

PIV-I/FRAC Technology Transition Working Group

The Problem

Local and State emergency response officials must be able to collaborate to ensure the public's safety. However, for this to happen, many identity management challenges must be overcome. While Federal agencies are rapidly deploying secure common identification standards based on guidance from the White House and other Federal entities, State and local emergency response officials are working to establish a Personal Identity Verification-Interoperable (PIV-I) / First Responder Authentication Credential (FRAC) standard that is interoperable between local, State, and Federal levels.

In the past, physical access to sites would be granted based on personal judgment, rather than on hard identity data. Logical access to computer systems required only a username and password. Today, Federal Information Processing Standard (FIPS) 201, Office of Management and Budget (OMB) memorandum M-05-24, and other White House guidance specify that access to all Federal computer systems requires secure forms of identification based on smart card technology and identity-proofing procedures. Local, State, and Federal stakeholders need to collaborate to solve these identity management challenges.

Working Group Goals

The Cyber Security Division (CSD) within the Science & Technology (S&T) Directorate, the FEMA Office of the 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 PIV-I/FRAC Technology Transition Working Group (TTWG). The TTWG is composed of Federal, State and local emergency management representatives, many of whom have already implemented innovative and secure identity-management solutions in their own jurisdictions.

The purposes of the working group include:

- Provide Federal policy makers with a unified state emergency manager perspective on Federal/Emergency Response Official (F/ERO) attributes
- Baseline current identity infrastructure and best practices to share with stakeholders
- Identify technological gaps where CSD can provide test bed research and development support
- Share information: State-to-State, State-to-Federal, Federal-to-State

State and Local Participants

- Colorado
- Maryland
- Virginia
- District of Columbia
- Missouri
- Southwest Texas
- Pennsylvania
- Chester County, PA
- Pittsburgh, PA
- West Virginia
- Hawaii
- Rhode Island

The working group is focused on exploring PIV-I credentials as the standard that enables interoperability between local and State emergency response officials. PIV-I is a trusted identity and credentialing standard developed by the Federal Government for non-Federal issuers. Non-Federal entities that elect to conform to the PIV-I standard will be trusted by and interoperable with Federal agencies at assurance levels 1-3, and potentially at level 4. These authentication assurance levels are described fully by OMB M-04-04.

Value

Identity management is a key enabling technology for all homeland security communications. This working group will ensure that identity management technologies are rapidly deployed in states, while ensuring that the S&T CSD Identity Management Program is performing research that meets end-user needs. State and local emergency responders are key stakeholders, and need secure, role-based methods of accessing Federal information.