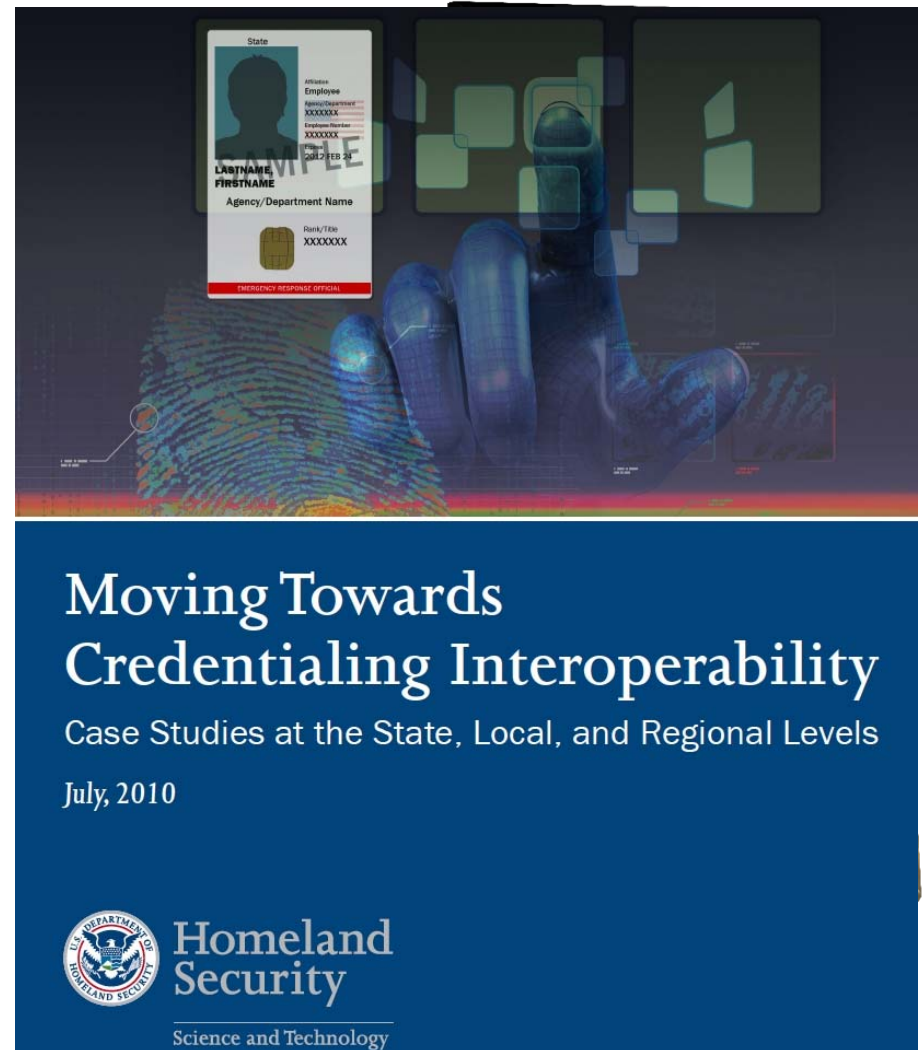Security in knowledge

INCIDENT SCENE AUTHORIZED ACCESS USING A MOBILE DEVICE

Karyn Higa-Smith

DHS Science and Technology Directorate

Homeland Security Advanced Research Projects Agency
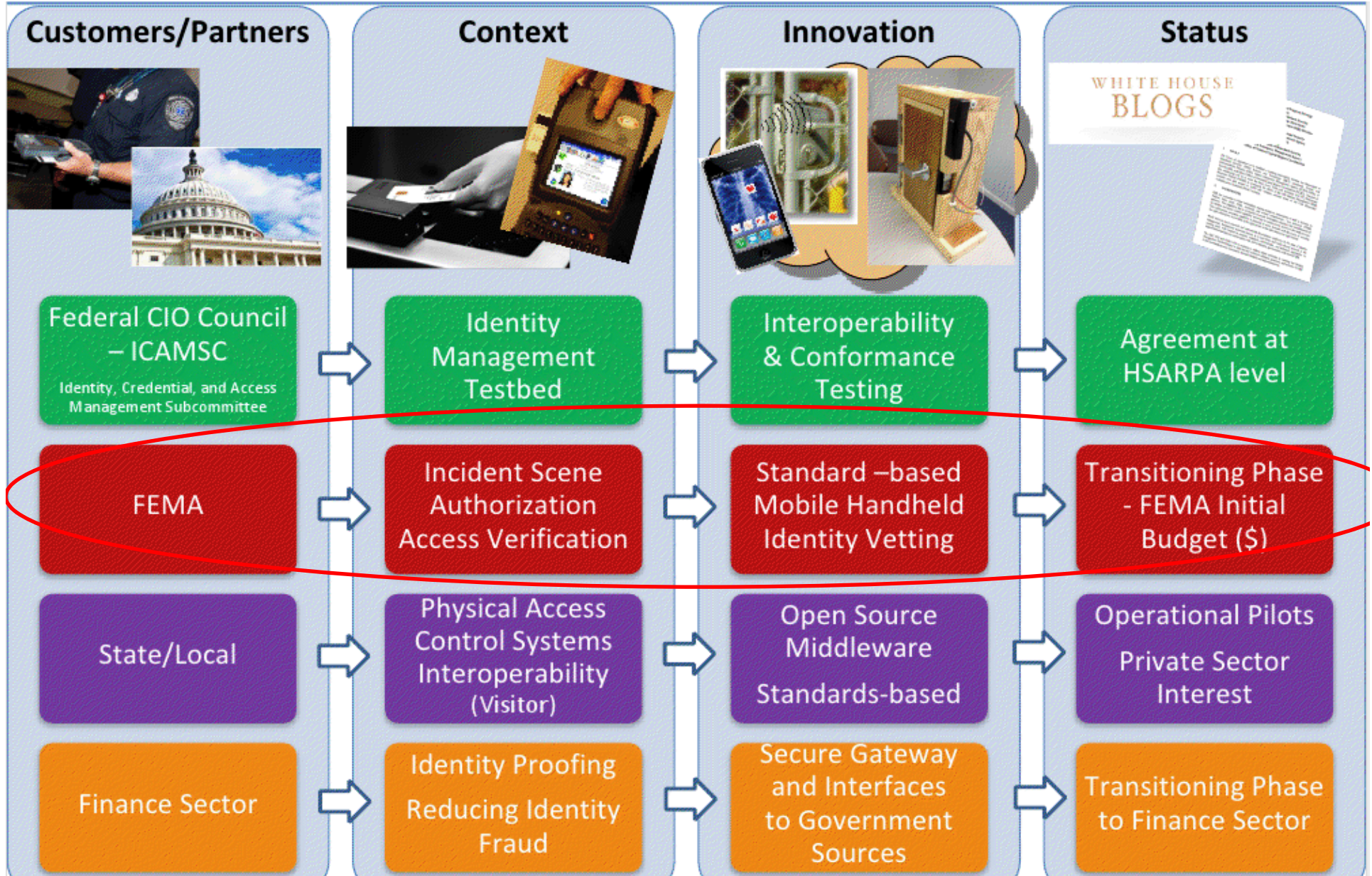
CyberSecurity Division

RSACONFERENCE**2013**

Session ID: PNG-F42A

Session Classification: Intermediate

Daunting Task of Emergency Response

► **Credentialing Challenges**
  ► Multi-jurisdiction coordination to large-scale disasters
  ► Stove-piped credentials
  ► Lack of trust and interoperability
  ► Too many credentials!
  ► Insecure/isolated physical and logical access
► Current Issue: No standard credential to identify CIKR responders

