PSCR SECURITY

Securing the first responder of the future

PSCR Security

Federated Identity & Enhanced Authentication

NIST National Institute of Standards and Technology
U.S. Department of Commerce

CTL Communications Technology Laboratory

Agenda

- PSCR Security Overview
- Federated Identity for Public Safety Introduction
- PSCR Research
  - Federated Identity Credential & Access Management (ICAM)
  - Mobile SSO
  - Enhanced Authentication
  - Next Steps

5 Key Research Areas

LMR to LTE

User Interface User Experience

Mission Critical Voice

Location-Based Services

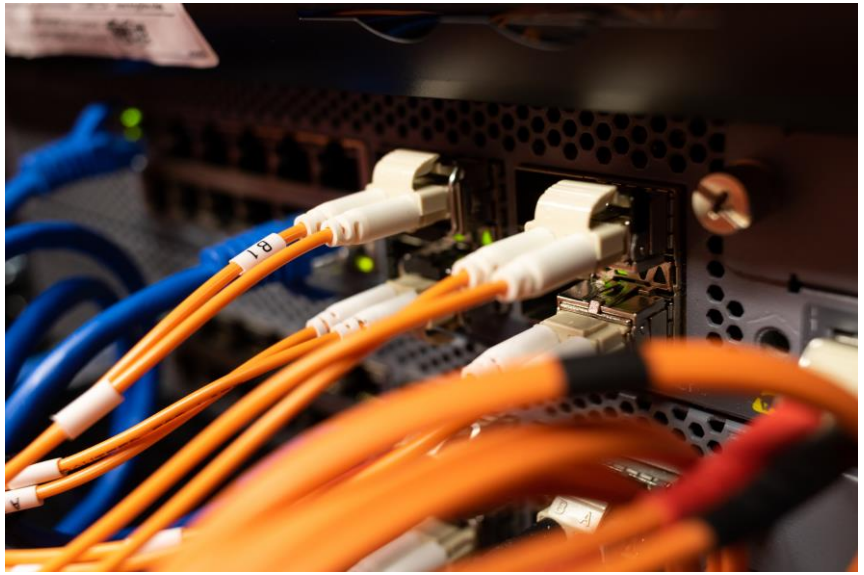
Public Safety Analytics

Security

Resilient Systems

Cross Cutting Research Areas

Cybersecurity



National Institute of Standards and Technology
U.S. Department of Commerce

PSCR SECURITY
Securing the first responder of the future


Access Controls
Mobile Application Security
Intrusion Detection
IoT/Wearables
Blockchain
LTE/5G Network Security
Encryption
Supply Chain
Identity Management
Privacy
Vulnerability Mitigation
Operating System
Over the air
Updates/patching
Forensics

PSCR Roadmap Process

1 ROADMAP WORKING GROUP

2 ROADMAP PUBLICATION

3 ROADMAP SUMMIT

4 SUMMIT REPORT

PSCR Security Research

- PSCR Security Services
  - Maintain Security of our Demonstration Network
  - Provide Security overlay for all PSCR research
  - Security specific research projects
- PSCR Security Projects
  - **Public Safety Federated ICAM/Mobile Single Sign On (SSO)**
  - Public Safety Handsets and Wearables Security
  - Expanding the use of the SIM for Public Safety
  - Mobile Application Security Vetting
  - 3GPP SA3 Workgroup Support

Introduction to Federated Identities

National Institute of Standards and Technology
U.S. Department of Commerce

CTL Communications Technology Laboratory

Time of Transition for Public Safety

Increase in Software as a service (SaaS) application architectures

# of mobile applications and data on mobile backends in the cloud

- Growth in smart phones and tablets
- Typical model is client (often a mobile application) on the device accessing data in third party cloud
- Common for SaaS offering to give users a new credential (username/password)

