FEMA

Spring Ahead
Federal and Mutual Aid Emergency Response Official Electronic Credentialing & Validation Interoperability Demonstration
May 19 – 21, 2009

After Action Report

Mr. Ken Wall
Acting Director,
Office of National Capital
Region Coordination (NCRC)

Contents

Executive Summary

In accordance with Title IV of Public Law (PL) 110-53, "Implementing Recommendations of the 9/11 Commission Act of 2007," the Administrator of the Federal Emergency Management Agency (FEMA) defined Federal and Mutual Aid Emergency Response Officials (F/EROs) as personnel with responsibilities under the National Response Framework (NRF), National Infrastructure Protection Plan (NIPP), the National Continuity Policy Implementation Plan (NCPIP), and / or the National Incident Management System (NIMS). Additionally, Title IV requires the establishment of an inventory or database system of F/EROs. FEMA established a F/ERO database system (F/ERO Repository) pilot within the National Capital Region (NCR) to account for all sponsored and registered F/EROs to support our preparedness mission. The Office of National Capital Region Coordination (NCRC) is the Execution Agent of the F/ERO Repository pilot in the NCR. The F/ERO Repository provides the capability to electronically validate F/ERO identities and attributes (qualifications, authorizations, certifications, and/or privileges) when deployed to expedite transiting to / from the scene, strengthen the decision process for entry into the incident scene, and provide secure electronic manifests of those who respond.

The Department of Homeland Security (DHS) FEMA NCRC joined public and private sector NRF, NIPP, and NCPIP stakeholders on May 19 - 21, 2009 to host Spring Ahead, a Federal and Mutual Aid multi-jurisdictional electronic validation demonstration leveraging Federal Information Processing Standard (FIPS) 201-compliant and FIPS 201-interoperable credentials. FIPS 201-compliant credentials are those credentials issued in accordance with Homeland Security Presidential Directive (HSPD)-12 (Federal Bridge Certificate Authority (FBCA) assurance level 4). FIPS 201-interoperable credentials are credentials that have adhered to FIPS 201 processes (FBCA assurance level 3 or higher) and technology requirements. The First Responder Authentication Credential (FRAC) is an example of a FIPS 201-interoperable credential.

Spring Ahead scenarios focused on FEMA Strategic Goal 1, "An integrated approach that strengthens the Nation's ability to address disasters, emergencies, and terrorist events;" FEMA Strategic Goal 3, "Provide reliable information at the right time for all users;" and FEMA Strategic Goal 5, "Build public trust and confidence through performance and stewardship," as well as the following Targeted Capabilities:

<u>Common Mission Area</u>
1. Communications
2. Community Preparedness and Participation
3. Planning
4. Risk Management

<u>Protect Mission Area</u>
1. Critical Infrastructure Protection
2. Epidemiological Surveillance and Investigation

<u>Respond Mission Area</u>
1. Citizen Evacuation and Shelter-in-Place
2. Emergency Operations Center Management
3. Medical Surge
4. Onsite Incident Management
5 Emergency Public Safety and Security Response

The objectives of Spring Ahead were (1) the electronic validation of cyber identity and cyber attributes of FIPS 201-compliant / -interoperable credentials; (2) establishment of just-in-time credential issuance business rules, critical infrastructure / key resources (CI / KR) affiliation business rules, and electronic validation business rules; (3) providing near real-time geospatial display of participants for situational awareness in multiple Emergency Operations Centers (EOCs); and (4) generation of reports that enabled accountability, traceability, and liability for post-event reconstruction, Stafford Act reimbursement, etc.

Spring Ahead was comprised of eight scenarios which included:

1. The electronic validation, in accordance with established business rules, of FIPS 201-compliant credentials of essential government F/EROs to out-of-area relocation sites.
2. The proof-of-concept validation of FIPS 201-compliant credentials to encrypt/decrypt critical deployment data and transfer same into a smart phone application.
3. CI / KR personnel followed affiliation access business rules and were issued credentials on-scene ("just-in-time") for electronic validation.
4. The electronic validation of the FIPS 201-compliant / PIV-I-interoperable credentials of Federal & Mutual Aid out-of-area ingress personnel, as well as the electronic validation of participants using the Transportation Workers Identification Credentials (TWICs) for access into seaports.
5. The transitioning of existing jurisdictional equipment to FIPS 201 technology for a migration strategy.