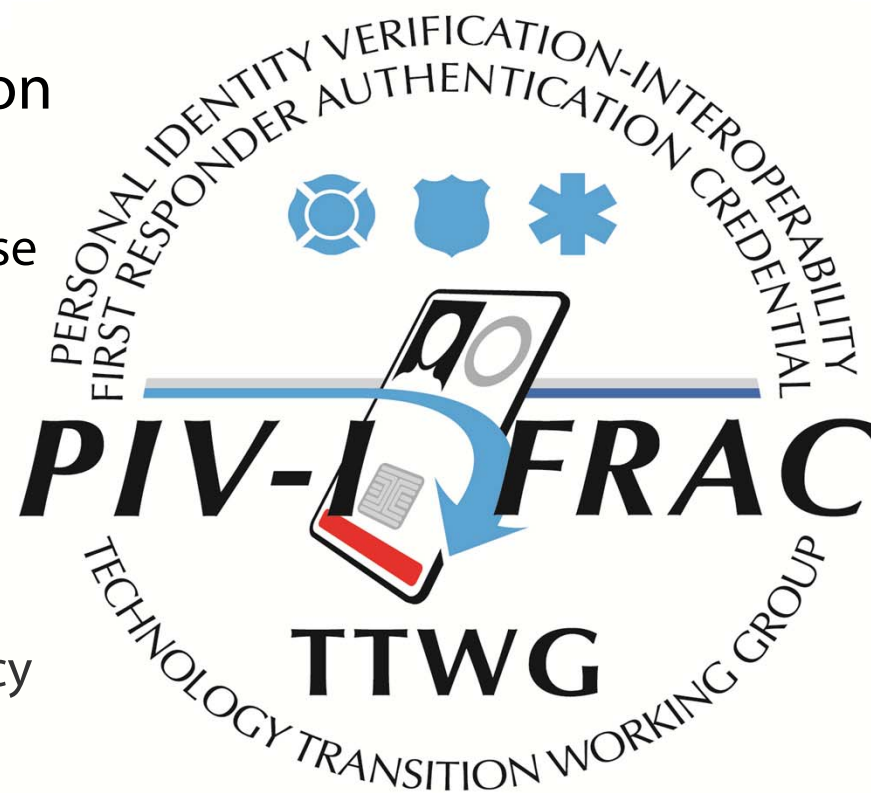**CIKR: Critical Infrastructure and Key Resources**

Moving Towards Credentialing Interoperability
Case Studies at the State, Local, and Regional Levels

July, 2010

Homeland Security
Science and Technology

Science and Technology CyberSecurity

R&D Identity Management Program

Customers/Partners	Context	Innovation	Status
Federal CIO Council – ICAMSC (Identity, Credential, and Access Management Subcommittee)	Identity Management Testbed	Interoperability & Conformance Testing	Agreement at HSARPA level
FEMA	Incident Scene Authorization Access Verification	Standard –based Mobile Handheld Identity Vetting	Transitioning Phase - FEMA Initial Budget ($)
State/Local	Physical Access Control Systems Interoperability (Visitor)	Open Source Middleware Standards-based	Operational Pilots Private Sector Interest
Finance Sector	Identity Proofing Reducing Identity Fraud	Secure Gateway and Interfaces to Government Sources	Transitioning Phase to Finance Sector

S&T Technology Transition Working Group

- ▶ **PIV-I/FRAC Technology Transition Working Group (TTWG)**
  - ▶ Public Safety/Emergency Response
  - ▶ Security
  - ▶ Federated Identity for First Responders
    - ▶ National standard, Interoperable, and trusted ID credential
  - ▶ One voice from the TTWG to policy makers
  - ▶ Sharing lessons learned
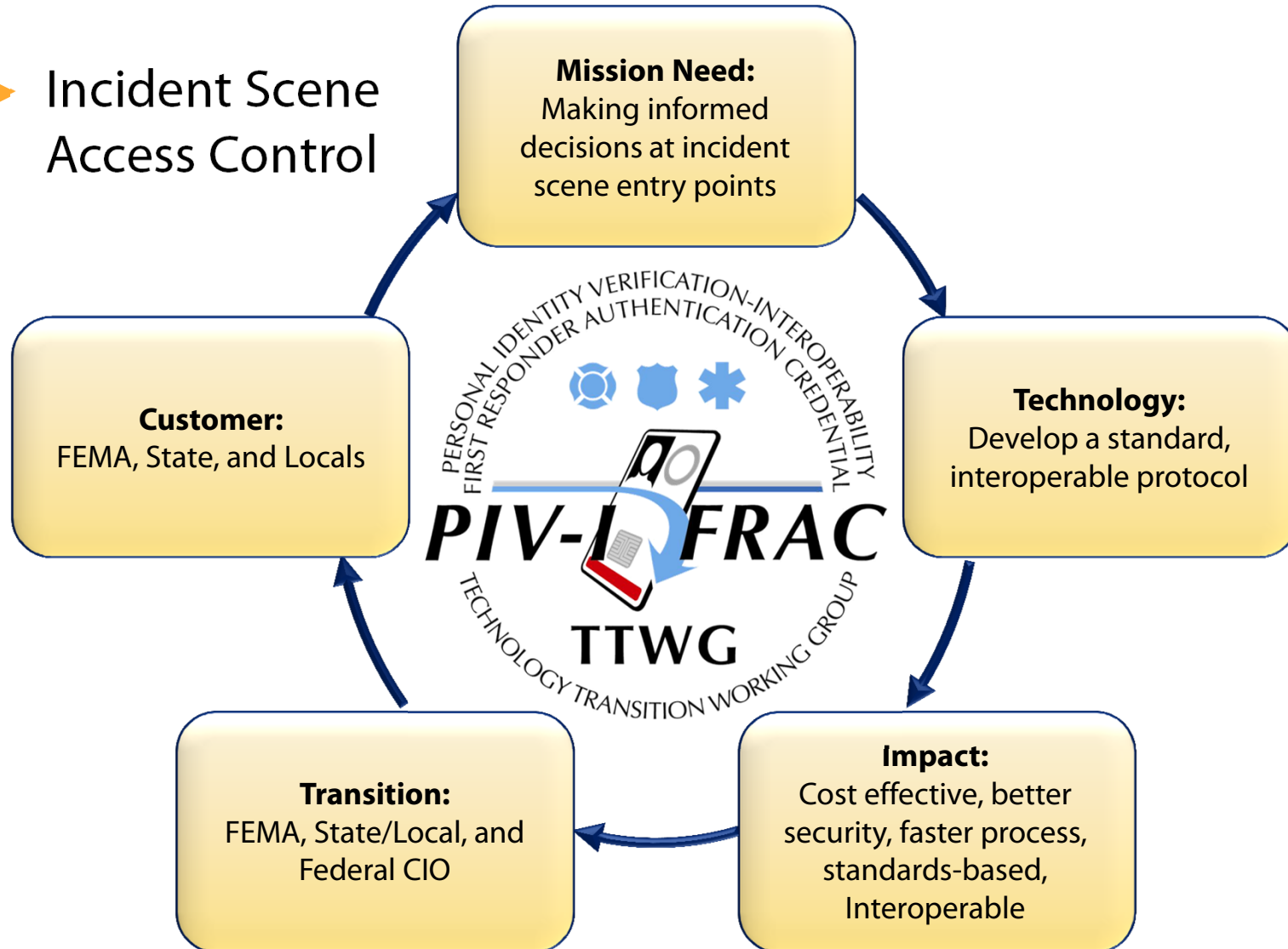 - ▶ **Provide innovative, Cost-effective solutions**

PERSONAL IDENTITY VERIFICATION-INTEROPERABILITY
FIRST RESPONDER AUTHENTICATION CREDENTIAL
PIV-I/FRAC
TTWG
TECHNOLOGY TRANSITION WORKING GROUP

Science and Technology
CyberSecurity

Hurricane: PRICE OF CREDENTIALING

Credentialing Cost	Reactive	Proactive
PIV-I Credential @ $25/3,000 personnel/year	$0	$75,000
400 **Bucket trucks** @ $3,000 delayed personnel/per day	$1,200,000	$0
3,000 deployed **personnel** @ $200 per day	$600,000	$0
Power restoration of 200,000 **delayed** one day @ $5 per day	$1,000,000/community	$0
Total cost per large scale incident	$2,800,000/disaster	$0

Mike McAllister
Deputy Secretary of Veterans Affairs and Homeland
Security
Office of Governor Robert F. McDonnell
Commonwealth of Virginia

Science and Technology
CyberSecurity

Research and Development (R&D)

▶ Incident Scene Access Control

Mission Need:
Making informed decisions at incident scene entry points

Customer:
FEMA, State, and Locals

PERSONAL IDENTITY VERIFICATION-INTEROPERABILITY
FIRST RESPONDER AUTHENTICATION CREDENTIAL

PIV-I FRAC

TTWG

TECHNOLOGY TRANSITION WORKING GROUP

Technology:
Develop a standard, interoperable protocol

Transition:
FEMA, State/Local, and Federal CIO

Impact:
Cost effective, better security, faster process, standards-based, Interoperable

Science and Technology
CyberSecurity

INCIDENT SCENE ACCESS CONTROL MISSION

Federal

State/Local/Tribal

Critical Infrastructure

Volunteers

> S&T providing an open standard solution for the FEMA and State/Local emergency response mission:
>> Provide **informed decision making tool** for authorized access using a mobile device
>> Single record or multiple record operations (batch attribute transmission)