Increase in number of credentials managed

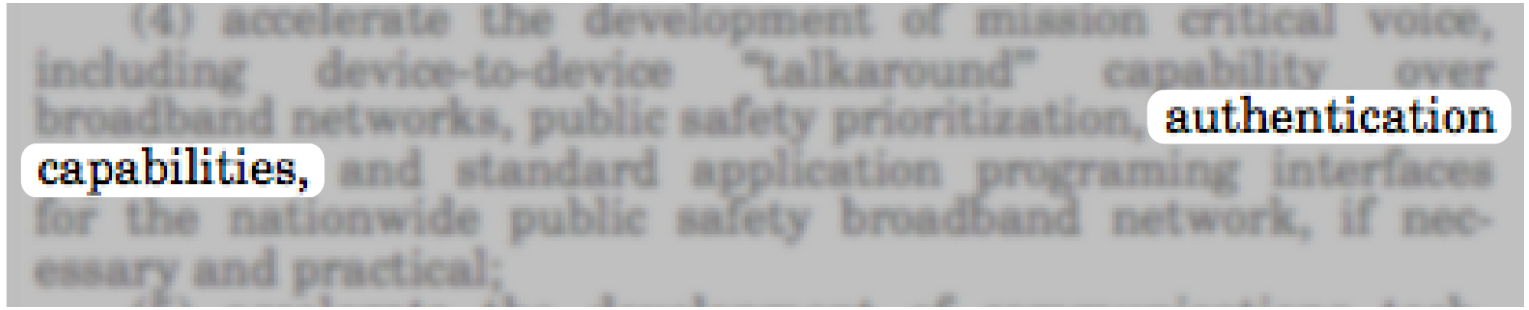
# of credential managed by Public Safety Personnel

- Number of credentials used by public safety first responders will grow as multiple SaaS applications are used in the line of duty
- Challenges with remembering passwords, often leads to password reuse
- Organizations will need to make sure user accounts in each SaaS resources are updated as the user leaves or changes roles

Need for Interoperability

Public Safety Position on Federated ICAM

Middle Class Tax Relief and Job Creation Act of 2012



(4) accelerate the development of mission critical voice, including device-to-device "talkaround" capability over broadband networks, public safety prioritization, authentication capabilities, and standard application programing interfaces for the nationwide public safety broadband network, if necessary and practical;

FirstNet RFP - Operational Architecture

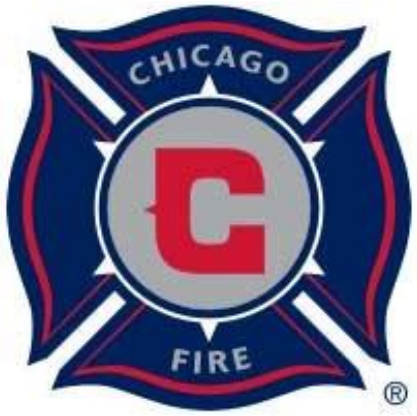
A.7.1.4.2 **Federated Identity Management**

Federated Identity Management provides the ability for users, systems and services in one domain or agency to get access to services and applications in a different domain or agency. Federated Identity Management requires standardization of the authentication and authorization methods and interfaces which allows for users, services and applications to interoperate across security boundaries (e.g. domains, agencies, etc.). Federated Identity Management allows for collaboration and reuse across agencies.

Public Safety Position on Federated ICAM

National Public Safety Telecommunications Council (NPSTC) Encourages Public Safety to Adopt the Trustmark Framework

Federation


CHICAGO
FIRE


ST. LOUIS FIRE DEPARTMENT
JUSTIFIABLY PROUD
1857


S·F·F·D·


LOS ANGELES FIRE DEPARTMENT
FOUNDED 1886


CHICAGO
POLICE

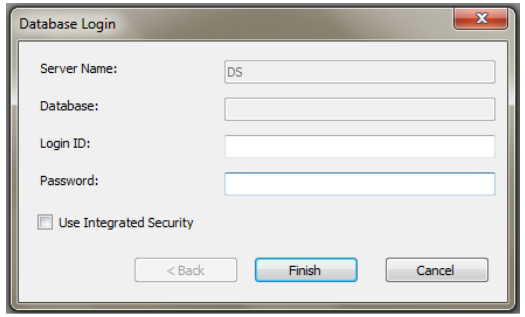
Federation Services

Microsoft Active Directory
IDP

Microsoft Active Directory
IDP

Federation

Existing Federation Service
IDP



Public Safety
Data Service

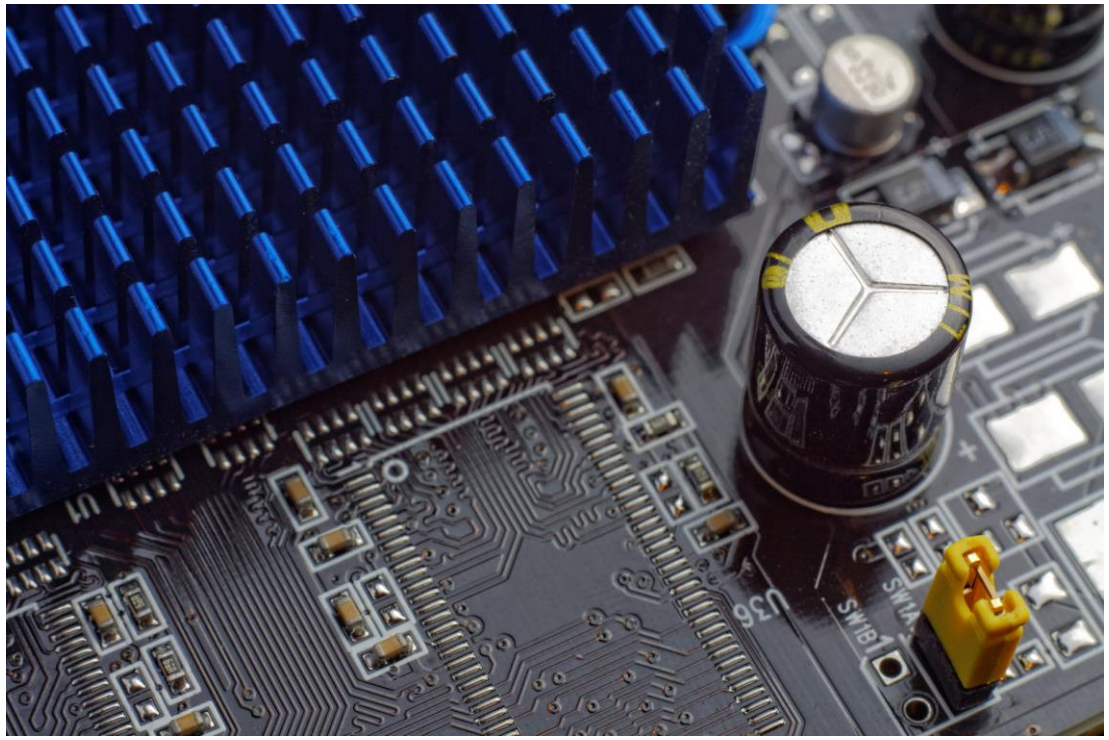
Public Safety
Mobile Apps

Public Safety
Application

Continuing need for information sharing

Need for identity infrastructure that supports cross-jurisdictional information sharing

Challenges? Complex Technology



- Combination of new and legacy apps
- Multiple standards OpenID, SAML & OAUTH
- Considerations for both security & privacy
- Few best practice implementations available
- Stakeholders lack of knowledge
- Policy and Politics (of course!)