Notable strengths in this demonstration were:

1. Participants used FIPS 201-compliant / -interoperable credentials that were issued from disparate production infrastructures across the country. This proved that credentials *issued to a standard* by different infrastructures using various industry partners are interoperable.
2. The F/ERO smart phone application proof-of-concept successfully demonstrated the ability to digitally and securely store an emergency response official's "resume" (attributes, licenses, certificates), deployment documents, etc. on commercially available mobile phones using the F/ERO's FIPS 201-interoperable credential.
3. The government relocation movement tracked essential government personnel across multiple jurisdictions using their agency-issued FIPS 201-compliant credentials from the departure site, at each waypoint, and again at the final destinations. This provided near real-time tracking of essential government personnel from departure to arrival using water, air, and ground assets—the first time ever in this country.
4. A mobile credential issuance vehicle was used to issue just-in-time credentials to West Virginia and NCR demonstration participants. Business rules were established and followed to simulate on-site credential issuance to deployers who arrive at a scene without interoperable credentials. These just-in-time credentials were validated during the demonstration as being interoperable with Federal agency- and State-issued FIPS 201 credentials.

Areas for improvement are:

1. Inclusion of electronic identity and attribute validation as a performance measure in all future NCR exercises (Federal, State, regional, private sector)
2. Integrate PIV / PIV-I usage into daily functionality for physical and network access permissions. Daily use of the credential will also enable the credential holders to remember their PINs and using the credential every day will ensure that they have their credential on "the day."

All scenarios had NRF Emergency Support Function (ESF) 13 (public safety and security) law enforcement officers (LEOs) acting as relying parties. All relying parties endorsed the electronic validation process as trusted capability for making informed decisions for granting access permissions. More than 30 organizations, in 20 locations across the United States, including the NCR, simultaneously participated in Spring Ahead.

Section 1: Demonstration Overview

Demonstration Name	Spring Ahead
Type of Demonstration	FIPS 201 functional demonstration
Demonstration Start Date	May 19, 2009
Demonstration End Date	May 21, 2009
Duration	Three days
Locations Washington, DC	1. Anacostia Park Police HQ 2. Denver / Centennial, CO 3. Harrisburg / Pittsburgh, PA 4. Honolulu, HI 5. Jefferson City, MO 6. Las Vegas, NV 7. Martinsburg, WV 8. Phoenix, AZ 9. Port Authority of New York/New Jersey 10. Port of Norfolk, VA 11. Richmond, VA 12. Salt Lake City, UT 13. San Antonio, TX 14. Springfield, IL 15. West Greenwich / Cranston, RI
Sponsor / Coordinator	Office of National Capital Region Coordination (NCRC)
Program	NCRC Credentialing Initiative
Funding Recipient	None (jurisdictions self-funded)
Mission	To demonstrate multi-jurisdictional interoperability leveraging standardized technology, capability, and business processes.
Capabilities	Secure electronic validation of F/ERO cyber identity and cyber attribute(s)
Scenarios	Natural disaster; other
Demonstration Planning Team	Health and Human Services (HHS)—medical scenario FEMA National Continuity Program (NCP)—relocation scenario FEMA—coordination NCRFirst—CI / KR business rules
Participating Agencies	Federal: ▪ DHS ▪ DoD Pentagon Force Protection Agency (PFPA) ▪ FEMA ▪ HHS ▪ Small Business Administration (SBA) ▪ Social Security Administration (SSA) ▪ US Marshal Service (USMS) ▪ US Park Police (USPP) State: ▪ CO ▪ HI ▪ IL ▪ NV

	▪ PA ▪ Port Authority of NY/NJ ▪ Port of Norfolk, VA ▪ RI ▪ VA ▪ WV Local: ▪ District of Columbia (DC) ▪ Southwest Texas Regional Advisory Council for Trauma (STRAC) CI/KR: ▪ ChicagoFirst ▪ NCRFirst ▪ The George Washington University (GWU) ▪ University of Pittsburgh Medical Center (UPMC)
Number of Participants	Approximately 200 players in various roles to include: ▪ 8 evaluators (proctors) ▪ 16 controllers (relying parties)

Section 2: Demonstration Design Summary

1. *Demonstration Purpose and Design:*
   Spring Ahead was conducted to demonstrate the fulfillment of the requirement of Public Law (PL) 110-53, "Implementing Recommendations of the 9/11 Commission Act of 2007" to establish an inventory or database system (Repository) of Federal and Mutual Aid Emergency Response Officials (F/EROs). The F/ERO Repository provides the capability to electronically validate deployed F/ERO's identities and attributes (qualifications, authorizations, certifications, and/or privileges) to expedite transiting to / from the scene, strengthen the decision process for entry at the incident scene, and provide secure electronic manifests of those who respond. Spring Ahead demonstrated the utility of the F/ERO Repository pilot by electronically validating the identities and attributes of sponsored F/EROs.

