements

- 1) Credentialing Requirement
 - a. Functionality - The first responder authentication credential (FRAC) will enable the bearer's identity and emergency attribute (qualification, certification, authorization, and/or privilege) to be electronically verified and trusted by any incident commander or designated relying party responsible for the security and access control into, out of, and/or within the incident area
 - b. Standardization - The FRAC is to contain standards-based technology in accordance with National Institute of Standards and Technology (NIST) Federal Information Processing Standards publication 201 (FIPS 201) to ensure multi-jurisdictional interoperability in a distributed environment
- 2) Minimum Criteria
 - a. Validation content for tiered authentication
 1. The FRAC will be a smart credential with embedded integrated circuit chip (ICC) containing sponsoring agency identity information to include digital certificates issued from a trusted authority, such as a certified member of the US Federal Bridge Certificate Authority (FBCA)
 2. Second factor authentication through a digital facial photograph
 3. Third factor authentication through a six to eight digit numeric personal identification number (PIN) in accordance with requirements as specified in FIPS 201
 4. Fourth factor authentication through a match-on-card finger biometric as specified in FIPS 201
 5. Sponsoring agency name, jurisdiction, and state
 - b. Topography - The FRAC is to be compliant with all topography requirements as specified in FIPS 201 for Emergency Response Officials
- 3) Architecture Requirements
 - a. Enrollment and Issuance Architecture - The FRAC enrollment and issuance architecture requirements are to be compliant with all technologies, roles and responsibilities as specified in FIPS 201 and all related special publications and will be executed in a distributed environment

- b. Validation Architecture
 - 1. Revocation of a card must be published within 18 hours via both the Certificate Revocation List (CRL) and the issuer's Online Certificate Status Protocol (OCSP) servers.
 - 2. The FRAC public-key certificate validation architecture is to be compliant with the requirements to utilize CRLs and OCSP to enable dynamic First Responder identity and attribute validation/revocation information to be generated real-time or at a minimum of every eighteen hours.

Personal Identity Verification (PIV) Roles and Responsibilities

- 1) Applicant
 - a. must be sponsored for a FRAC by home agency
 - b. will be identity vetted at a minimum to the FBCA basic level (level 2 - see Appendix A.1)
 - c. may be identity vetted to the FBCA medium level (level 3) due to the nature of their emergency response requirements
- 2) Sponsor
 - a. must be identity vetted to FBCA for level of routine support
 - b. endorses applicant's request for a FRAC up to sponsor's FBCA level
- 3) Enrollment Official
 - a. enrolls applicant into system; reviews/authenticates/captures applicant's identity documents
 - b. must be identity vetted to FBCA medium level
 - c. must adhere to checks/balances: can not enroll and issue to same applicant
- 4) Registrar
 - a. reviews applicant's enrollment package, performs and adjudicates background checks as required
 - b. must be identity vetted to FBCA medium level
 - c. must adhere to checks/balances: can not enroll/issue to applicant
- 5) Issuance Official
 - a. re-verifies applicant's documentation; authenticates biometric
 - b. issues FRAC to applicant
 - c. must be identity vetted to FBCA medium level
 - d. must adhere to checks/balances: can not enroll and issue to same applicant
 - e. Data Elements: HR databases must conform to the agreed-upon data elements for personal identity verification at FBCA basic or medium levels (see Appendix A.2)

Products and Services

Procurement of cards, equipment, shared service providers (SSPs), and validation authority providers must be on the General Services Administration (GSA) FIPS 201 Approved Products List (APL) which can be found <http://www.idmanagement.gov>.

Sponsoring Agency Attribute Assignment Requirements

- 1) Categorize emergency response officials (ERO) in accordance with the 15 Emergency Support Functions (ESFs) in the National Response Plan (NRP) (see Appendix C)
- 2) Sub-categorize ERO in accordance with the NRP/National Incident Management System (NIMS) approved resource typing skill sets
- 3) Categorize all critical infrastructure protection (CIP) personnel in accordance with the 17 sectors as defined in the National Infrastructure Protection Plan (see Appendix A.3)
- 4) Sub-categorize CIP personnel in accordance occupation description

Sponsoring Agency Attribute Validation / Revocation Requirements

- 1) Real-time update (minimum every 18-hours) of agency certificate revocation list (CRL) and Online Certificate Status Protocol (OCSP) servers that must be publicly available from the card issuer
- 2) Standardized hand held data fields (see Appendix A.4)
- 3) Standardized challenge & response procedures

APPENDIX A.1:

Public Key Infrastructure (PKI) Federal Bridge Levels of Assurance for Personal Identity Verification

