



FISCAL YEAR 2014

HOMELAND SECURITY GRANT PROGRAM

**SUPPLEMENTAL RESOURCE: FEDERAL
(AND MUTUAL AID) EMERGENCY RESPONSE
OFFICIAL (F/ERO) CREDENTIALING AND
VALIDATION**



FEMA

1. Purpose

This document is intended to provide Federal Emergency Management Agency (FEMA) grant recipients guidance on:

- Federal (and Mutual Aid) Emergency Response Official (F/ERO) credentialing and validation activities that can be funded through Federal grants
- Technical standards that facilitate interoperability
- Recommendations for planning, coordinating, and implementing credentialing and validation projects.

Grant recipients can obtain additional information by contacting [FEMA-FRACSupport@fema.dhs.gov](mailto:FEMAFRACSupport@fema.dhs.gov).

2. Background

The FEMA National Continuity Programs Directorate manages the F/ERO Credentialing and Validation program. Non-Federal issuers of identity credentials and cyber attributes have expressed a desire to produce identity cards that can technically interoperate with Federal government Personal Identity Verification (PIV) systems and can be trusted by Federal government relaying parties. In response, the Federal Chief Information Officer (CIO) Council released the Personal Identify Verification Interoperability (PIV-I) for Non-Federal Issuers Guidance in May 2009, which provides information for entities wishing to implement an identity credential that is technically interoperable with a Federally-issued PIV card and can be trusted by Federal relaying parties.

The 9/11 Commission and Post-Hurricane Katrina reports cited a lack of credentialing of F/EROs as a major flaw in national preparedness. Title IV of Public Law 110, signed into law August 2, 2007, designates the Federal Emergency Management Agency (FEMA) as the Execution Agent to define a Federal Preparedness standard for credentialing and typing all Federal and Emergency Response Officials (F/EROs), to establish a Federal Preparedness database system for the real-time accountability and awareness of the Federal Preparedness force, and provide written guidance, expertise and technical assistance to Federal, state, local, and Tribal government agencies.

FEMA has re-engineered its enterprisewide Physical Access Control Systems (PACS) to include all FEMA regional and joint field offices (JFOs) to accept and recognize Department of Defense Common Access Cards (CAC), Federal Personal Identity Verification (PIV) credentials, non-Federally issued PIV- interoperable (PIV-I) credentials. The all hazards risk management enabled public safety and security officials to implement hazards risk mitigation best practice solutions and intelligence sharing to make informed decisions for access permissions in a communications-in or -out environment. Demonstrating electronic validation used in incident management can ensure the right people with the right attributes get to the right places at the right times, providing on-scene physical access in a timely manner based on trusted-information and thereby reducing response/recovery/reimbursement times.

3. Applicable Standards

The applicable standards and reference materials for F/ERO credentialing and validation are:

- a. Federal Information Processing Standard (FIPS) 201 – Personal Identity Verification (PIV) of Federal Employees and Contractors
<http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf>
- b. National Incident Management System (NIMS) Guideline for the Credentialing of Personnel – 2011
http://www.fema.gov/pdf/emergency/nims/nims_cred_guidelines_report.pdf
- c. Personal Identity Verification Interoperability, Approved by the Federal CIO Council May 6, 2009,
http://www.idmanagement.gov/documents/PIV_IO_NonFed_Issuers_May2009.pdf

Additional special publications associated with FIPS 201, National Institute of Standards and Technology (NIST) standards, and technical references for are provided in Section 6 of this supplemental guidance.

4. Overview

Achieving the benefits of an integrated enterprise strategy for digital identity is a focus and challenge for State, local, territorial, and Tribal jurisdictions. Currently, states maintain a variety of duplicative identity records, including driver's licenses, benefits cards, emergency response official badges, system passwords, and many others. As a result, a single person carries multiple credentials for a single common purpose: to prove that person's identity as the basis for receiving a privilege. Maintaining these redundant systems is costly, inefficient, and rife with security risks for the State as well as the resident, achieving interoperability across multiple jurisdictions and multiple stakeholder communities of interest. This capability includes FIPS 201/PIV-I credentials and National Doctrine cyber attributes as defined in the National Continuity Policy Implementation Plan (NCPIP), National Response Framework (NRF), National Disaster Recovery Framework (NDRF), National Infrastructure Protection Plan (NIPP), and NIMS for inter-state skill sets for state/local Emergency Response Officials that aligned with Federal Emergency Response Officials.

The F/ERO Credentialing and Validation program encourages interoperable validation services and capabilities for local, state, territorial, tribal, and Federal authorities that will enable interoperability and accountability for the purposes of response, relocation, recovery, and reimbursement. PIV-I credentials can be trusted and interoperable across jurisdictional lines, and used for both physical and logical access.