- ✓ "Give me a list of all Users with Attribute X, Y, and Z"
- ✓ "Give me all the **Emergency Support Function** (ESF) attributes of User X"
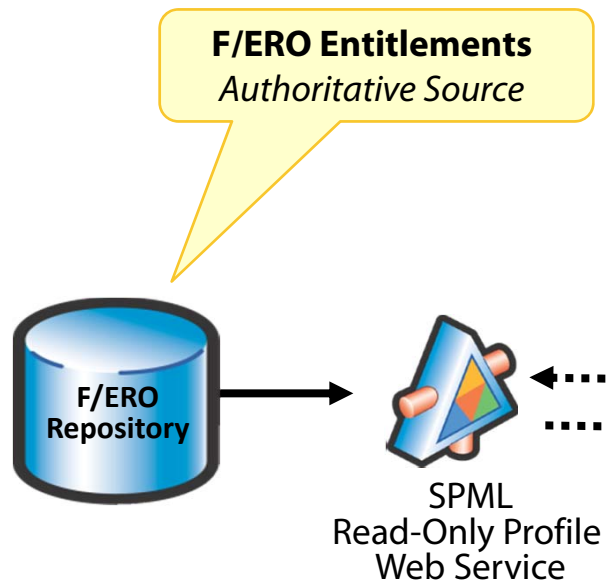- ✓ "Give me all authorized users for the incident"