Assurance Level	Applicability
Test	To be established in the MOA with the Entity (will depend upon test circumstances)
Rudimentary (Level 1)	No identification requirement; applicant may apply and receive a certificate by providing his or her e-mail address
Basic (Level 2) Agency sponsored First Responders (plus FR attribute)	Identity may be established by in-person proofing before a Registration Authority or Trusted Agent; or comparison with trusted information in a data base of user-supplied information (obtained and/or checked electronically, through other trusted means (such as the U.S. mail), or in-person); or by attestation of a supervisor, or administrative or information security officer, or a person certified by a State or Federal Entity as being authorized to confirm identities.
Medium (Level 3) -Fed Gov (HSPD 12) -Sponsoring Agencies (FIPS 201: enrollment/issuance officials)	Identity shall be established by in-person proofing before the Registration Authority, Trusted Agent or an entity certified by a State or Federal Entity as being authorized to confirm identities; information provided shall be verified to ensure legitimacy. A trust relationship between the Trusted Agent and the applicant which is based on an in-person antecedent may suffice as meeting the in-person identity proofing requirement. Credentials required are either one Federal Government-issued Picture I.D., or two Non-Federal Government IDs, one of which shall be a photo I.D. (e.g., Drivers License)
High (Level 4)	Identity established by in-person appearance before the Registration Authority or Trusted Agent; information provided shall be checked to ensure legitimacy. Credentials required are either one Federal Government-issued Picture I.D., or two Non-Federal Government IDs, one of which shall be a photo I.D. (e.g., Drivers License)

APPENDIX A.2:

PIV Data Elements

Data Elements	Level of Assurance (LOA) 2		First Responder Recommended Requirements		Level of Assurance (LOA) 3		FIPS 201	
	Mandatory	Optional	LOA 2	LOA 3	Mandatory	Optional	Mandatory	Optional
State/Territory Locale	✓		✓	✓	✓		✓	
Jurisdiction, e.g., County, Borough, Parish, etc.	✓		✓	✓	✓		✓	
Full Legal Name								
* First Name	✓		✓	✓	✓		✓	
* Middle Initial	✓		✓	✓	✓		✓	
* Last Name	✓		✓	✓	✓		✓	
Email (per National Institute of Standards and Technology (NIST), assumes using on-line services)		✓		✓	✓		✓	
Department Acronym	✓	▪	✓	✓	✓		✓	
Agency & Sub-Agency Acronyms	✓	▪	✓	✓	✓		✓	
Work Location	✓		✓	✓	✓		✓	
Position Title	✓		✓	✓	✓		✓	
Position Description	✓		✓	✓	✓		✓	
Background Check		✓		✓	✓		✓	
Badge Type, e.g. Employee, Temporary Employee, Contractor, First Responder (FR), Volunteer	✓		✓	✓	✓		✓	
If Contractor:								
* Contract Number		✓		✓	✓		✓	
* Contract Start Date		✓		✓	✓		✓	
* Contract End Date		✓		✓	✓		✓	
If Contractor:								
* Employer		✓	✓	✓	✓		✓	
* Address Line 1		✓	✓	✓	✓		✓	
* Address Line 2		✓	✓	✓	✓		✓	
* City		✓	✓	✓	✓		✓	
* State/Territory		✓	✓	✓	✓		✓	
* Zip Code		✓	✓	✓	✓		✓	
Date of Birth	✓		✓	✓	✓		✓	
Place of Birth	✓		✓	✓	✓		✓	

PIV Data Elements (continued)

Data Elements	Level of Assurance (LOA) 2		First Responder Recommended Requirements		Level of Assurance (LOA) 3		FIPS 201	
	Mandatory	Optional	LOA 2	LOA 3	Mandatory	Optional	Mandatory	Optional
Financial Information, e.g., credit card number, checking account, savings account, loan number, etc		✓		✓	✓		✓	
Current Address of Record: * Line 1 * Line 2 * City * State/Territory * Zip Code	✓ ✓ ✓ ✓ ✓		✓ ✓ ✓ ✓ ✓	✓ ✓ ✓ ✓ ✓	✓ ✓ ✓ ✓ ✓		✓ ✓ ✓ ✓ ✓	
Daytime Phone Number (best as a wired land-line)		✓		✓	✓		✓	
Evening Phone Number (best as a wired land-line)		✓		✓	✓		✓	
Per Govt-Issued Photo ID: * Height- feet * Height- inches * Eye Color * Hair color * Gender * Type of ID presented, e.g., state driver license or ID, passport * Unique identifier of the identification presented	✓	✓✓✓✓✓ ✓	✓✓✓✓✓ ✓✓✓✓	✓✓✓✓✓ ✓✓✓✓	✓✓✓✓✓✓✓✓ ✓		✓✓✓✓✓✓✓✓ ✓	
Federal or State Government issued ID	▪	✓	✓	✓	▪	✓	✓	
Additional Identification presented (non-photo)	▪	✓	✓	✓	✓	▪		✓
US Citizenship	✓		✓	✓	✓		✓	
Biometric: * Digital Photo * Fingerprint * Other biometric capture, e.g., Iris scan, etc	✓	✓ ✓	✓	✓ ✓	✓	✓ ✓	✓ ✓	✓
Social Security Number or VISA number	▪	✓	▪	✓	✓		✓	