Mobile Application Single Sign On (SSO)

National Institute of Standards and Technology
U.S. Department of Commerce

CTL Communications Technology Laboratory


Yelp
Instagram
Phoster
Facebook
Twitter


POLICE DEPARTMENT
LOGIN
PASSWORD
CITY OF NEW YORK

Mobile Single Sign-on (SSO)

2 Factor Authentication

DRAFT

NIST SPECIAL PUBLICATION 1800-13A

Mobile Application Single Sign-On

Improving Authentication for Public Safety First Responders

Volume A:
Executive Summary

Paul Grassi
Applied Cybersecurity Division
Information Technology Laboratory

Bill Fisher
National Cybersecurity Center of Excellence
Information Technology Laboratory

Santos Jha
William Kim
Taylor McCorkill
Joseph Portner
Mark Russell
Sudhi Umarji
The MITRE Corporation
McLean, VA

April 2018

DRAFT

This publication is available free of charge from:
https://www.nccoe.nist.gov/projects/use-cases/mobile-sso

NIST National Institute of Standards and Technology U.S. Department of Commerce

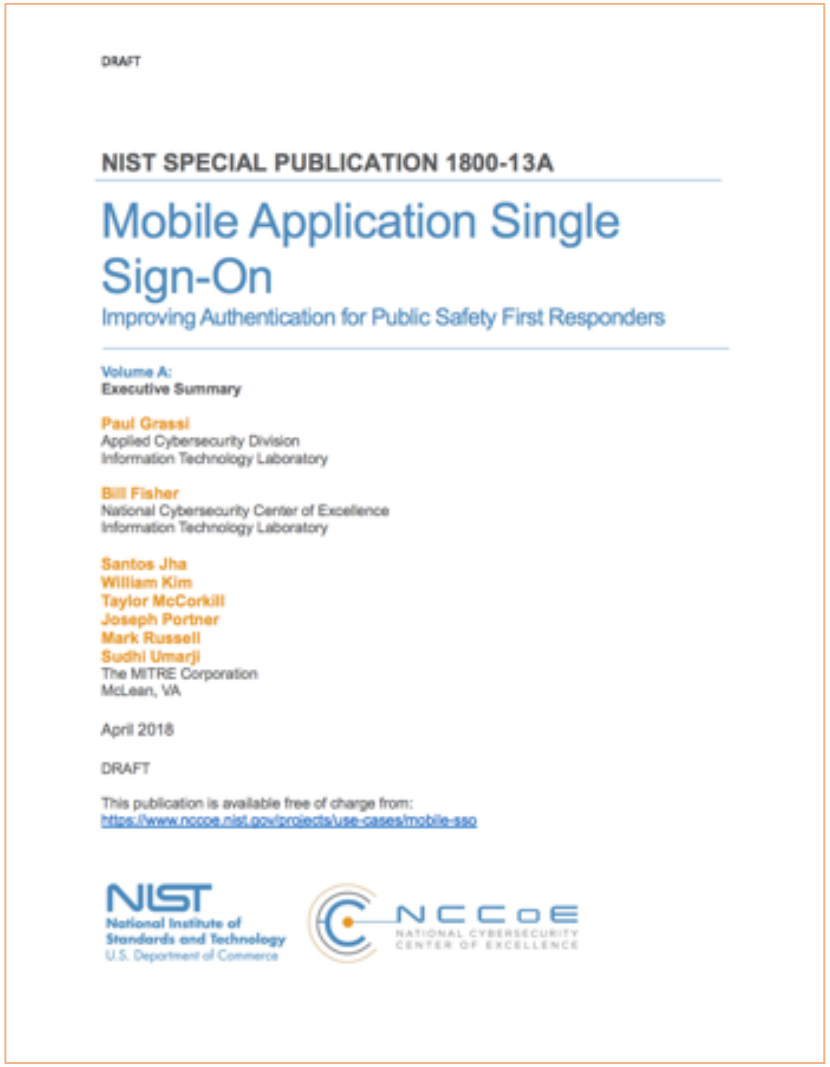
NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Enhanced Authenticators

Mobile SSO for Public Safety

Demonstrate strong and reliable multi-factor authentication and SSO using standards-based, commercially available technology to enable rapid and secure data access in the Public Safety operational environment

This project resulted in a publicly available NIST Cybersecurity Practice Guide that will enable Public Safety organizations to implement this in their own environments



DRAFT

NIST SPECIAL PUBLICATION 1800-13A

Mobile Application Single Sign-On

Improving Authentication for Public Safety First Responders

Volume A:
Executive Summary

Paul Grassi
Applied Cybersecurity Division
Information Technology Laboratory

Bill Fisher
National Cybersecurity Center of Excellence
Information Technology Laboratory

Santos Jha
William Kim
Taylor McCorkill
Joseph Portner
Mark Russell
Sudhi Umarji
The MITRE Corporation
McLean, VA

April 2018

DRAFT

This publication is available free of charge from:
https://www.nccoe.nist.gov/projects/use-cases/mobile-sso

NIST National Institute of Standards and Technology U.S. Department of Commerce

NCCoE National Cybersecurity Center of Excellence

Mobile SSO: Core Capabilities

Multifactor Authentication (MFA) to Mobile Resources

p@$$w0rd +

- Biometrics, external hardware authenticators and other authentication options

Single Sign-on (SSO) to Mobile Resources

- Authenticate once with mobile native app or web apps
- Leverage initial MFA when accessing multiple applications

Identity Federation

- Leverage directory services already in place

NCCoE Benefits – Industry Collaboration

NCCoE brings in Industry experts to design and build the reference design:

Mobile SSO Technology Vendor Build Team:

NCCoE Benefits – Standards Based

NCCoE solutions implement standards and best practices:

OpenID OAUTH 2 IETF NFC fido alliance AppAuth

Using modern commercially available technology:

FIDO Solutions

FIDO UAF Authentication

- Leverages fingerprint registered to device
- No Password Input

FIDO U2F Authentication

- Using FIDO key as second factor
- Public key pair on the device

FIDO Security Benefits

- Multifactor authentication in line with NIST 800-63-3 Requirements
- No secrets (private keys or biometric templates) are stored server-side
- Phishing resistance

NCCoE Benefits – Practical Guidance

NIST Cybersecurity Practice Guide (SP 1800-13) is available now and includes:

DRAFT

NIST SPECIAL PUBLICATION 1800-13A

Mobile Application Single Sign-On

Improving Authentication for Public Safety First Responders

Volume A:
Executive Summary

Paul Grassi
Applied Cybersecurity Division
Information Technology Laboratory

Bill Fisher
National Cybersecurity Center of Excellence
Information Technology Laboratory

Santos Jha
William Kim
Taylor McCorkill
Joseph Portner
Mark Russell
Sudhi Umarji
The MITRE Corporation
McLean, VA

April 2018

DRAFT

This publication is available free of charge from:
https://www.nccoe.nist.gov/projects/use-cases/mobile-sso

- Technical Decisions
- Trade-offs
- Lessons Learned
- Build Instructions
- Functional Tests