   Additionally, Spring Ahead demonstrated the interoperability between Federal Information Processing Standard (FIPS) 201-compliant and FIPS 201-interoperable credentials issued from disparate infrastructures and organizations to include Federal, State, and CI/KR. This resolves the issue of the lack of standardized credentials / attributes that has been an area of concern in both the post-9/11 and post-Katrina reports.

2. *Demonstration Objectives:*
   a. electronic validation of FIPS 201-compliant / interoperable credentials for ingress of out-of-area responders into disaster site
   b. electronic validation of National Response Framework (NRF) Emergency Support Functions (ESFs), National Continuity Policy Implementation Plan (NCPIP) Continuity of Operations (COOP)/Continuity of Government (COG) designations, and National Infrastructure Protection Plan (NIPP) sectors as registered in the DoD or FEMA F/ERO repositories
   c. electronic validation of just-in-time credential issuance business rules
   d. electronic validation of CI / KR affiliation business rules

e. electronic validation of electronic validation business rules
f. electronic validation of F/EROs using jurisdiction-owned handhelds and Incident Command Systems (ICS)
g. near real-time geospatial display of participants for situational awareness in multiple Emergency Operations Centers (EOCs)
h. validation of electronic manifest for post-event reconstruction
i. validation of routine and emergency access into seaport using the Transportation Workers Identification Credential (TWIC)

2. Capabilities and Activities Identified for Demonstration:

Spring Ahead demonstrated a commitment to FEMA's Strategic Goals and the DHS Targeted Capabilities List as follows:

a. To demonstrate FEMA Strategic Goal 1, "An integrated approach that strengthens the Nation's ability to address disasters, emergencies, and terrorist events," the objectives were to demonstrate:
   - standardization of vetting processes, business rules, and technology (FIPS 201) for credential issuance to ensure multi-jurisdictional interoperability
   - interoperability is achieved even when using disparate infrastructures and industry partners
   - FIPS 201-interoperable migration strategies
b. To demonstrate FEMA Strategic Goal 3, "Provide reliable information at the right time for all users," the objectives were
   - the standardization of skill sets (attributes) across all ESFs and NIPP sectors to ensure that the ISC has reliable, electronic information to allow for the best use of the on-scene assets.
   - To ensure credential reading devices and just-in-time credentialing are operable in a communications-in or –out environment to provide necessary information during any situation
c. To demonstrate FEMA Strategic Goal 5, "Build public trust and confidence through performance and stewardship," the objectives were
   - to meet the mandates of PL 110-53 which requires FEMA to identify all F/EROs nation-wide and to establish a FEMA F/ERO Repository, of which FEMA NCRC is the steward
   - To make continued progress in refining the processes for F/ERO identification and registration in the Repository to ensure maximum performance levels during any all hazards event
d. Following is a list of the DHS Targeted Capabilities which Spring Ahead scenarios were designed to address (highlighted in yellow).

Figure 1.0: DHS Targeted Capabilities List

Common Mission Area
1. Communications
2. Community Preparedness and Participation
3. Planning
4. Risk Management
5. Intelligence/Information Sharing and Dissemination

Prevent Mission Area
6. CBRNE Detection
7. Information Gathering and Recognition of Indicators and Warnings
8. Intelligence Analysis and Production
9. Counter-Terror Investigations and Law Enforcement

Protect Mission Area
10. Critical Infrastructure Protection
11. Epidemiological Surveillance and Investigation
12. Food and Agriculture Safety and Defense
13. Laboratory Testing

Respond Mission Area
14. Animal Health Emergency Support
15. Citizen Evacuation and Shelter-in-Place
16. Critical Resource Logistics and Distribution
17. Emergency Operations Center Management
18. Emergency Public Information and Warning
19. Environmental Health
20. Explosive Device Response Operations
21. Fatality Management
22. Fire Incident Response Support
23. Isolation and Quarantine
24. Mass Care (Sheltering, Feeding, and Related Services)
25. Mass Prophylaxis
26. Medical Supplies Management and Distribution
27. Medical Surge
28. Onsite Incident Management
29. Emergency Public Safety and Security Response
30. Responder Safety and Health
31. Emergency Triage and Pre-Hospital Treatment
32. Search and Rescue (Land-Based)
33. Volunteer Management and Donations
34. WMD/Hazardous Materials Response and Decontamination

Recover Mission Area
35. Economic and Community Recovery
36. Restoration of Lifelines
37. Structural Damage Assessment

4. Scenario Summaries:
Spring Ahead consisted of eight scenarios as follows:

Scenario One: Essential Government Relocation (May 19, 2009—6:00AM – 2:00PM) (all scenario times are Eastern Standard Time (EST))
This scenario entailed essential government F/EROs assembled at two NCR rally points controlled by the US Marshal Service (USMS) for egress to two relocation sites in two States using a combination of water, air and ground assets from both States. It focused on NRF ESF 1 (see Appendix A: ESF and NIPP Tables on page 15), ESF 5, ESF 13, ESF 15; NIPP Sector 9, NIPP Sector 16; and National Continuity Policy Implementation Plan (NCPIP) ESF 5 (COOP, COG). The objective was the electronic validation of participants using valid FIPS 201-compliant or -interoperable credentials which provided near real-time tracking of essential government personnel from departure to arrival using water, air, and ground assets—the first time ever in this country.

Scenario Two: F/ERO Smart Phone Application (Proof-of-Concept) (May 20, 2009—1:00PM – 3:00PM)
This scenario focused on NRF ESF 5, ESF 8 (primarily Emergency System for the Advance Registration of Volunteer Health Professionals (ESAR-VHP)), and NIPP Sector 14. The premise was that FEMA, HHS, and SBA had disaster work force personnel activated in an emergency.

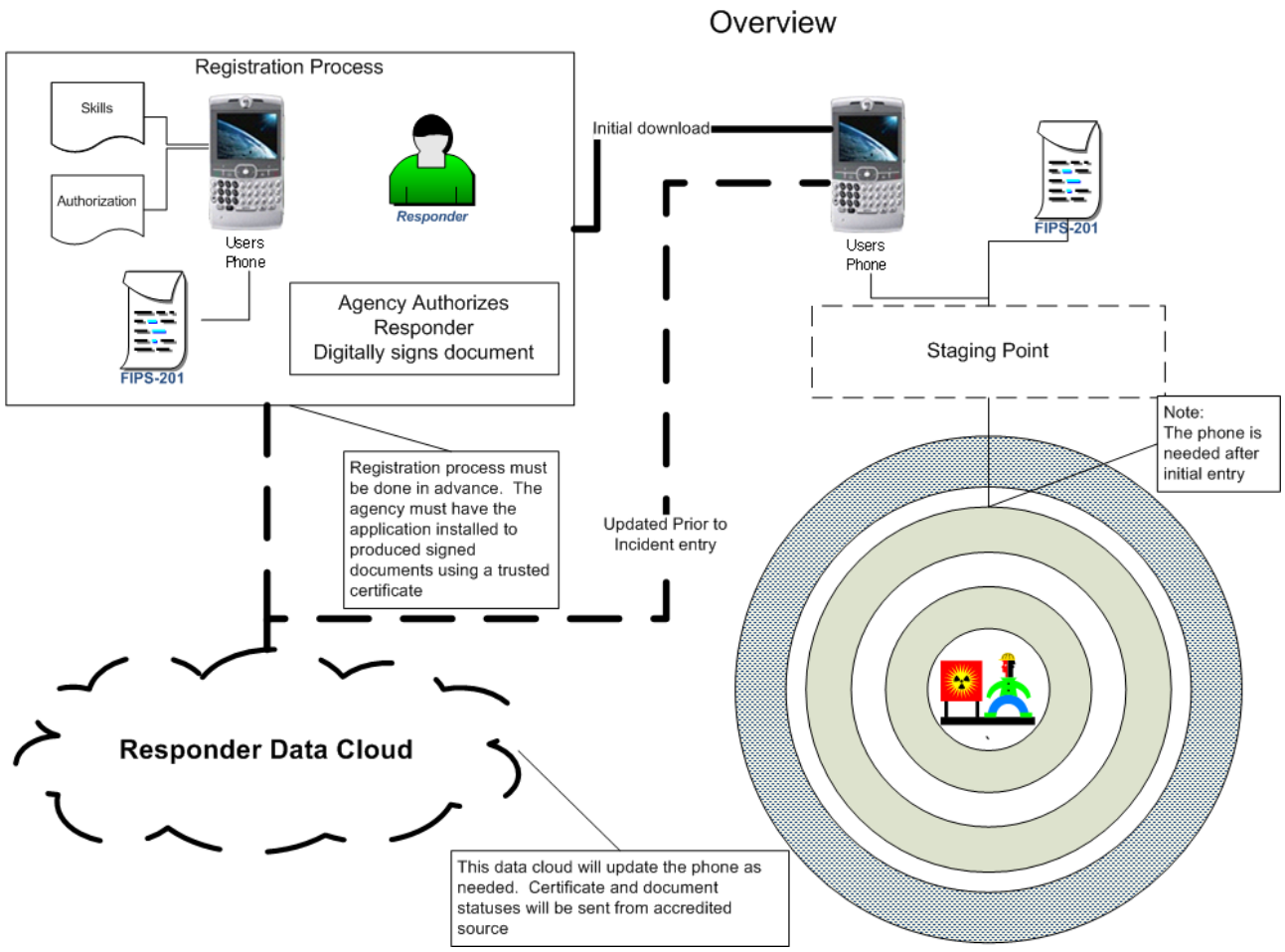
Precepts and assumptions for this scenario were that only Personal Identity Verification (PIV) test credentials from HHS, SBA, and FEMA Homeland Security Presidential Directive (HSPD)-12 infrastructures were demonstrated; the demonstration portrayed the F/ERO smart phone application already encrypted and loaded in a Microsoft (MS) windows mobile 5/6 operating system; deployment source authorities are governmental or CI/KR affiliations with established agreements; and deployed F/EROs required additional documentation (education, qualifications, licenses) in order to assist with disaster work force integration.

The National Incident Management System (NIMS) deployment criteria require verification of the responding F/ERO's identity, attribute or affiliation (CI/KR), and source authority to deploy. Using FIPS 201 technology enables electronic validation of PIV and PIV-Interoperability (PIV-I) credentials; electronic validation of sponsored attributes or CI/KR affiliation; and reliability in a communication-in or -out all hazards environment. The F/ERO Smart Phone Application is a proof-of-concept for using encryption certificates on PIV or PIV-I credentials; encrypting detailed attribute / affiliation and deployment authorization data; transferring encrypted data into a windows mobile 5/6 smart phone; transporting, transferring, and decrypting data from smart phone to incident scene personnel accountability system.

Next steps are the final development of the application based on field testing; application program interfaces (APIs) to feed Incident Command System (ICS) applications; final development of the encoding platform for authorized sources to enable a commercially available smart phone with the application; and multi phone / multi network availability.

Following is a graphic overview of the F/ERO smart phone application.

Figure 2.0: Smart Phone Application (Proof-of-Concept)



Scenario Three: Just-in-time Credential Issuance (May 19, 2009 in Martinsburg, WV—8:00AM – 3:00PM; May 20, 2009 in Washington, DC—8:00AM – 3:00PM)

In this scenario, response and recovery personnel followed business rules to be issued FIPS 201-interoperable "just-in-time" credentials on-scene and were electronically validated for emergency access. The scenario focused on NRF ESF 1, ESF 4, ESF 5, ESF 8, ESF 15; NIPP Sector 2, NIPP Sector 14; NCPIP ESF 5 COOP, and NCPIP ESF 5 COG. Just-in-time credentials were issued to DC Government, GWU, NCRFirst, and WV.

Established business rules for just-in-time credential issuance were to present (1) two forms of identity source documents from the list of acceptable documents included in Form I-9, OMB No. 1115-0136, Employment Eligibility Verification with one being a valid State or Federal government-issued photo identification (ID), (2) deployment authorization document to include NRF ESF attribute or NIPP CI / KR Sector affiliation, and (3) source authority for deployment and reimbursement.

A self-contained mobile credential issuance vehicle, which can operate in a communications-in or –out environment, went to West Virginia on May 19 and to the DC demonstration location on May 21. All personnel pre-registered at a website and arrived at the issuance site with 2 forms of ID and deployment authorization (as defined in the business rules). They were issued their just-in-time credentials and preceded to the demonstration location to have their credentials electronically validated during the demonstration. The credentials issued from this mobile issuance vehicle were validated to be interoperable with all other FIPS 201-interoperable credentials issued from disparate infrastructures. Additionally, this capability allows the incident scene commander to assign F/EROs to work at the incident scene more efficiently and effectively.

Scenario Four: Routine and Emergency Access into Seaports (May 21, 2009—7:00AM – 10:00AM)
This scenario involved personnel requesting routine and emergency access into the Port of Norfolk, VA and the Port Authority of New York / New Jersey. It focused on NRF ESF 1, ESF 5, ESF 13 and NIPP Sector 16. Individuals entering the Ports had his/her PIV, TWIC, or DoD Common Access Card (CAC) credential electronically validated using a hand held credential reader which also produced an electronic roster which could be used for traceability, liability, accountability, post-event reconstruction, etc.

Scenario Five: Federal & Mutual Aid Out-of-Area Ingress for Disaster Response (May 21, 2009—10:00AM – 12:00PM)
This scenario demonstrated Federal & Mutual Aid ingress of out-of-area personnel processed through the Joint Receiving Staging Operations Integration (JRSOI) location for response/recovery assistance. Participants were Federal NRF and NIPP F/EROs, CO, DC, HI, IL, MD, RI, STRAC, VA, and WV. This scenario focused on NRF ESF 1, ESF 2, ESF 4, ESF 5, ESF 8, ESF 9, ESF 10, ESF 13, ESF 15; NIPP Sector 2, Sector 9, Sector 11, Sector 14, Sector 16; and NCPIP ESF 5 (COOP, COG).

All PIV-compliant and PIV-interoperable credentials were proven to be interoperable during Spring Ahead regardless of the issuing infrastructure. Law enforcement relying parties concurred that the information provided by the electronic reading of the credentials allowed them to make a more informed decision for granting access permissions. Additionally, the attributes associated with the identity allow the incident scene commander visibility of the on-scene assets. The electronic rosters produced by the handhelds / laptop also provided traceability, liability, and post-event reconstruction.
.
Scenario Six: FIPS 201 Technology Migration (May 21, 2009—9:00AM – 10:30AM)
Scenario six showed emergency access into State Emergency Operations Centers (EOCs) using jurisdiction-owned handhelds / laptops and incident command systems upgraded to FIPS 201 technology. Participating entities were CO, DC, and IL and focused on NRF ESF 2, ESF 4, ESF 5, ESF 8, ESF 9, ESF 10, ESF 13, ESF 15; NIPP Sector 14; and NCPIP ESF 5 (COOP). This scenario demonstrated the cost-saving capability of using previously-owned equipment and upgrading it to be FIPS 201 interoperable. Interoperability achieved in this manner was validated to be interoperable with all other infrastructures.

Scenario Seven: Citizen Evacuation / Post-Disaster Re-entry / Shelter-in-Place (May 21, 2009—9:00AM – 12:00PM)

This scenario depicted the electronic validation of FIPS 201-interoperable credentials and/or electronic verification of State-issued drivers licenses (DLs) which enabled real-time accountability of citizens or legal residents requiring evacuation, shelter-in-place, or post-disaster re-entry into devastated communities. The electronic rosters produced by the handhelds / laptop provide traceability, liability, and post-event reconstruction. Participating entities were CO, HI, IL, PA, RI, STRAC, VA, WV, and the Women's Memorial in DC.

Scenario Eight: EOC Geospatial Situational Awareness (May 21, 2009—10:30AM – 12:00PM)

Scenario Eight demonstrated the ability to provide EOCs around the nation with Spring Ahead near real-time situational awareness through a Virginia Department of Emergency Management (VDEM) web-enabled geospatial application named Virginia Interoperability Picture for Emergency Response (VIPER). Participants either sending and / or viewing information were **Federal:** DoD, State Department (STATE), Federal Aviation Administration (FAA), Federal Communications Commission (FCC), National Aeronautics and Space Administration (NASA), SSA, Treasury Department (TREAS); **State**: AZ, CO, HI, IL, MO, NV, PA, RI, UT, VA, WV; **Local**: PA Region 13, STRAC, Women's Memorial; and **CI/KR:** GWU, NCRFirst, Port Authority NY/NJ, Port of Norfolk, and UPMC.

For all scenarios, all participants were able to view an electronic roster of their own emergency response officials, by name and attribute(s), as well as those of other entities across the country. This capability was strongly endorsed by all participants and proctors as being an extremely useful tool.

Statistics:

More than 30 organizations participated simultaneously in over 20 locations across the United States. There were 569 total electronic ID scans:

1. PKI credentials from the following entities:
    - HSPD-12 PIV
        1. Dept of Defense CAC
        2. HHS
        3. Dept of Homeland Security (DHS)
        4. FEMA
        5. PFPA
        6. SBA
    - PIV-I (includes FRAC)
        1. Colorado (CO)
        2. District of Columbia (DC)
        3. Hawaii (HI)
        4. Illinois (IL)
        5. Pennsylvania (PA)
        6. Rhode Island (RI)
        7. San Antonio, TX
        8. Virginia (VA)
        9. West Virginia (WV)

- Transportation Workers Identification Credential (TWIC)
    1. Port Authority of New York/New Jersey (PA NY/NJ)
    2. Port of Norfolk, VA
    3. West Virginia (WV)

2. Other government-issued photo identification scans (State-issued driver's license barcodes) from the following States:
    - Colorado (CO)
    - Connecticut (CT)
    - District of Columbia (DC)
    - Illinois (IL)
    - Maryland (MD)
    - Massachusetts (MA)
    - New Jersey (NJ)
    - Pennsylvania (PA)
    - Texas (TX)
    - Virginia (VA)
    - West Virginia (WV)

5. Planned Simulations

One scenario depicted the electronic validation of State-issued drivers licenses (DLs) to enable real-time accountability of citizens or legal residents requiring evacuation, shelter-in-place, or post-disaster re-entry into devastated communities. The electronic rosters produced by the handhelds / laptop provided traceability, liability, and post-event reconstruction. Participating entities were CO, HI, IL, PA, RI, STRAC, VA, WV, and the Women's Memorial in DC.

Section 3: Analysis of Capabilities

Precepts and Assumptions:

1. Federal participants possessed agency-issued PIV / FIPS 201 credentials
2. Non-Federal participants possessed PIV-I / FIPS 201 interoperable credentials or State-issued drivers licenses
3. Electronic attributes were assigned in accordance with:
    - NRF ESFs
    - NIPP Sector Functions
    - NCPIP Essential Government Functions
4. Relying parties were ESF 13 public safety & security officials trained to operate the handhelds / laptops and to electronically validate all identities and attributes of emergency response officials before granting access

Electronic Validation Business Rules:

1. All relying parties were ESF 13 Public Safety and Security personnel
2. All PIV and PIV-I credentials were electronically challenged for single-factor authentication of currency or revocation status
3. All credential bearers were electronically challenged with 2 or more factor authentication procedures
    a) Authentication procedures were defined as follows:

   b) 2-factor: single-factor credential validation plus PIN insertion
   c) 3-factor: 2-factor plus credential validation of digital photo on integrated circuit chip (ICC)
4. 4-factor: 3-factor plus credential validation of biometric on ICC
5. The 2 or more factor electronic validation process was used for initial and final access control points
6. Single-factor validation procedures were used for intermediate control points

Relying parties strongly endorsed the FIPS 201 process as being superior to scanning the DLs because the irrefutable electronic information garnered from the FIPS 201-compliant / -interoperable credentials allowed them to make an informed decision. Scanning the DL barcodes forced the relying parties to make a discretionary decision by reviewing the scanned data and comparing it to the information on the front of the DL. Additionally, not all State drivers' licenses had bar code technology; thus, the relying party did not have any information with which to make an informed decision for access.

Validated Outcomes:

The validated outcomes were:

1. 100% electronic validation of FIPS 201-compliant / interoperable credentials for ingress of out-of-area responders into disaster site
2. 100% electronic validation of NRF ESFs, NCPIP COOP/COG designations, and NIPP sectors as registered in the DoD or FEMA F/ERO repositories
3. 100% electronic validation of just-in-time credential issuance business rules
4. 100% electronic validation of CI / KR affiliation business rules
5. 100% electronic validation of electronic validation business rules
6. 100% electronic verification of drivers license
7. 100% electronic validation of F/EROs using jurisdiction-owned handhelds and Incident Command Systems (ICS)
8. 100% near real-time geospatial display of participants for situational awareness in multiple Emergency Operations Centers (EOCs)
9. 100% validation of electronic manifest for post-event reconstruction
10. 100% validation of routine and emergency access into seaport using TWIC

Section 4: Conclusion

Spring Ahead was successful on several levels:

1. Interoperability was validated:
   a) for credentials issued to a standard (FIPS 201) from disparate infrastructures (Federal / State)
   b) for just-in-time credentials issued on site using newly-established CI / KR business rules
2. Relocation:
   a) Multi-State, multi-agency relocation demonstration using newly-established electronic validation business rules
   b) Near-real time tracking of personnel from departure to arrival—the first time in this country
3. Technology migration:
   a) CO and IL had existing equipment which they successfully upgraded to be FIPS 201-interoperable
   b) DC used an existing Toughbook laptop used in the Metropolitan Police Department (MPD) cruisers and successfully upgraded it to be FIPS 201-interoperable
4. Business rules development:

a) FEMA relocation personnel adopted newly-established business rules designed to validate identity, justify presence on scene (relocation attribute), and track personnel. These business rules are now standard operating procedure (SOP) for Federal relocation efforts in the NCR.
b) CI / KR communities evaluated the newly-established business rules designed to incorporate present CI / KR requirements with FIPS 201 technology which includes validation of identity (2 forms of I-9 identity documents) and documentation to justify being on-scene (source authority to deploy). CI / KR participants approved of the new business rules as fulfilling their requirements and see them as expediting their ability to work quickly and efficiently at the scene.

Areas for improvement are:

1. Inclusion of electronic identity and attribute validation as a performance measure in all future NCR exercises (Federal, State, regional, private sector)
2. Integrate PIV / PIV-I usage into daily functionality for physical and network access permissions. Daily use of the credential will also enable the credential holders to remember their PINs and using the credential every day will ensure that they have their credential on "the day."
3. Provide more education and outreach to those entities with responsibilities under the NRF, NIPP, and NCPIP to ensure they understand the responsibilities and the process.

The next steps for continued progress are:

1. Continue coordination of the enrollment of F/ERO personnel within the NCR who have responsibilities in the NRF, NIPP, NCPIP or NIMS into the F/ERO Attribute Repository
2. Continue coordination for exchanging attribute information between partnering entities to enable the electronic validation of human resource assets for situational awareness
3. Work with Federal and non-Federal partnership members for implementation in all of the NCR as a model for national implementation
4. Work with Federal and non-Federal partners for NRF, NIPP, NCPIP, and NIMS credentialing integration.

Appendix A: ESF and NIPP Tables

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

Sector 1	Agriculture and Food
Sector 2	Banking and 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 and Icons
Sector 12	Nuclear Reactors, Materials and Waste
Sector 13	Postal and Shipping
Sector 14	Public Health and Healthcare
Sector 15	Communications
Sector 16	Transportation Systems
Sector 17	Water
Sector 18	Critical Manufacturing

Appendix B: Acronyms

AAR	After Action Report
AZ	Arizona
CAC	Common Access Card
CI/KR	Critical Infrastructure / Key Resources
CO	Colorado
COG	Continuity of Government
COOP	Continuity of Operations
DC	District of Columbia
DHS	Department of Homeland Security
DL	Drivers License
DoD	Department of Defense
EOC	Emergency Operations Center
ESAR-VHP	Emergency System for the Advance Registration of Volunteer Health Professionals
ESF	Emergency Support Function
FERO	Federal and Mutual Aid Emergency Response Official
FIPS	Federal Information Processing Standard
FRAC	First Responder Authentication Credential
GWU	The George Washington University
HHS	Health and Human Services
HI	Hawaii
HSPD	Homeland Security Presidential Directive
ICC	Integrated Circuit Chip
ICS	Incident Command System
IL	Illinois
LEO	Law Enforcement Official
MD	Maryland
MO	Missouri
MPD	Metropolitan Police Department (DC)
MS	Microsoft
NCP	National Continuity Program
NCPIP	National Continuity Program Implementation Plan
NCR	National Capital Region
NCRC	Office of National Capital Region Coordination
NIMS	National Incident Management System
NIPP	National Infrastructure Protection Plan
NIST	National Institute for Standards and Technology
NRF	National Response Framework
NV	Nevada
PA	Pennsylvania
PA NY/NJ	Port Authority of New York / New Jersey

PFPA	Pentagon Force Protection Agency
PIN	Personal Identification Number
PIV	Personal Identity Verification
PIV-I	Personal Identity Verification-Interoperable
PL	Public Law
RI	Rhode Island
SBA	Small Business Administration
SOP	Standard Operating Procedure
SSA	Social Security Administration
STRAC	Southwest Texas Regional Advisory Council for Trauma
TWIC	Transportation Workers Identification Credential
UPMC	University of Pittsburg Medical Center
USMS	US Marshal Service
USPP	US Park Police
UT	Utah
VA	Virginia
VIPER	Virginia Interoperability Picture for Emergency Response
WV	West Virginia