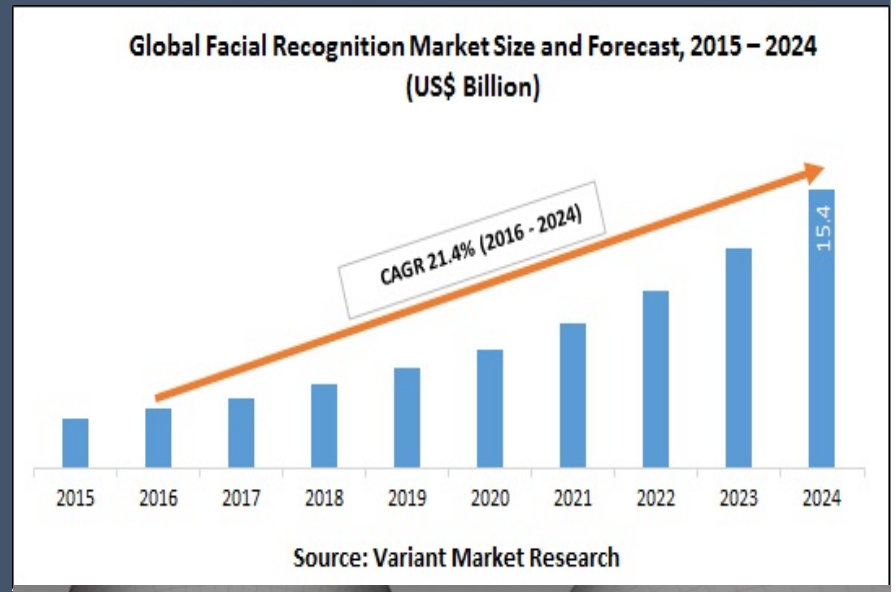
FACIAL RECOGNITION TECHNOLOGY

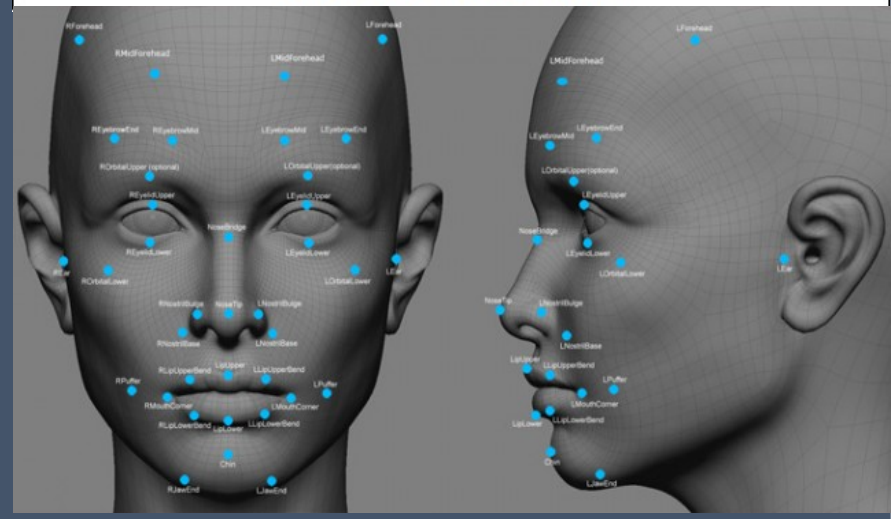
MEASURING EFFICIENCY AND EFFECTIVENESS, BUSINESS AND PUBLIC SAFETY VALUE

Pam Scanlon, Executive Director, ARJIS
The Automated Regional Justice Information System

Facial Recognition Research

- Global Facial Recognition Market is estimated to reach $15.4 billion by 2024; growing at a CAGR of 21.4% from 2016 to 2024.
- Primary factor driving growth of global facial recognition market is rising demand for improved surveillance and monitoring at public places
- Upsurge in the use of facial recognition technologies in industries such as government and defense have also boosted the market growth.
- However, lack of policies, metrics, standardization, potentially high implementation costs, and government regulation of this technology are the major hindrances for the growth of the market.

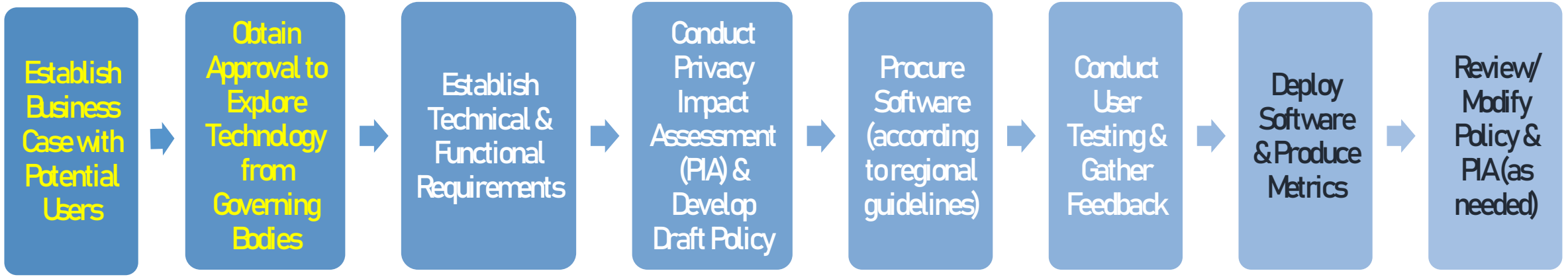




Lessons Learned: Facial Recognition Technology

1. Know why you are implementing facial recognition technology (Document the Business Case)
2. Develop a regional policy with community input in public settings
3. Collaborate with other agencies and look to national organizations for standards and guidance
4. Make sure that you are protecting your data in compliance with security and privacy laws, and federal and state policies

ARJIS Regional Process for Adopting New Technologies



ARJIS-RAND Information Sharing Study

- 2013 – 2017 ARJIS partnered with RAND to assess information sharing and police technologies such as facial recognition
- Key part of this study was evaluating the ARJIS Mobile Program and how officers were using facial recognition technology
- ARJIS selected three San Diego agencies to receive 200+ new ARJIS Mobile Devices with facial recognition technology
- Mobile surveys were administered pre and post deployment of mobile devices with facial recognition
- Facial recognition was the most desired technology before the pilot, and the most heavily used 3 months after deployment!

Knowing More, but Accomplishing What?

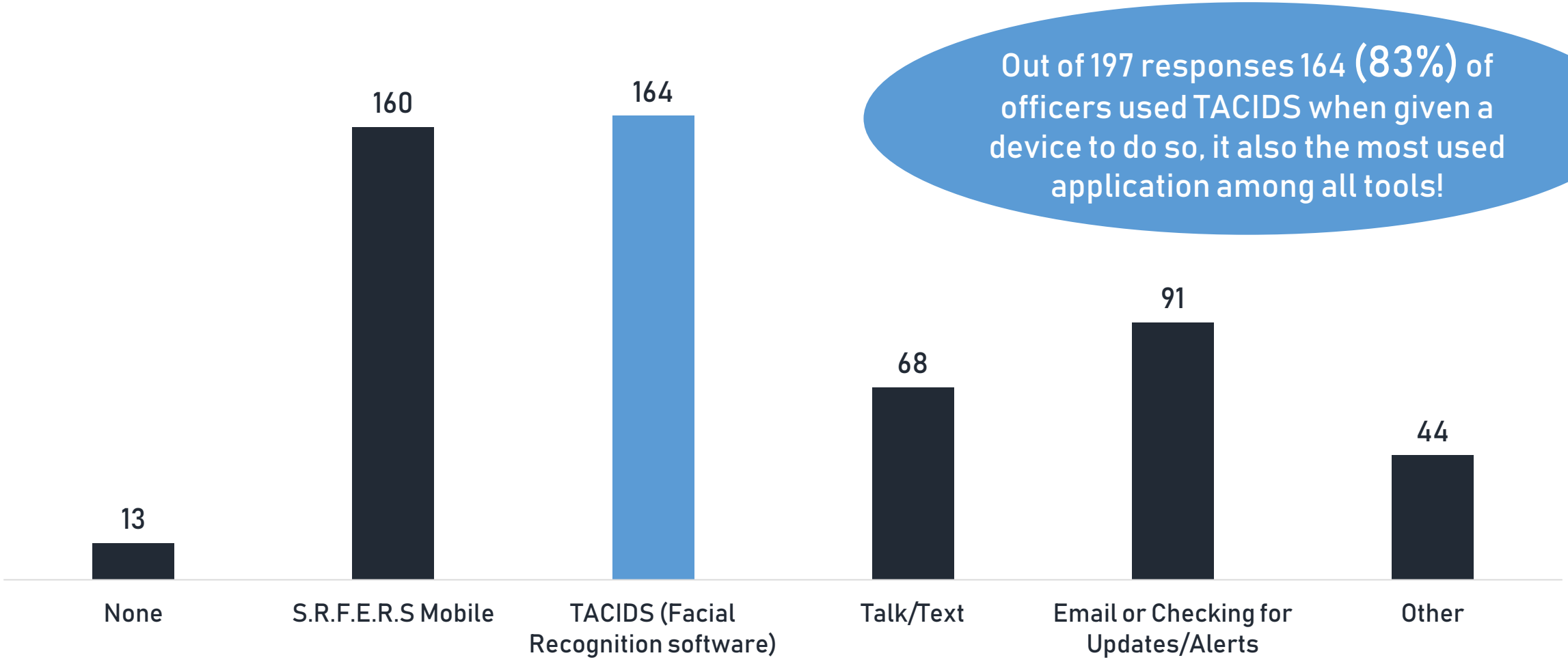
Developing Approaches to Measure the Effects of Information-Sharing on Criminal Justice Outcomes

Brian A. Jackson, Lane F. Burgette, Caroline Stevens, Claude Messan Setodji, Erinn Herberman, Stephanie Ann Kovalchik, Katie Mugg, Meagan Cahill, Jessica Hwang, Joshua Lawrence Traub