Science and Technology
CyberSecurity

INCIDENT SCENE ACCESS CONTROL PILOT

DHS S&T IdM Testbed

State and Local

F/ERO Entitlements
Authoritative Source

SPML Read-Only
Request

1. **DHS, FEMA (PIV)**
2. *DOD (CAC)*
3. *Chester Co PA (PIV-I)*

Unique Identifier

F/ERO Repository

SPML
Read-Only Profile
Web Service

Field Station

Handheld

Credential
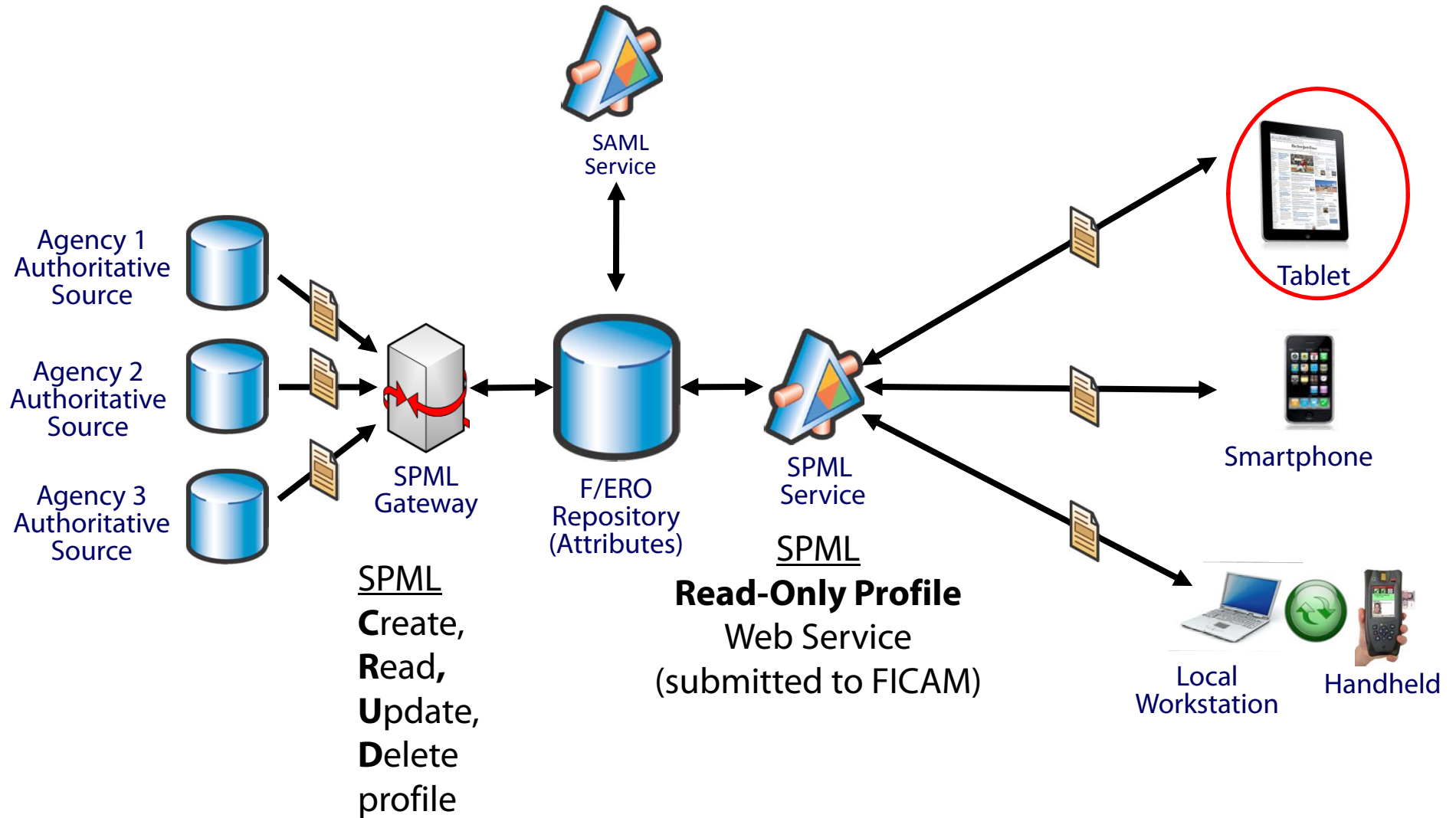
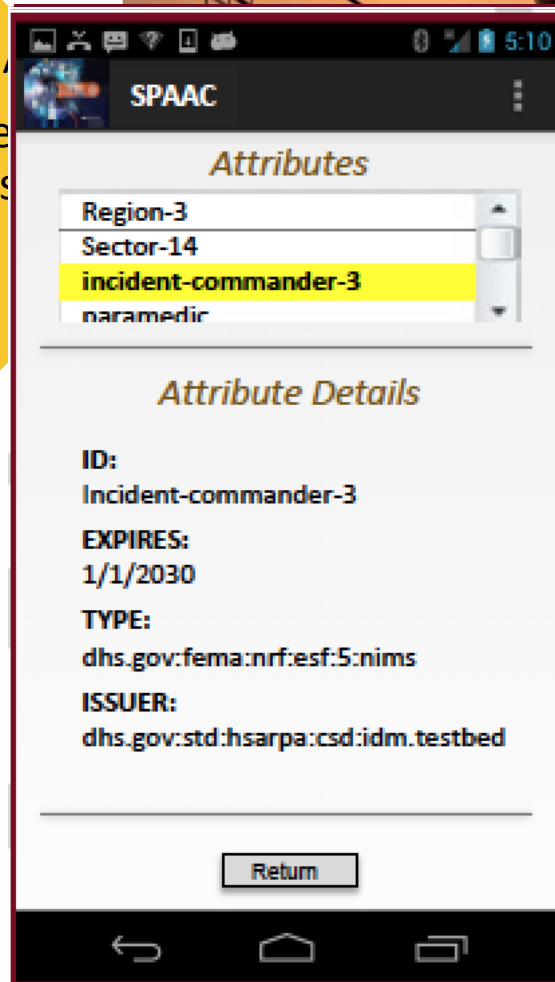**NO COMMUNICATIONS**