The mandatory data model elements for a PIV-I credential are:

- A Card Capability Container
- A Cardholder Unique Identifier (CHUID)
- An authentication key (one asymmetric key pair and corresponding certificate)
- A card authentication key (one asymmetric key pair and corresponding certificate)
- Two biometric fingerprints
- Facial image buffer.

The maximum validity of PIV-I certificates is three years. National Institute of Standards and Technology (NIST) 800-78 specifies the algorithms to be used for PIV-I credentials. A link to the NIST standard is provided in Section 6 of this supplemental guidance.

Credentialing and validation 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. Credentialing must be based on an approved source authority's assigned cyber attributes. Cyber attributes must align to the five national doctrines to include:

- Emergency Support Functions (ESFs), as outlined in the National Response Framework
- National Incident Management System (NIMS) skill sets for cross-border mutual aid
- National Infrastructure Protection Plan (NIPP) for Critical Infrastructure/Key Resources (CIKR)
- National Continuity Policy Implementation Plan (NCPIP) for contingency personnel
- National Disaster Recovery Framework (NDRF) recovery support function.

5. Eligible Activities

The section below details eligible F/ERO credentialing and validation activities commonly funded by Federal grants, based on the four common cost categories: Planning, Training, Exercises, and Equipment.

5.1 Planning

Planning activities help to identify and prioritize needs, define capabilities, update preparedness strategies, refine communications plans, allocate resources where they are needed most, and deliver preparedness programs across multiple disciplines and levels of government. Planning is essential for emergency responders using the F/ERO program. In order for the program to be effective, emergency responders providing assistance to a jurisdiction other than their home jurisdiction must have their identity and credentialing information provided to the jurisdiction receiving assistance. Grant recipients are encouraged to use grant funding for planning, which may include:

- Working group meetings, workshops, and conferences relating to emergency responder credentialing and validation
- Compiling data to enter into an emergency responder repository
- Coordinating with other state, local, territorial, and tribal partners to ensure interoperability among existing and planned credentialing and validation systems and equipment
- Planning to incorporate emergency responder identity and credential validation into training and exercises
- Planning for credentialing and validation equipment procurement.

5.2 Training

Recipients are encouraged to allocate Federal grant funds to support credentialing and validation training. This may include training relating to policies and governance, or training on how to operate the equipment. Funds used for training pertains to the costs associated with virtual and in-person training. Funds used for travel related to training can include accommodations, transportation, meals, and mileage. These costs must be reasonable and conform to the General Services Administration (GSA) schedule regarding all per diem travel expenses.

5.3 Exercises

Exercises should be used to both demonstrate and validate skills learned in training and to identify training gaps and gaps in capabilities. To the extent possible, exercises should include participants from multiple jurisdictions and agencies with varied cyber-attributes such as emergency management, emergency medical services, law enforcement, fire, hospital officials, and other disciplines, as appropriate.

All Federally-funded exercises must be managed and executed in accordance with the Homeland Security Exercise and Evaluation Program (HSEEP). The HSEEP library provides guidance for exercise design, development, conduct, and evaluation of exercises, as well as sample exercise materials. The HSEEP library can be found at:

<https://hseep.dhs.gov>.

All Federally-funded exercises must be NIMS-compliant. On February 28, 2003, the President issued Homeland Security Presidential Directive (HSPD-5), Management of Domestic Incidents, which requires all Federal departments and agencies to adopt NIMS and to use it in their individual incident management programs and activities, including all preparedness grants. Grantees should review the NIMS requirements on the following site: <http://www.fema.gov/emergency/nims/index.shtm> and ensure that all Federally-funded training and exercise activities are NIMS-compliant.

5.4 Equipment

Mobile validation devices, PIV-I cards, card printer stations, transparent readers, fingerprint capture devices, facial image capturing cameras, and other equipment supporting

credentialing and validation is developed, produced, and distributed by multiple vendors. FEMA does not endorse any specific vendors or any specific piece of equipment. A list of equipment meeting FIPS 201 standards is available in the United States General Service Administration (GSA's) approved products list. <http://fips201ep.cio.gov/apl.php>