An Innovative Solution

Prize Challenge

Teamwork

PSCR OPEN INNOVATION

Solving the Public Safety needs of tomorrow...today

PSCR SECURITY

ITL

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

nok nok

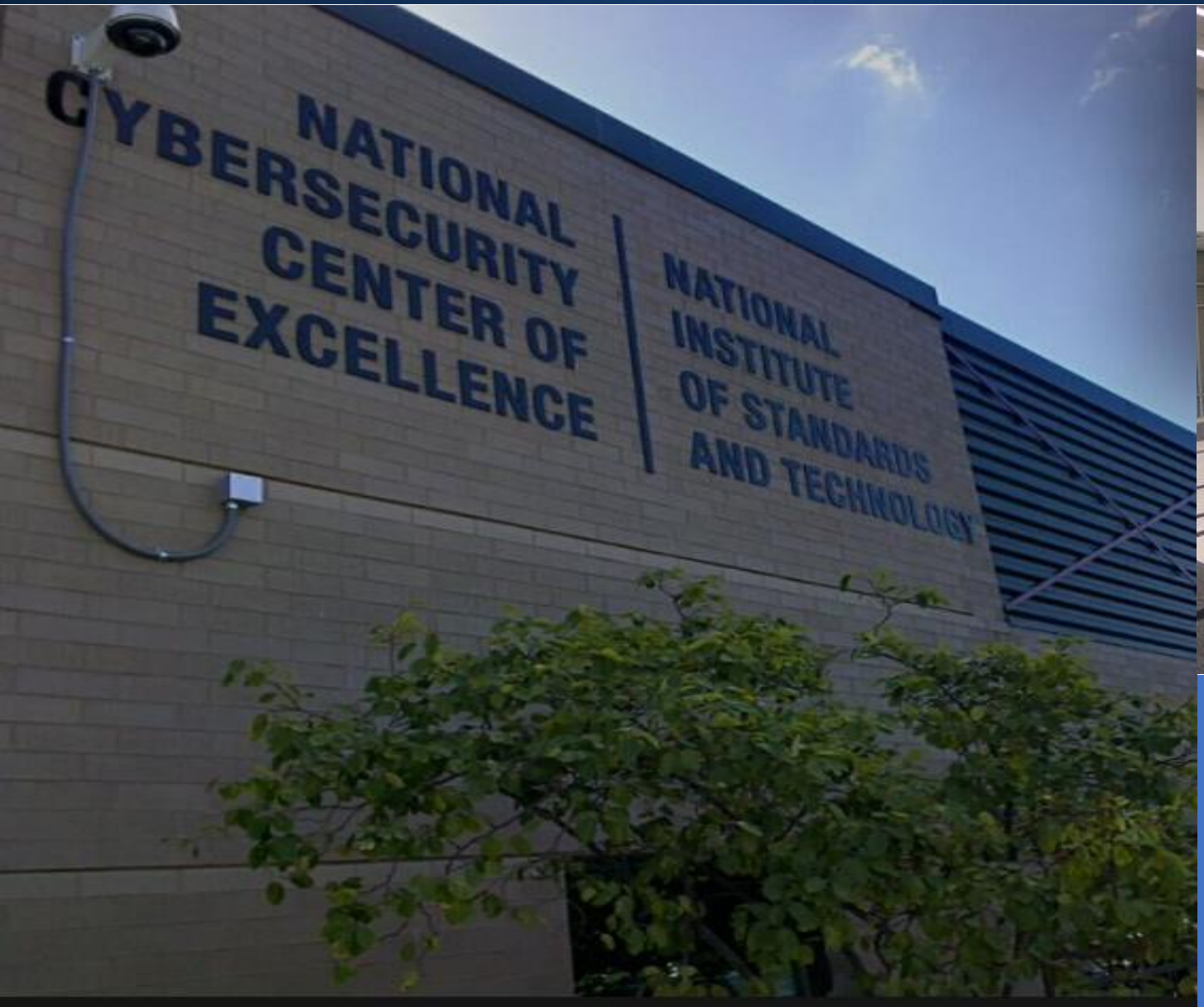
IBM

Federated Identities: Next Steps

National Institute of Standards and Technology
U.S. Department of Commerce

CTL Communications Technology Laboratory

ICAM Workshop



NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