SPML Read-Only
Response
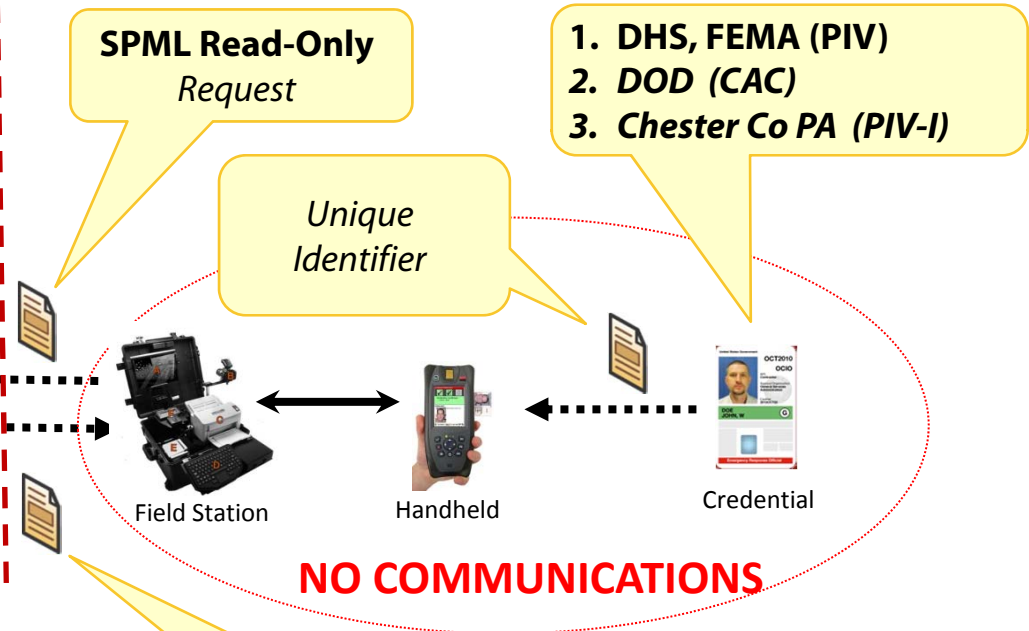
PIV: Personal Identity Verification
PIV-I: PIV– Interoperability
CAC: Common Access Card
OASIS: Organization for the Advancement of Structured Information Standards
F/ERO: Federal/Emergency Response Official
SPML: Service Provisioning Markup Language

Science and Technology
CyberSecurity

END-TO-END TOOL USING STANDARDS

SAML
Service

Agency 1
Authoritative
Source

Agency 2
Authoritative
Source

Agency 3
Authoritative
Source

SPML
Gateway

F/ERO
Repository
(Attributes)

SPML
Service

Tablet

Smartphone

Local
Workstation

Handheld

SPML
Create,
Read**,**
Update,
Delete
profile

SPML
Read-Only Profile
Web Service
(submitted to FICAM)

Science and Technology
CyberSecurity

Smart Phone Attribute-based Access Control (SPAAC)

Fire
Police
Medical

Bucket

FEMA
Other
Feds

SPAAC

Attributes

Region-3
Sector-14
incident-commander-3
paramedic

Attribute Details

ID:
Incident-commander-3

EXPIRES:
1/1/2030

TYPE:
dhs.gov:fema:nrf:esf:5:nims

ISSUER:
dhs.gov:std:hsarpa:csd:idm.testbed

Return

Samsung Galaxy Nexus smartphone
Apps screen

RSACONFERENCE2013

Science and Technology
CyberSecurity

Technology Transition

▶ Transition to TTWG:

▶ **FEMA is adopting the standard specifications for** the F/ERO Repository and attribute model

▶ **State and local** users will utilize the model for their own repositories

▶ The architecture specifications will be transitioned to **Federal CIO for government-wide** adoption of the open standard-based protocol

▶ The capability may be used across other domains for control physical locations such as port security

Local and State Participants

➢ Colorado

➢ Maryland

➢ Virginia

➢ District of Columbia

➢ Missouri

➢ Southwest Texas

➢ Pennsylvania

➢ Chester County, PA

➢ Pittsburgh, PA

➢ West Virginia

➢ Hawaii

➢ Rhode Island

➢Nevada

Science and Technology
CyberSecurity

CAPABILITY IMPACT

"The standard technology developed by S&T will save me an initial outlay of $365,000 and then $41,500 per year on operations and maintenance." –Chester County, Pennsylvania Emergency Management

No Solution	• Delayed access • Risk of wrongful permissions
Proprietary Solution	• High cost due to license expense • Since it is not interoperable, partners need to buy into proprietary vendor solution
S&T Solution	• Standard communications allow for transactions across multiple platforms • Low cost allows for widespread adoption • Provides real-time ability to electronically validate users

Science and Technology
CyberSecurity

RESOURCES

▶ Websites

   ▶ http://www.ahcusa.org/PIV-I%20TTWG.htm

   ▶ https://www.cyber.st.dhs.gov/idmdp.html

   ▶ http://www.idmanagement.gov/documents/BAE_v2_Ov
erview_Document_Final_v1.0.0.pdf

Science and Technology
CyberSecurity

Karyn Higa-Smith

Program Manager

DHS Science and Technology Directorate

HSARPA Cybersecurity Division

Karyn.Higa-Smith@dhs.gov

202.254.5335

Security in knowledge