6. References

- Public Law 110-53, Implementing Recommendations of the 9/11 Commission Act of 2007, Title, IV, August 3, 2007, <http://intelligence.senate.gov/laws/pl11053.pdf>
- Homeland Security Presidential Directive (HSPD)-12, Personal Identity Verification (PIV) Credential, August 27, 2004, http://www.dhs.gov/xabout/laws/gc_1217616624097.shtm#1
- Cyberspace Policy Review (OMB M-11-11), May 5, 2009, <http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-11.pdf>
- National Security Presidential Directive (NSPD)-51/Homeland Security Presidential Directive (HSPD)-20, National Continuity Public and Private Sector Interoperability, <http://www.fas.org/irp/offdocs/nspd/nspd-51.htm>
- Presidential Policy Directive (PPD)-8, National Preparedness, March 30, 2011, <http://www.dhs.gov/presidential-policy-directive-8-national-preparedness>
- FBCA CP X.509 Certificate Policy for the Federal Bridge Certificate Authority (FBCA) http://www.idmanagement.gov/fpkipa/documents/FBCA_CP_RFC3647.pdf
- FICAM Roadmap Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance http://www.idmanagement.gov/documents/FICAM_Roadmap_Implementation_Guidance.pdf
- FIPS 140-2 National Institute of Standards and Technology Federal Information Processing Standards 140-2, Security Requirements for Cryptographic Modules <http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>
- FIPS 180 National Institute of Standards and Technology Federal Information Processing Standards 180, Secure Hash Standard (SHS) http://csrc.nist.gov/publications/fips/fips180-3/fips180-3_final.pdf
- ISO/IEC 7816 International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC) 7816, Identification Cards – Integrated Circuit Cards Parts 1-15 http://www.iso.org/iso/iso_catalogue.htm
- ISO/IEC 14443 International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC) 14443, Identification cards -- Contactless integrated circuit cards -- Proximity cards Parts 1-4 http://www.iso.org/iso/iso_catalogue.htm
- NIST SP 800-21 National Institute of Standards and Technology Special Publication 800-21, Guideline for Implementing Cryptography in the Federal Government http://csrc.nist.gov/publications/nistpubs/800-21-1/sp800-21-1_Dec2005.pdf
- NIST SP 800-37 National Institute of Standards and Technology Special Publication 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems <http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf>
- Public Law (PL) 110-53: Implementing Recommendations of the 9/11 Commission Act of 2007, Title, XVI, Section: 1615, August 3, 2007,

- <http://intelligence.senate.gov/laws/pl11053.pdf>
- Executive Order (E.O.) 13407, *Public Alert and Warning System*, dated June 26, 2006. <http://www.fas.org/irp/offdocs/eo/eo-13407.htm>
 - Executive Order (E.O.) 13636, *Improving Critical Infrastructure Cybersecurity*, dated February 12, 2013. <http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity>
 - Presidential Policy Directive -21 (PPD-21): *Critical Infrastructure Security and Resilience*, dated February 12, 2013. <http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>
 - NIMS Guideline for the Credentialing of Personnel: http://www.fema.gov/pdf/emergency/nims/ng_0002.pdf
 - NIST SP 800-53 National Institute of Standards and Technology Special Publication 800-53, *Security Controls for Federal Information Systems and Organizations* http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf
 - NIST SP 800-57 National Institute of Standards and Technology Special Publication 800-57, *Recommendation for Key Management* http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57-Part1-revised2_Mar08-2007.pdf
 - NIST SP 800-63-1 National Institute of Standards and Technology Special Publication 800-63-1, *Electronic Authentication Guidance* <http://csrc.nist.gov/publications/PubsSPs.html>
 - NIST SP 800-73 National Institute of Standards and Technology Special Publication 800-73, *Interfaces for Personal Identity Verification (4 Parts)* <http://csrc.nist.gov/publications/PubsSPs.html>
 - NIST SP 800-76 National Institute of Standards and Technology Special Publication 800-76, *Biometric Data Specification for Personal Identity Verification*, http://csrc.nist.gov/publications/nistpubs/800-76-1/SP800-76-1_012407.pdf
 - NIST SP 800-78 National Institute of Standards and Technology Special Publication 800-78, *Cryptographic Algorithms and Key Sizes for Personal Identification Verification (PIV)* <http://csrc.nist.gov/publications/nistpubs/800-78-3/sp800-78-3.pdf>
 - NIST SP 800-79 National Institute of Standards and Technology Special Publication 800-79, *Guidelines for Accreditation of Personal Identity Verification Card Issuers* <http://csrc.nist.gov/publications/nistpubs/800-79-1/SP800-79-1.pdf>
 - NIST SP 800-85 National Institute of Standards and Technology Special Publication 800-85, *PIV Middleware and PIV Card Application Conformance Test Guidelines* <http://csrc.nist.gov/publications/PubsSPs.html>
 - NIST SP 800-116 National Institute of Standards and Technology Special Publication 800-116, *A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)* <http://csrc.nist.gov/publications/nistpubs/800-116/SP800-116.pdf>
 - NIST SP 800-131 National Institute of Standards and Technology Special Publication 800-131, *Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths* <http://csrc.nist.gov/publications/nistpubs/800-131A/sp800-131A.pdf>
 - NISTIR 7539 National Institute of Standards and Technology Internal Report *Symmetric Key Injection onto Smart Cards*

http://csrc.nist.gov/publications/nistir/ir7539/nistir-7539-Symmetric_key_injection_final.pdf

- OMB M-04-04 Office of Management and Budget Memorandum M-04-04, E-Authentication Guidance for Federal Agencies
<http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf>