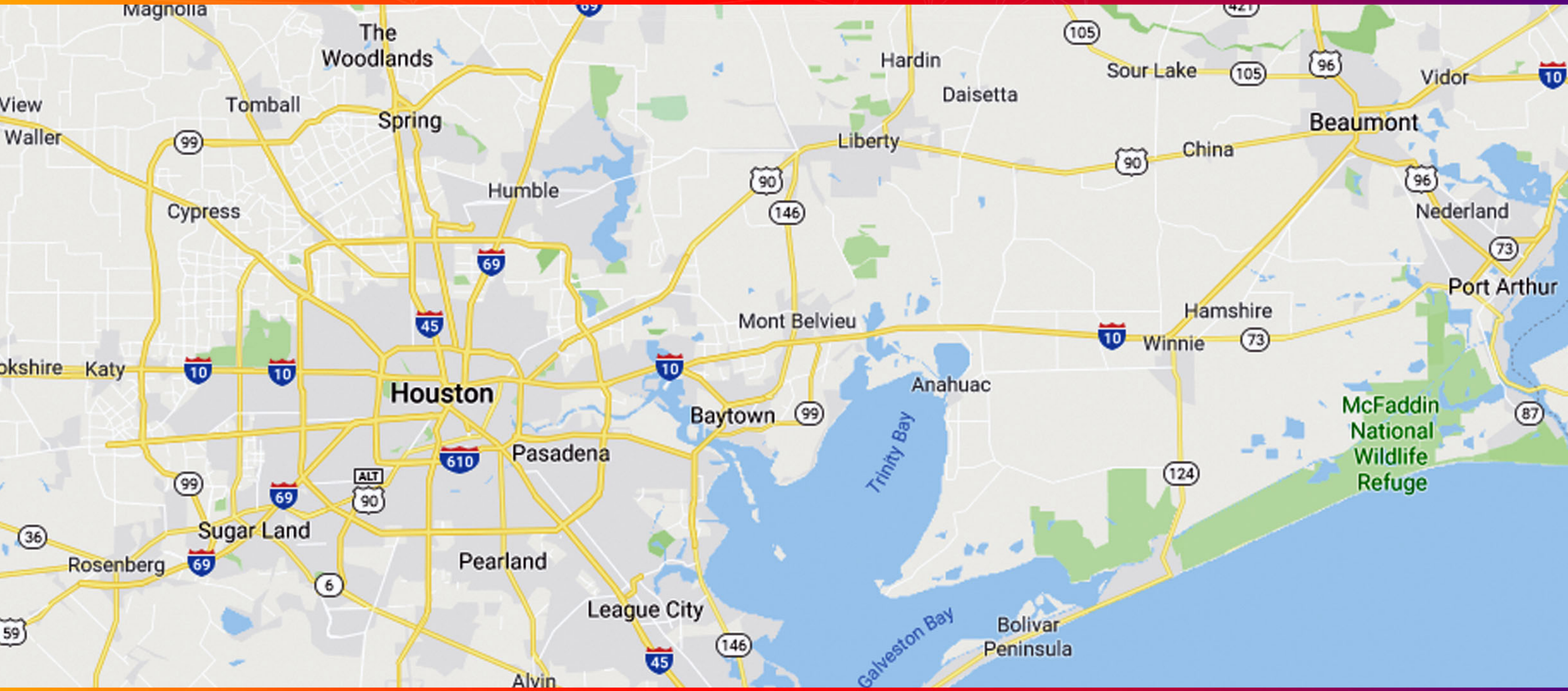
# Southeast Texas First Responder Identity, Credential & Access Management (ICAM) Plan



M4bility
Public Safety

# Southeast Texas ICAM Workshop Summary

Produced For: Southeast Texas Regional Advisory Council (SETRAC)

Date Published: August 30, 2019

Prepared by: Mobility 4 Public Safety

Principle Author: Niki Papazoglakis

Contributing Authors: Chris Collier, SETRAC
Rick Retz, City of Houston
Michael Jumonville, Mobility 4 Public Safety

Please send comments to: Niki Papazoglakis
Principal
Mobility 4 Public Safety
1307 Waugh Dr #787
Houston, TX 77019
Phone: 346-291-5575
Email: niki@mobility4ps.com

# Table of Contents

# Executive Summary

Identity, Credentialing and Access Management (ICAM) is a broad term that encompasses a variety of challenges for verifying the identity of first responders and other personnel authorized to access physical locations and virtual systems in the performance of public safety operations.

Historically, the management of physical access control systems (PACS) and logical access to information systems have been separate and distinct functions typically managed by different organizational units. Technology is evolving to provide the ability to:

1. Utilize standard processes for verifying identity across departments and jurisdictions
2. Issue credentials which provide authorized access to both physical and logical systems
3. Build frameworks to trust the identities and credentials of practitioners across organizations

These advancements offer tremendous opportunities to improve security and information sharing across departments.

As more buildings are automating access control and implementing other "smart building" technologies, the management of physical and virtual access control systems is converging. Meanwhile, the availability of reliable mobile broadband is allowing public safety agencies to adopt mobile technologies at an accelerated pace. At the same time that public safety is becoming more electronic, automated and mobile, hackers and terrorists are also becoming more sophisticated and posing even greater threats.

It is critical that public safety leaders understand the importance of developing ICAM plans and implementing systems that meet industry standards and best practices to ensure the safety and security of first responders and the communities they serve.

Due to the rapid technology advancement in recent years and the complexity of ICAM, industry efforts to develop solutions to address these problems have been fragmented. There are arguably four primary efforts leading the innovation and thought leadership in public safety cybersecurity:

1. **National Institute of Standards and Technology (NIST) National Cybersecurity Center of Excellence (NCCoE) -** NCCoE efforts have focused predominantly on building an open framework for implementing standards-based technologies for authentication, federation and single sign-on.
2. **Department of Homeland Security (DHS) Emergency Communications Division (ECD) & SAFECOM -** the DHS/SAFECOM work has centered around the development of the Trustmark Framework to build a federated model for public safety agencies to establish trust relationships to share identities across agencies and manage authorized access to information systems.
3. **DHS Science & Technology Directorate (S&T) -** DHS S&T has conducted extensive research in developing an ICAM framework that utilizes an exchange hub to manage identities and credentials for secure information sharing. This work has focused largely on developing repeatable, low-cost, standards-based solutions for smaller public safety agencies with limited internal IT resources.
4. **Federal Emergency Management Agency (FEMA) -** The FEMA ICAM Working Group has been leading the adoption of the Personal Identity Verification Interoperable (PIV-I) card to allow non-federal agencies to follow the federal processes, guidelines, and standards for identity proofing and credentialing to issue physical ID cards which can allow federal and non-federal government personnel to share secure access to facilities and information systems.

## Problem Statement

First Responders in the H-GAC region currently have no mechanism for confirming the identity of authorized response personnel in multi-jurisdictional / multi-discipline incident response. Terrorists are increasingly impersonating first responders and using “cloned” emergency vehicles to carry out acts of terrorism around the world, so having the ability to verify identity and restrict or permit access to buildings, incident scenes and information is vital to our community safety.

Credentialing is essential to the emergency response community in that it ensures and validates the identity and attributes (e.g., affiliations, skills, or privileges) of individuals or members of response teams. Having established standards allows the community to plan for, request, and have confidence in resources deployed from other jurisdictions for emergency assistance. Credentialing ensures that personnel resources match requests, and it supports effective management of deployed responders. With no current responder credentialing system, approved ICAM plan, guidelines, or common approach implemented in the Houston area leaves the region’s jurisdictions vulnerable for terrorist attacks. The development of a regional ICAM plan will address the region’s risk by implementing - through the development of a systematic region-wide approach - a plan for addressing ICAM and credentialing of first responders; giving law enforcement and authorities the ability to authenticate credentials and control access when needed to critical sites, incidents sites, and critical information for disaster response.

There is not a regional identity management approach or strategy universally accepted or implemented that provides a pathway for members of public safety agencies to have trusted access to critical information at either their desktops or on mobile devices. Law enforcement, justice, and public safety entities need access to this information on a regular basis from mobile devices, and the methods to access information need to be low-cost, simple, and standardized. Today, Individual jurisdictions have identification systems in place however there is no regional credentialing system or plan in place that crosses all disciplines/jurisdictions meeting United States Federal Government FIPS-201 standards; with capabilities and oversite needed to implement/manage a regional FRAC program; additionally not meeting NIMS Credentialing Criteria.