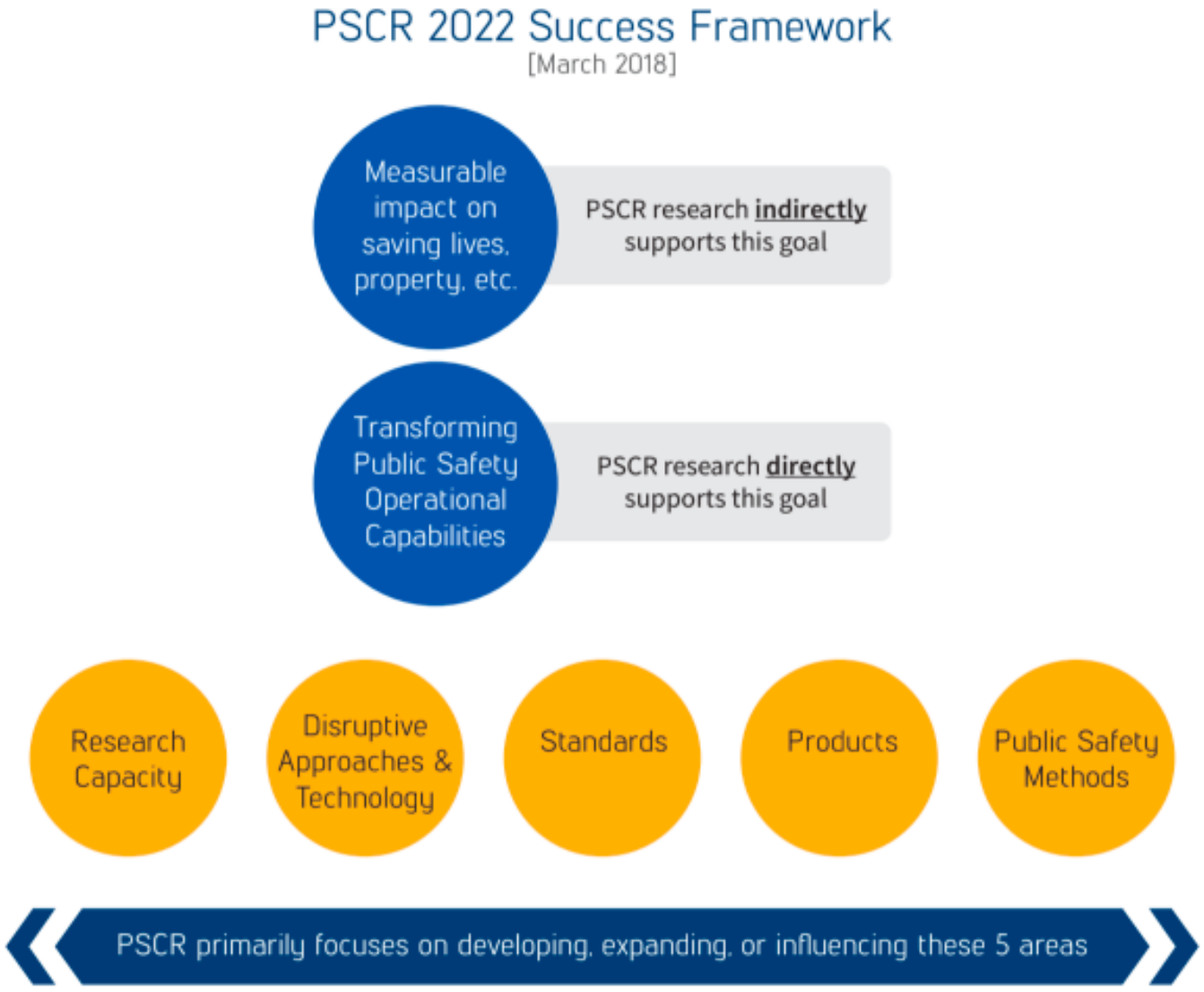
ICAM Workshop Attendees

PSCR-NCCoE Planning Information

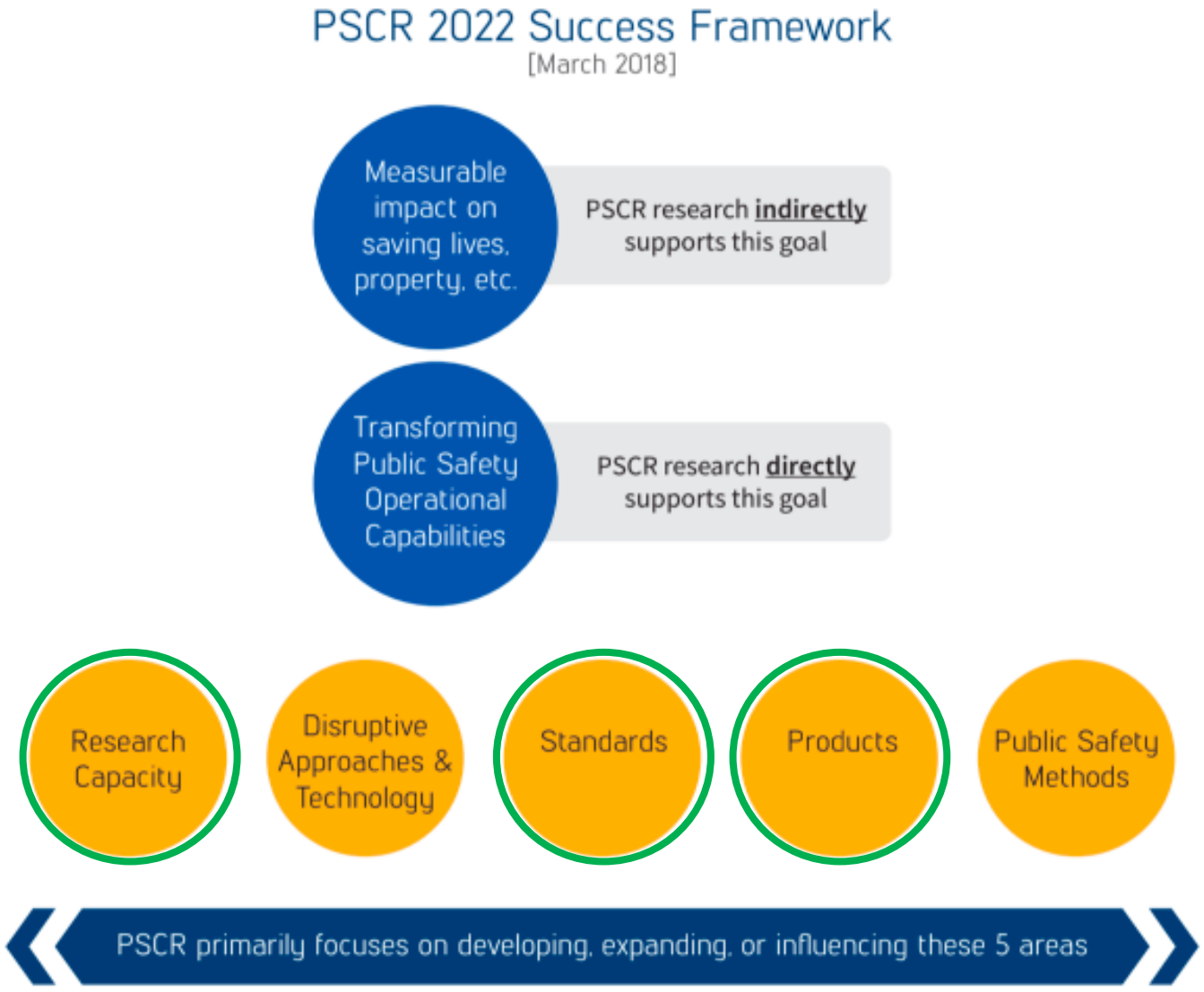
PSCR is planning a partner research project with the National Cybersecurity Center of Excellence (NCCoE) to build a Public Safety Federated ICAM Research Network with the following high level objectives:

- Provide **proof of concept** public safety federated ICAM architecture
- Provides **education** opportunities to all public safety stakeholders
- **Identify technological and functional gaps** in existing capabilities and facilitate **innovative solutions**
- Provide detailed **build documentation**
- Support the creation/adoption of policies and standardization
- Provide a **test bed** where industry, PSCR, and other research organizations can evaluate and incorporate other public safety communication research objectives

PSCR Success Framework



PSCR Success Framework



QUESTIONS?