RAND CORPORATION

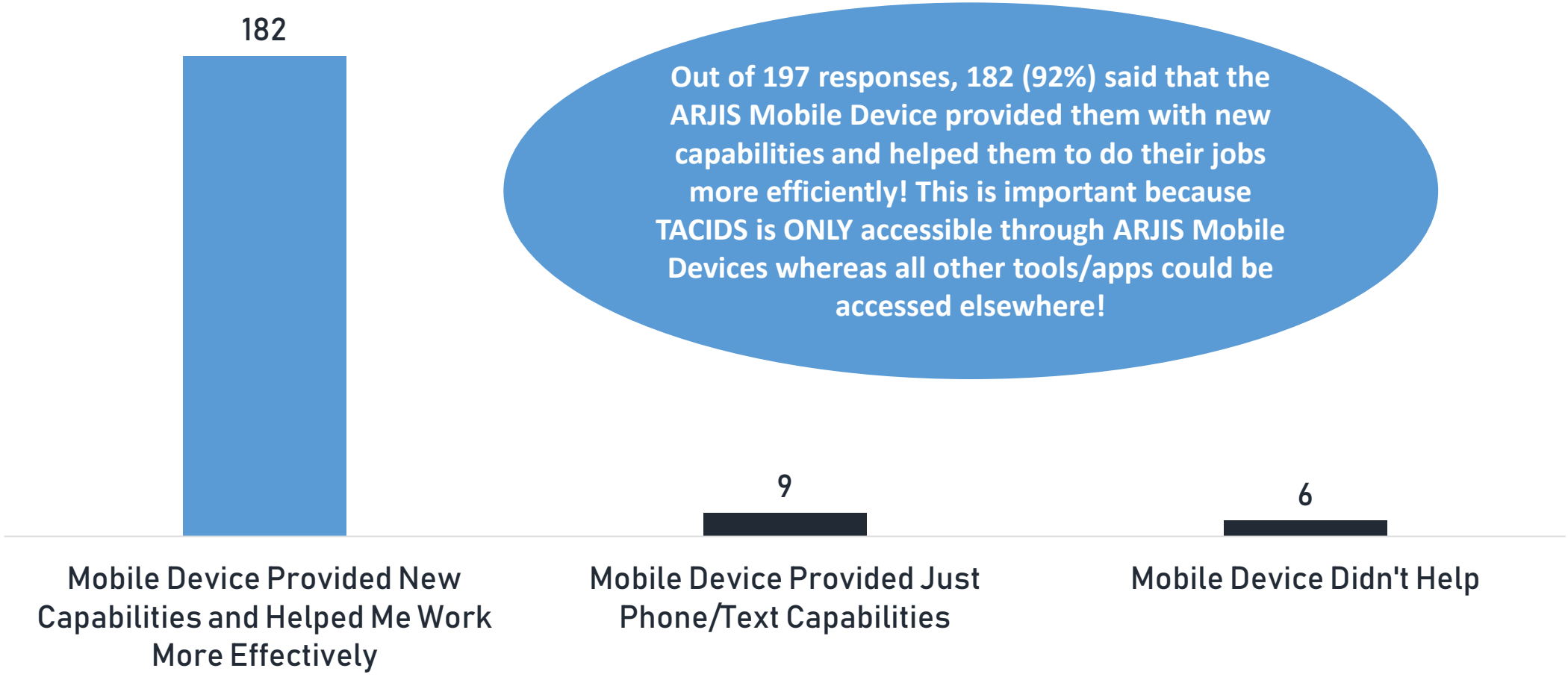
ARJIS Mobile Survey Results

Which applications/tools did you use on you ARJIS Mobile Device? (Check all that apply)



ARJIS Mobile Survey Results

Which statement best reflects your experience using an ARJIS Mobile Device?



Process for Policy Development

- Identify operational vs. technical (acceptable use) policy components
- ARJIS is responsible for the technical aspects of the regional technologies it develops and maintains
- Acceptable Use Policy – under the purview of ARJIS governing bodies and pertains to network security, privacy protocols, access and performance of software
- Operational Use Policy – pertains to how the software is actually used in the field and is the responsibility of Individual agencies which is based on regional protocols adopted by San Diego County Chiefs/Sheriff's Association

ARJIS Public Portal & Policy Webpage

APPLICATIONS & SERVICES

The ARJIS Public Web Portal includes a web page on just our policies and governance structure where the public can download and read Facial Recognition Policies and more. This page was our third most visited site page in 2018!

POLICY PAGE VIEWS: 4,899

‘

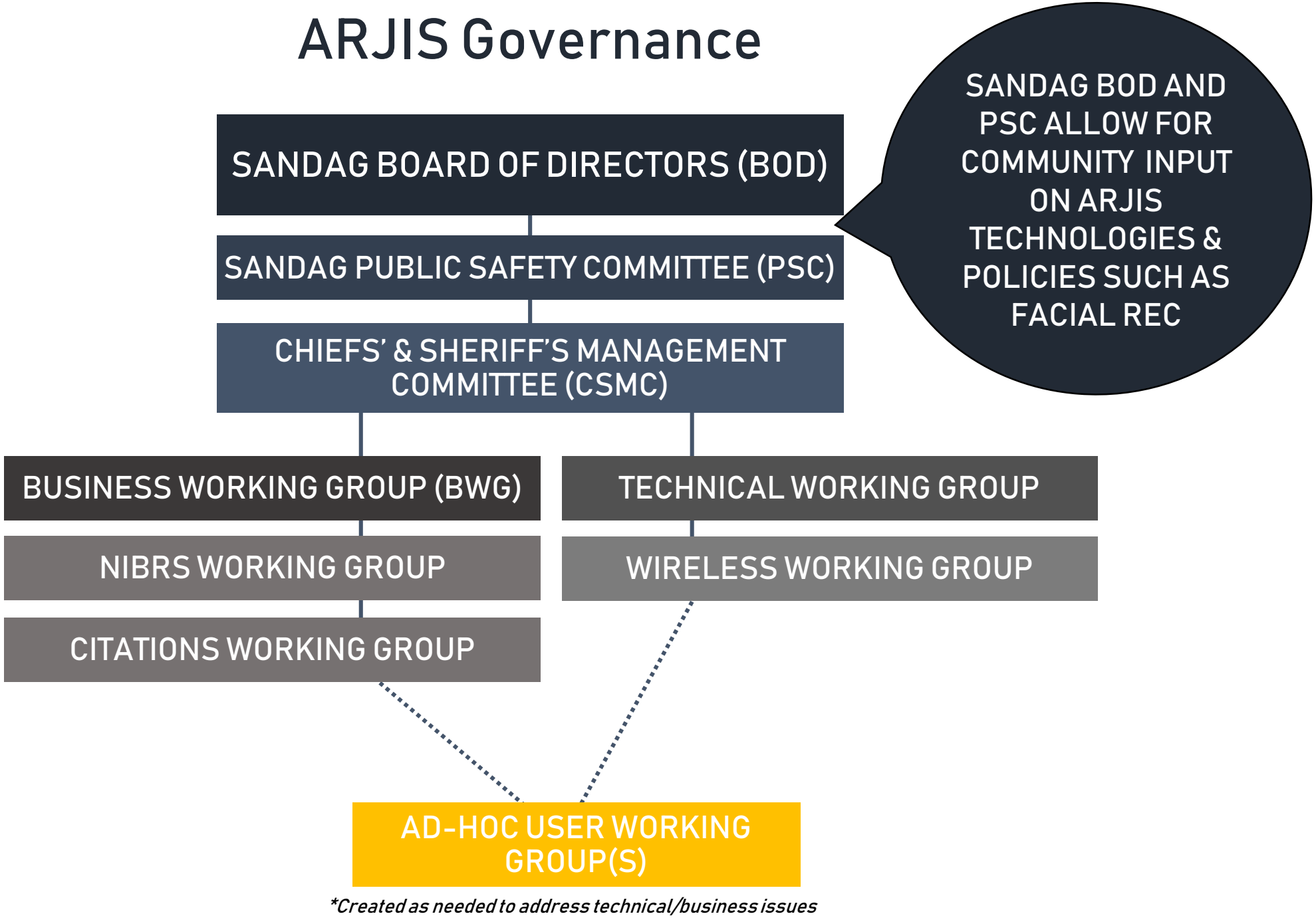
Privacy Impact Assessment – 2011

Acceptable Use Policy – 2012 rev. 2015

Operational Use Policy – SDPD 2012

Facial Recognition Use Case Catalog - 2019

ARJIS Governance



**Created as needed to address technical/business issues*

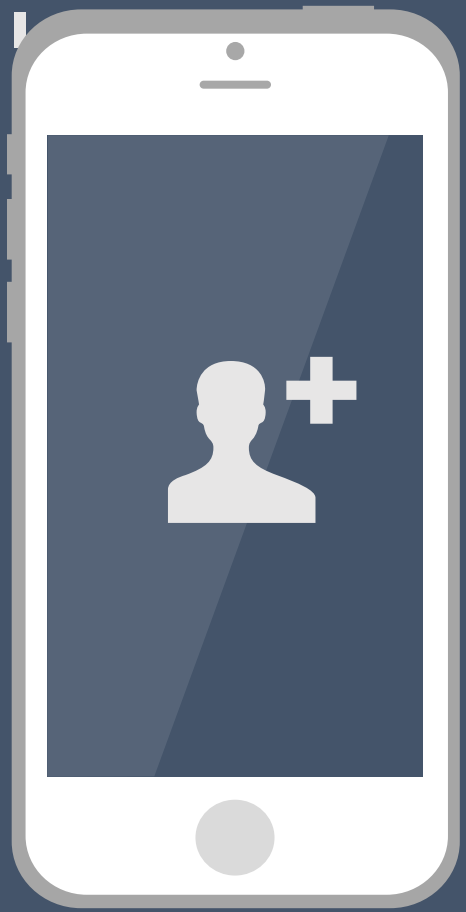
ARJIS Mobile Program = Efficiency

1200+ Devices

30+ Agencies

10+ Applications

24/7 Support



ARJIS Mobile Devices provide officers with an “untethered” office where they can investigate cases in the field, on-the-go, while still continuing their regular patrol and/or community policing responsibilities.

ARJIS Fingerprint Scanners

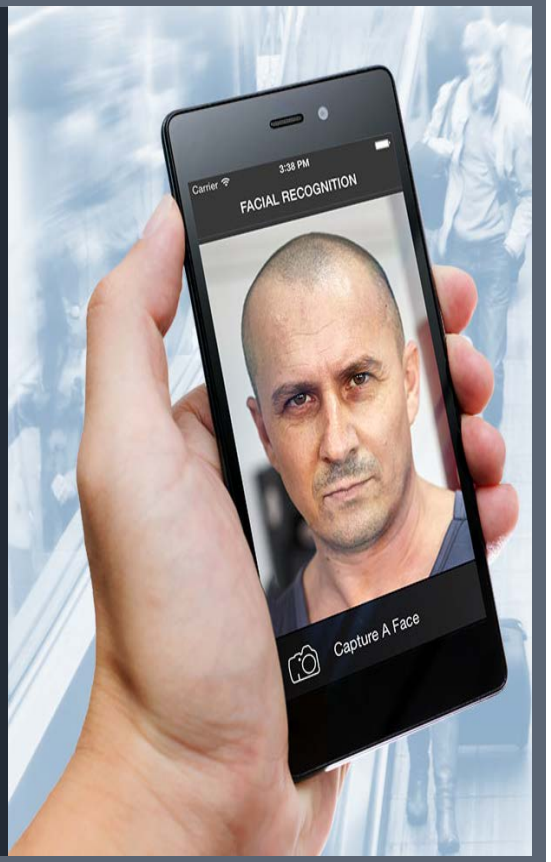
- Another type of biometric is a finger print scan
- Device: Thales BluCheck 3 Mobile Identification Handheld Device (500 ppi, Bluetooth Connection, FBI Certified)
- 400+ Fingerprint scanners in the field today
- Plan to provide one with each authorized Smartphone.
- Fingerprint scanners used to ID people using one or both index fingers
- Results display on ARJIS Mobile Device
- Fast, accurate and very secure!

How ARJIS Agencies Use Facial Recognition

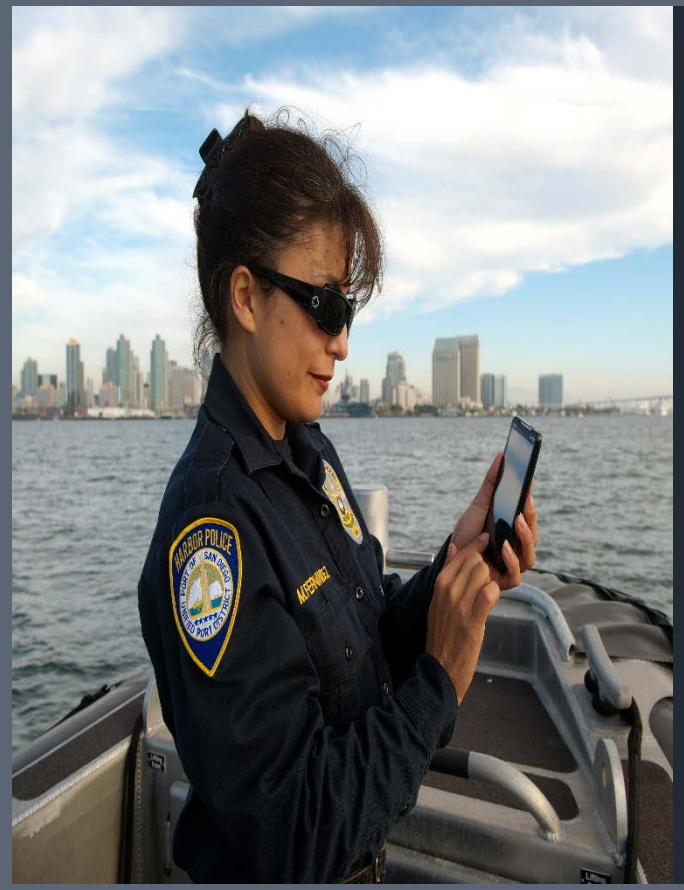
- Officers use a smartphone to photograph an individual when:
  - The officer has detained the individual based on probable cause
  - Verification of an individual's identity is not possible, or
  - The officer suspects the self-reported information is false
- Officer submits the image for comparison against the San Diego Booking Photo Database (currently about 1.8 million images)
  - ARJIS ingests booking photos daily from the San Diego Sheriffs Department

How is ARJIS Using Facial Recognition?

- TACIDS – Tactical Identification System
- Utilizes a mathematical algorithm for biometric comparison of person's face against photos from Booking Photo Database
- System returns leads or suggested matches with varying level of confidence – ordered from highest to lowest
- Potential matches considered advisory in nature and subsequent verification of the individual's identify and/or follow-on action should be based on an agency's operating procedures
- After completing the request for facial recognition field identification results, the image used for comparison shall be manually deleted from the device used to capture the image



Specification of Use for TACIDS
(Agency Operational Policy)

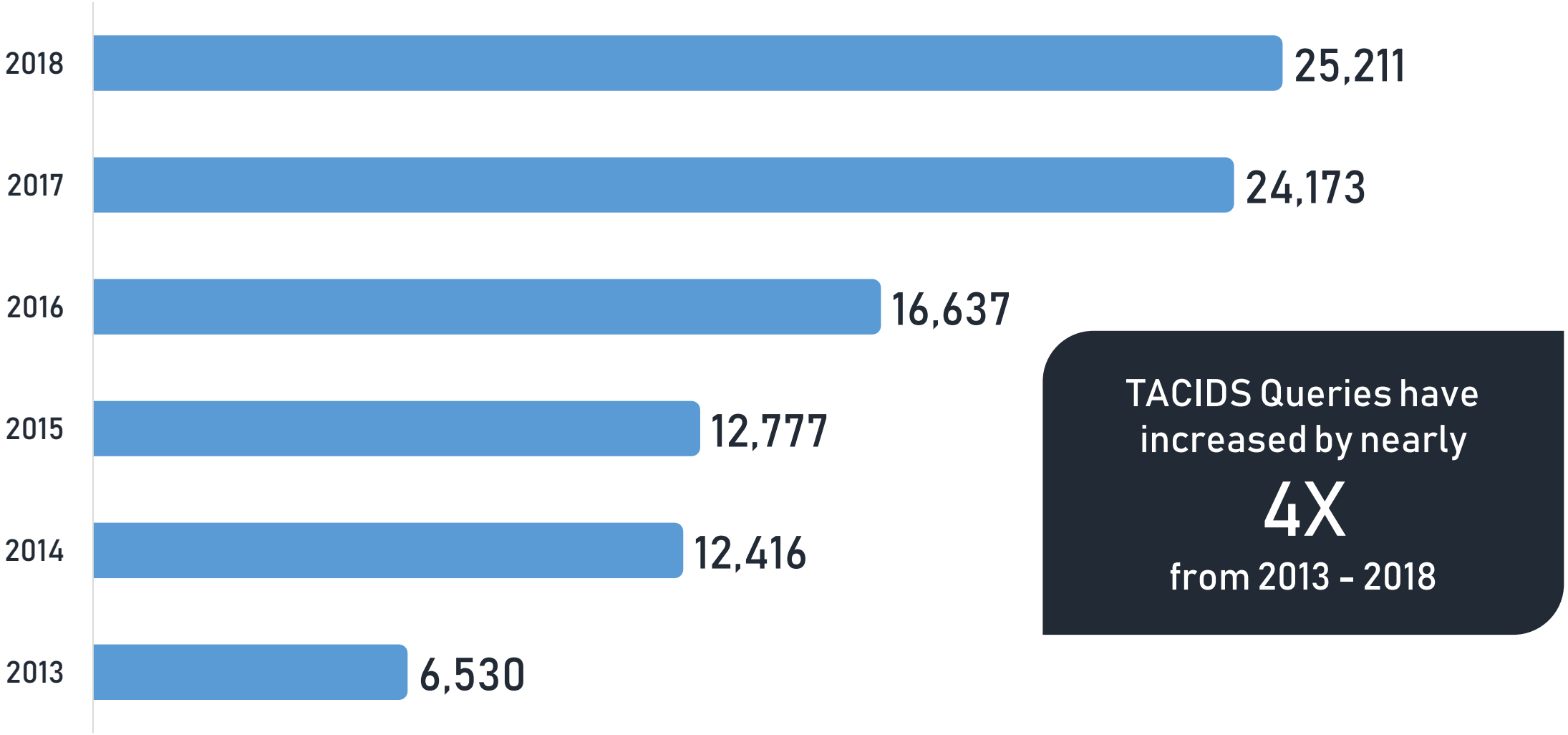


- Three primary uses for using TACIDS
  - Assist in identification of suspects of criminal investigations
  - Help locate missing persons
  - Assist in identification of individuals for whom a warrant has been issued
- Law enforcement may also use TACIDS when…
  - An officer suspects driver license or ID is fraudulent
  - Or officer suspects ID belongs to another person
- Potential matches presented by TACIDS are considered advisory in nature and any subsequent verification of the individual's identity and/or follow-on action should be based on an agency's operating procedures

Facial Recognition Technology

Reporting, Metrics, and Success Stories

Facial Recognition Queries by Year

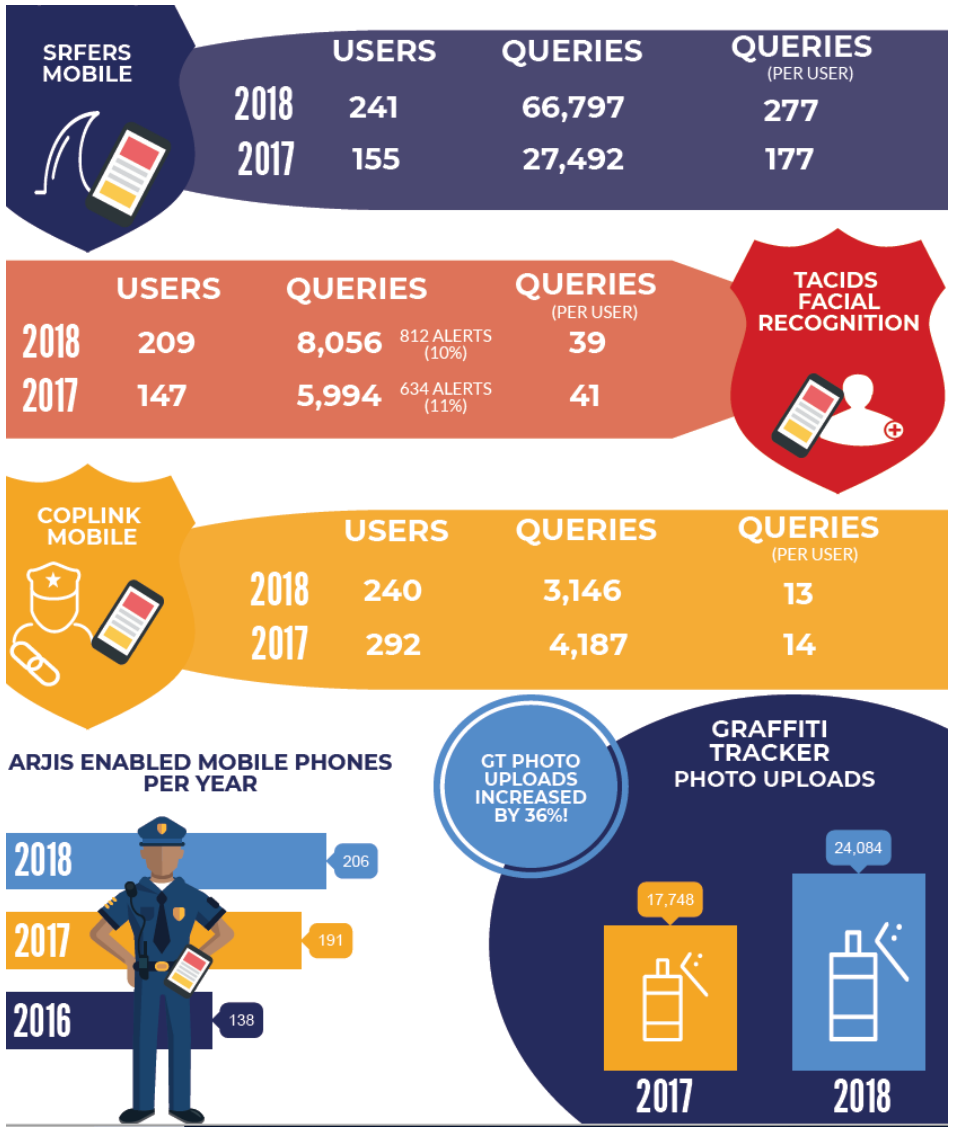


TACIDS Queries have increased by nearly

4X

from 2013 - 2018

ARJIS Management & Metrics Reports



Each year ARJIS creates a comprehensive management report for each agency detailing…

- Total number of users
- Total number of mobile devices
- Queries per User for each application
- Year over year changes in applications use

This gives our agencies the information they need to grow and truly benefit from ARJIS applications and access!

ARJIS Facial Recognition

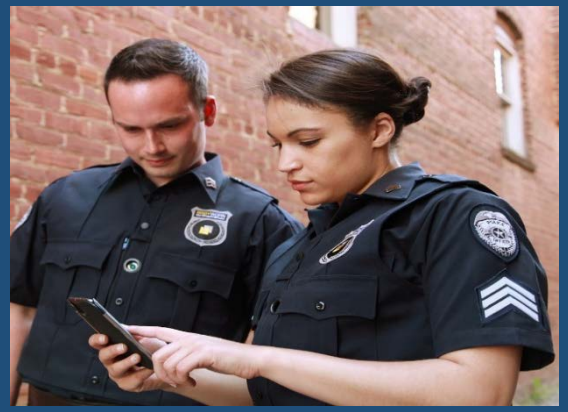
Success Stories

The SD Homeless Outreach Team uses our devices daily to ID subjects who need to be connected back to their service providers. With ARJIS Mobile Devices this becomes possible!

Officer used facial recognition to ID suspect who had assaulted a bus driver and sexually assaulted a passenger. He had absconded 18 months earlier and was a registered sex offender with two prior felony convictions for child molestation. Without TACIDS we never would have been able to close these cases and apprehend the suspect.

Suspect Identification & Investigative Research

Recently one of my officers was able to use TACIDS to identify 2 people who had been driving erratically and then continued to abscond on foot. It turns out that both men were wanted for murder and robbery in the state of Washington. ARJIS Mobile phones play a huge part in our success as an agency!

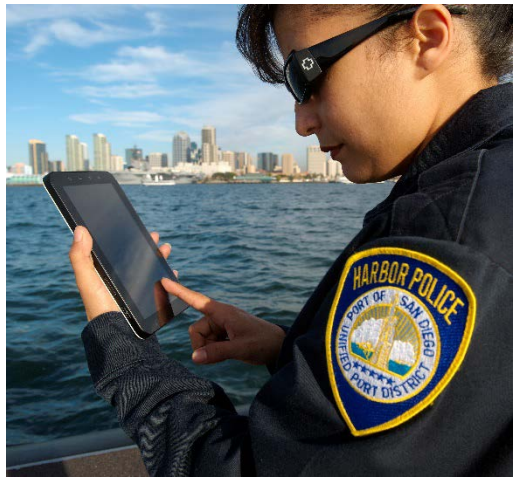


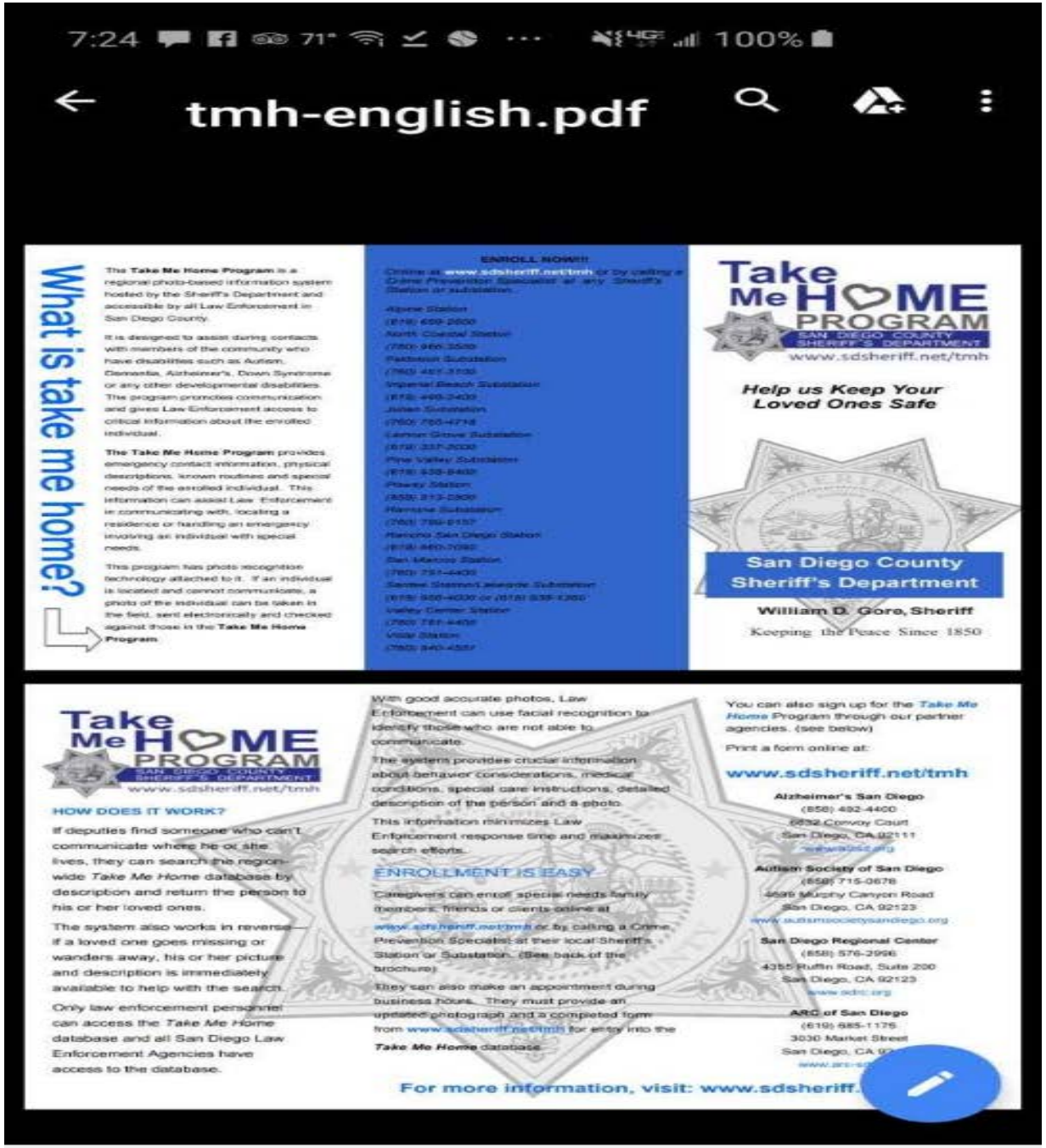
Officer responded to the ER with his department issued facial recognition device in an attempt to identify a subject who was transported by medics for a possible overdose. The subject was identified with use of the device and we were able to notify the family to come to the hospital during a critical time.

Success Story – San Diego Harbor Police

“On September 25, 2018, San Diego Harbor Police were hit by a cyber-attack that ultimately brought down our network. In an effort to protect our network and to protect our partner networks, all outside traffic was physically disabled at the onset of the attack.

This normally would result in an immediate disruption in police services at least until an agreement with a neighboring agency could be struck to provide the needed CJIS data. However, there was no disruption of services. In fact, the cyber-attack went unnoticed by the citizens in our area of responsibility. **The ability to maintain a seamless level of service was solely due to our adoption of the ARJIS smartphone program.**”





Take Me Home – San Diego County – 2015

- Database of at risk individuals

- Public can register at risk family members diagnosed with dementia, autism, Alzheimer's, etc.

- Contains detailed emergency contact info, physical desc, and photos

- Available on line, or by calling 211

- Accessible by select law enforcement officers

Collaboration & Guidance with National Organizations

- Collaborate with the International Association of Chiefs of Police (IACP) and IJIS Institute
  - IACP: Largest membership organization of police executives developing national policies and protocols for law enforcement technology
  - IJIS: Co-Chaired and produced Facial Recognition Use Case Catalog for Law Enforcement (Published March 2019)
- Refer to:
  - Federal Bureau of Investigation - Criminal Justice Information System (FBI-CJIS) Security Policies
  - California Department of Justice (CAL-DOJ) California Law Enforcement Telecommunications System (CLETS) Policies, Practices, and Procedures

Privacy, Transparency & Security Protocols

1. Make sure to review FBI CJIS Security Policy, CalDOJ CLETS Policies, Practices and Procedures for implementing/deploying new technologies
2. Have a plan for releasing data under California Public Records Act (CPRA) & federal Freedom of Information Act, most data is protected but not everything!
3. Be sure that you can conduct audits which contain the name of the person running the search and the specifications of that search for security purposes
4. Provide annual updates, improvements and metrics reports to your users and governing bodies to ensure transparency and use
5. Agencies ensure that users are trained early and often according to policy

FACIAL RECOGNITION TECHNOLOGY

MEASURING EFFICIENCY AND EFFECTIVENESS, BUSINESS AND PUBLIC SAFETY VALUE

Pam Scanlon, Executive Director, ARJIS
The Automated Regional Justice Information System