In spite of the successes in improving information sharing, identity verification, and access management both physically and digitally, great difficulty still exists in making the connection to the last mile—primarily the officer, deputy sheriff, firefighter, and paramedic in a vehicle or in the field. The access to critical information and the ability to verify responders on the ground enhances the region’s capability to prevent, protect against, and respond to high profile incidents or suspected acts of terrorism. A regional ICAM plan will help reduce identified gaps by:

- Fostering effective region-wide identity and access management
- Aligning regional agencies around common identity and access management practices
- Reducing the identity and access management burden for individual agencies by fostering common interoperable approaches
- Ensuring alignment across all identity and access management activities that cross individual agency boundaries
- Collaborating with external identity management activities through inter-agency cooperation to enhance interoperability
- Identity proofing of network users—the process of verifying a user’s identity

# Regional ICAM Plan: Program Summary

**Step 1: Conduct Regional ICAM Educational Seminar**

Hold an educational seminar involving regional stakeholders, for the purpose of generating involvement and consensus for a Regional ICAM Plan.

Invite Subject Matter Experts (SME) from STRAC, FEMA, DHS, NCCoE, FTI, and other state/local executives with successful ICAM programs to showcase best practices.

**Step 2: Gain executive support for Regional ICAM Initiative**

Conduct executive meetings with key stakeholder organizations
Ensure representation of jurisdictions and disciplines throughout the region

**Step 3: Assemble Regional ICAM Working Group**

<u>Executive Steering Committee</u>

- Develop priorities for the region (i.e. changing policies, adopting technologies, standardizing purchasing/procurement procedures, legislative updates, etc.);

<u>Technical Working Group</u>

- Support regional education/outreach
- Conduct data collection for existing systems

**Step 4: Develop a Baseline Regional ICAM Plan**

Tactical Actions for Individual Departments/Jurisdictions

- Adopt federally approved ICAM standards & protocols
  - Multi-Factor Authentication (MFA)
    - Personal Identity Verification Interoperable (PIV-I)
    - Fast Identity Online (FIDO)
  - Single Sign-On
    - OAuth
  - Federation
    - Security Assertion Markup Language (SAML)
    - OpenID Connect
- Provide standardized ICAM procurement language for new systems
- Identify and apply for eligible grant funding

Strategic Planning - Regional Coordination for Sharing First Responder Identities & Credentials

- Define <u>**WHAT**</u> information organizations want to share
- Identify <u>**WHO**</u> organizations want to share with
- Develop a regional framework for <u>**HOW**</u> organizations share identities and information

# Technology Requirements: Standards-Based Approach

Homeland Security Presidential Directive 12 (HSPD-12) mandates a standard for a secure and reliable form of identification to be used by all Federal employees and contractors. Signed by President George W. Bush in August 2004, HSPD-12 initiated the development of a set of technical standards and issuance policies (Federal Information Processing Standard 201 [FIPS 201]) that create the Federal infrastructure required to deploy and support an identity credential that can be used and trusted across all Federal agencies for physical and logical access.

The federal government's standardization on PIV cards and infrastructure has produced numerous benefits for federal agencies and owners of critical infrastructure including:

1. Enhancing secure access to facilities and information systems
2. Streamlining access procedures to secure facilities for authorized personnel
3. Reducing the cost of PIV cards to be competitive with other MFA technologies

These same benefits are being leveraged by state and local organizations around the country. Cities like San Antonio, TX, and Victoria, TX have implemented multi-agency, multi-jurisdictional ICAM systems that have produced other benefits including a variety of operational efficiencies and cost savings.

For departments wanting to move to a standards-based MFA solution for Logical Access Control Systems (LACS) and enhance Physical Access Control Systems (PACS) to allow authorized First Responders access as operationally necessary, investment in PIV-I technology offers security, control, compliance, flexibility, and interoperability.

The federal government commits significant resources in vetting products and maintaining lists of compliant products and product combinations. The Approved Products List (APL)[1] provides federal agencies with products and services that have been approved for FICAM implementation based on rigorous security vulnerability and interoperability testing performed by the FIPS 201 Evaluation Program[2].

The Federal government's standardization around the policies, procedures, and technologies to build a trusted federal identity framework over the last 15 years has yielded irrefutable benefits. On May 21, 2019, the Executive Office of the President, Office of Management and Budget (OMB) issued OMB Memorandum M-19-17 [3]updating the Federal Government's ICAM policy to expand guidance to support evolving technology requirements.

> *HSPD-12 remains the Government-wide policy for the promulgation of standards-based, secure, and reliable forms of identification issued by the Federal Government to its employees, contractors, and other enterprise users. Additionally, Federal Information Processing Standard (FIPS) 201-2, Personal Identity Verification (PIV) of Federal Employees and Contractors (or successive version), remains the Government-wide standard for common identification, as called for by HSPD-12. In accordance with this standard, NIST guidelines, and Office of Personnel Management (OPM) requirements, a PIV credential is the aggregate output of the processes used for identity proofing,*

[1] https://www.idmanagement.gov/approved-products-list/

[2] https://www.idmanagement.gov/fips201

[3] https://www.whitehouse.gov/wp-content/uploads/2019/05/M-19-17.pdf

> *vetting, and authoritatively binding the identity of a human credential holder to an authenticator. However, as technology evolves, the Government must offer flexible solutions to meet changing technology needs and shift the focus from managing the lifecycle of credentials to the lifecycle of identities.*

This memorandum emphasizes the importance of adhering to the established and proven PIV standard for common identification while also enhancing flexibility to adopt other compatible, standards-based solutions to support evolving technology requirements.

> ***IV. Shifting the Operating Model beyond the Perimeter***
> *The interwoven technical architecture of the Federal Government creates complexity in managing access to resources, safeguarding networks, and protecting information. While hardening the perimeter is important, agencies must shift from simply managing access inside and outside of the perimeter to using identity as the underpinning for managing the risk posed by attempts to access Federal resources made by users and information systems. To ignite adoption of this new mindset around ICAM capability deployment across the Federal Government, each agency must harmonize its enterprise-wide approach to governance, architecture, and acquisition.*

As enterprises are becoming more mobile, IT and cybersecurity personnel must evaluate ICAM technologies that support physical, logical and mobile access. As these technologies converge, a regional plan should address the various requirements to include multiple platforms within an interoperable ICAM framework.

The architecture of mobile technologies differs from traditional Windows-based systems. And the smaller form factors of phones and tablets are not as conducive to utilizing an ID card to provide multi-factor authentication. Considering all of these factors along with recent federal guidance, below is a list of the best practices for moving towards a regional ICAM framework for public safety

**Identity**

- Leverage the trusted identity vetting process of the FIPS 201-2 standard for common identification of all First Responders throughout the region

**Credentialing**

- Issue PIV-I cards to First Responders for physical and logical access
- Issue derived credentials for mobile access through systems which support the FIDO 2 standard on mobile devices

**Access Management**

- Install/upgrade federally-compliant PACS during new construction, building renovations and/or replacement of existing, end-of-life access control systems
- Integrate PIV-I to provide MFA for accessing logical systems
- Follow federal best practices guidance when implementing mobile systems which support standards and protocols to enable information sharing
    - Multi-Factor Authentication (MFA): Fast Identity Online (FIDO)
    - Single Sign-On: OAuth
    - Federation
        - Security Assertion Markup Language (SAML)
        - OpenID Connect

# Financial Overview

Security vulnerabilities and regulatory changes are forcing public safety organizations to adopt MFA solutions. Many departments in the H-GAC region are actively procuring and/or testing MFA technologies. Investing in products that meet federal standards will enhance our region's ability to move towards a truly interoperable ICAM framework.

Procurement: organizations can leverage federal and regional procurement vehicles currently in place for PIV-I solutions.

Funding: the region should explore grant opportunities to offset the costs of obtaining PIV-I credentials for First Responders and explore regional procurement opportunities for upgrading the necessary PACS and LACS to maximize the value of the PIV-I cards by expanding the physical and logical systems they can be used with.

# Implementation Plan

Achieving a truly interoperable identity framework throughout the region will require a combination of individual department-level actions along with a variety of regionally coordinated planning, funding, and policy development activities.

**Regional Coordination**

Many public safety executives understand the operational necessity of sharing access to facilities and information with personnel from other organizations. Security vulnerabilities and regulatory changes are forcing departments to address some of these challenges. In order to securely share physical and logical access across organizations, they must be able to 1) trust identities of personnel from other organizations 2) issue credentials which can be shared across organizations, and 3) control what access is granted to who and when.

There is agreement by many public safety stakeholders in the H-GAC region on the value of a regional approach to ICAM, and numerous successful programs around the country provide evidence and lessons learned. Since there is no funding or mandate for this initiative, the choice to participate in a regional effort is up to each individual department/jurisdiction. As with any decision, the value to each organization of participating must outweigh the cost.

The establishment of a regional H-GAC ICAM Working Group can coordinate strategic planning efforts while suggesting tactical department and/or jurisdictional level activities. Below is a list of the types of strategic and tactical actions that should be addressed moving forward by organizations interested in participating in a regional ICAM initiative.

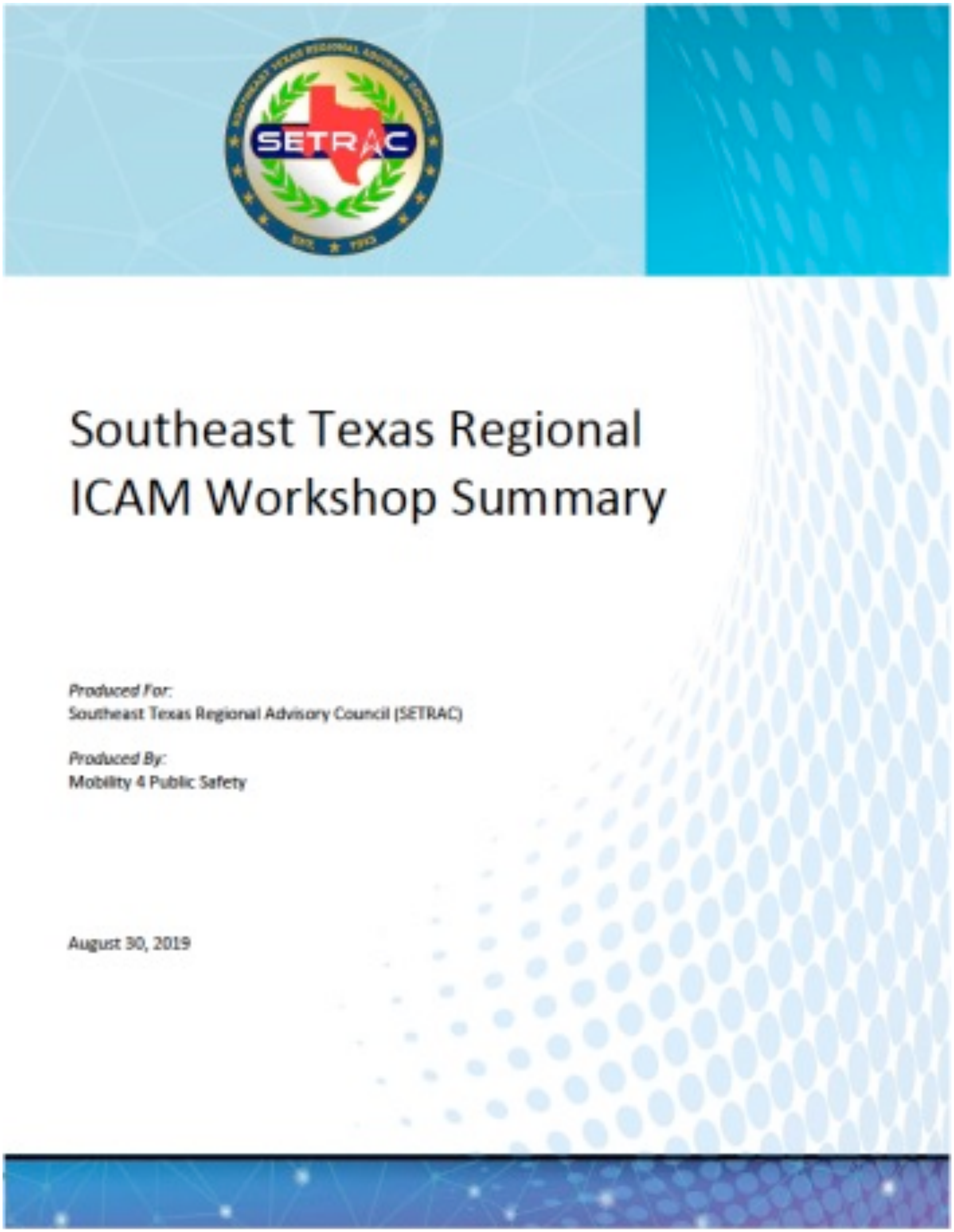
Strategic Planning Activities

1. Define regionally approved standards/protocols based on federal guidance and best practices
2. Develop common procurement language which can be utilized for all technology projects
3. Ensure all grant-funded projects adhere to the regional ICAM framework
4. Define the Vision and Goals for Regional Identity Sharing
    - Define **WHAT** information organizations want to share
    - Identify **WHO** organizations want to share with
    - Develop a regional framework for **HOW** organizations share identities and information
5. Develop regionally-acceptable policies to support the secure sharing of identities and information
6. Secure funding to offset the cost of migration to PIV-I

Department/Jurisdictional Activities

1. Agree to the adoption of regionally-approved ICAM standards & protocols
2. Utilize standard regional ICAM procurement language in all new system acquisitions

# Appendix A – Regional ICAM Workshop Report



Southeast Texas Regional ICAM Workshop Summary

*Produced For:*
Southeast Texas Regional Advisory Council (SETRAC)

*Produced By:*
Mobility 4 Public Safety

August 30, 2019