APPENDIX A.3:

15 NRP ESFs / 17 NIPP Sectors

National Response Plan/National Incident Management System (NIMS)

- ESF-1 - Transportation
- ESF-2 - Communication
- ESF-3 - Public Works & Engineering
- ESF-4 - Firefighting
- ESF-5 - Emergency Management
- ESF-6 - Mass Care, Housing, & Human Services
- ESF-7 - Resource Support
- ESF-8 - Public Health & Medical Services
- ESF-9 - Urban Search & Rescue
- ESF-10 – Oil & Hazardous Materials Response
- ESF-11 – Agriculture & Natural Resources
- ESF-12 – Energy
- ESF-13 – Public Safety & Security
- ESF-14 – Long-Term Community Recovery & Mitigation
- ESF-15 – External Affairs

National Infrastructure Protection Plan (NIPP)

- Sector 1 – Agriculture & Food
- Sector 2 – Banking & Finance
- Sector 3 – Chemical
- Sector 4 – Commercial Facilities
- Sector 5 – Dams
- Sector 6 – Defense Industrial Base
- Sector 7 – Emergency Services
- Sector 8 – Energy
- Sector 9 – Government Facilities
- Sector 10 – Information Technology
- Sector 11 – National Monuments & Icons
- Sector 12 – Nuclear Reactors, Materials & Waste
- Sector 13 – Postal & Shipping
- Sector 14 – Public Health & Healthcare
- Sector 15 – Telecommunications
- Sector 16 – Transportation
- Sector 17 – Water

APPENDIX A.4:

Standardized Handheld Data Fields

- 1. Identity Authentication Confirmation**
Unconfirmed
Incorrect Pin
- 2. Identity Assurance Level**
Basic (Level 2)
Medium (Level 3)
High (Level 4)
- 3. Emergency Support Function (ESF) Information**
- 4. Critical Infrastructure Protection (CIP) Information**
- 5. Additional Attribute Information (e.g., weapons, codes, special qualifications, etc.)**
- 6. Identity Sponsoring Agency (Static information)**
- 7. Jurisdiction Location (Static information)**
- 8. State (Static information)**

APPENDIX B:

Participants: Middle-Atlantic / NCR

Federal

- Department of Homeland Security
- Department of Defense, Pentagon Force Protection
- Department of State
- Central Intelligence Agency
- House of Representatives, Emergency Operations
- Fort Detrick USAG

District of Columbia

- Office of Chief Technology Officer

Virginia

- Virginia Department of Transportation
- Virginia Department of Public Health

Private

- American Red Cross National Headquarters
- The George Washington University

Maryland

- Maryland Strategic National Stockpile
 - Department of Health and Mental Hygiene (DHMH) Emergency Operations Center (EOC)
- Frederick County
 - County EOC
 - Office of Emergency Management
- Montgomery County
 - County EOC
 - County Police
 - County Fire
 - County Office of Homeland Security

Participants: Commonwealth of Pennsylvania

PA Region 13 Emergency Response Group

- Southwestern PA Emergency Response Group (13 County and City of Pittsburgh Emergency Management Agencies)
- PA Department of Health - SW PA office
- PA Emergency Management Agency - SW PA office
- University of Pittsburgh Medical Center
- Allegheny County Health Department
- The Washington Hospital
- Pittsburgh Poison Center
- Monongahela Valley Hospital
- The Western PA Hospital of West Penn Allegheny Health System
- Hospital Council of Western PA
- Emergency Medical Services, Inc.
- Allegheny General Hospital of WPAHS
- Mercy Hospital of Pittsburgh

Pennsylvania Department of Health

- Pennsylvania Department of Health
- Pennsylvania National Guard

Federal Government

- Health & Human Services, R-III

Participants:

South East

JAXPORT

- Navy Military Sealift Command, Damage Control
- Blount Island USMC Tenant Command
- US Coast Guard, Sector Jacksonville
- Florida National Guard Recruiting & Retentions
- US Army, 832- Transportation Division, SDDC
- Crowley Maritime Corporation

Illinois

Illinois State Emergency

Operations Center

- Illinois State Police
- Illinois Emergency Management Agency
- Illinois National Guard

San Antonio

Southwest Texas Regional Advisory Council for Trauma

- City of San Antonio Office of Emergency Management
- City of San Antonio Police Department
- City of San Antonio Fire Department
- Southwest Texas Regional Advisory Council for Trauma (STRAC)
- Bexar County
- Texas National Guard 6th Civil Support Team
- US Air Force
- NORTHCOM 5th Army
- Texas Army National Guard 6th Civil Support Team
- Texas Department of Health Services, Region VIII
- Federal Bureau of Investigation (FBI)

APPENDIX C:

Human Resource Situational Awareness

