Identifying and Categorizing Mobile Application Data Types for Public Safety

Michael Ogata
NIST
michael.ogata@nist.gov

Disclaimer / Disclosure

Trade names and company products may be mentioned during this presentation. In no case does such identification imply recommendation or endorsement by the National Institute of Standards and Technology, nor does it imply that the products are necessarily the best available for their stated purpose.

Public Safety Mobile App Data Types

- *Identifying and Categorizing Data Types for Public Safety Mobile Applications*
- Held June 2015
- Workshop Goals
  - Enumerate public safety specific mobile data types
  - Categorize data types by impact to security
  - Examine possible security mechanisms
  - Examine relationships between data types and attribute based access

Previous Work

- Identifying Public Safety's Security Requirements for Mobile Apps
  - Held February 2014 at APCO Emerging Tech Forum
  - Published findings in NISTIR 8018
    - http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8018.pdf
- Workshop Goals
  - Refine APCO's *Key Attributes of Effective Apps for Public Safety and Emergency Response*
  - *Identify areas of further research*

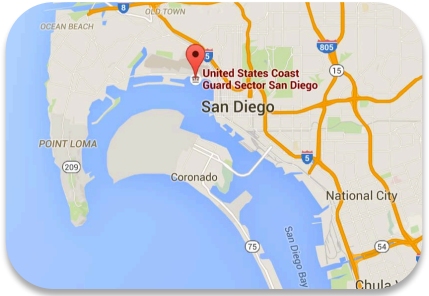
Workshop 1: Focus Areas

- Battery Life
- Unintentional DoS
- **Data Protection**
- Location Information
- Identity Management
- Mobile Application Vetting

Data Protection Recommendations

- Applications will declare data that is
  - Consumed
  - Transmitted
  - Stored
- Develop a data dictionary describing different first responder specific data types and their data

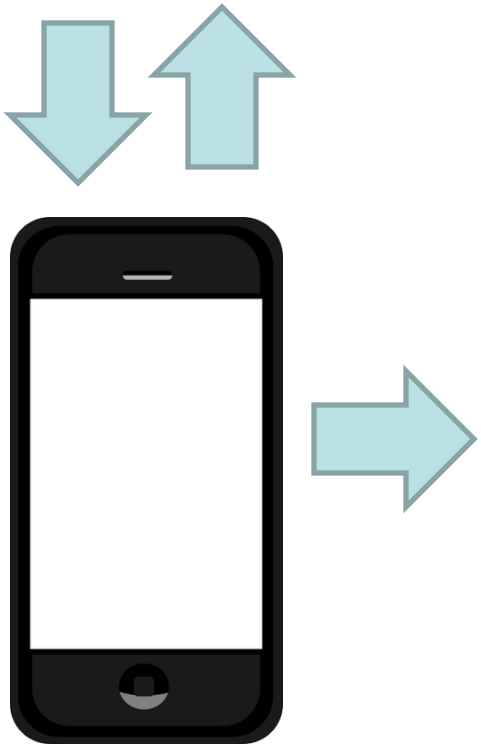
Workshop 2: Identifying Data Types



Benefits of a Data Dictionary

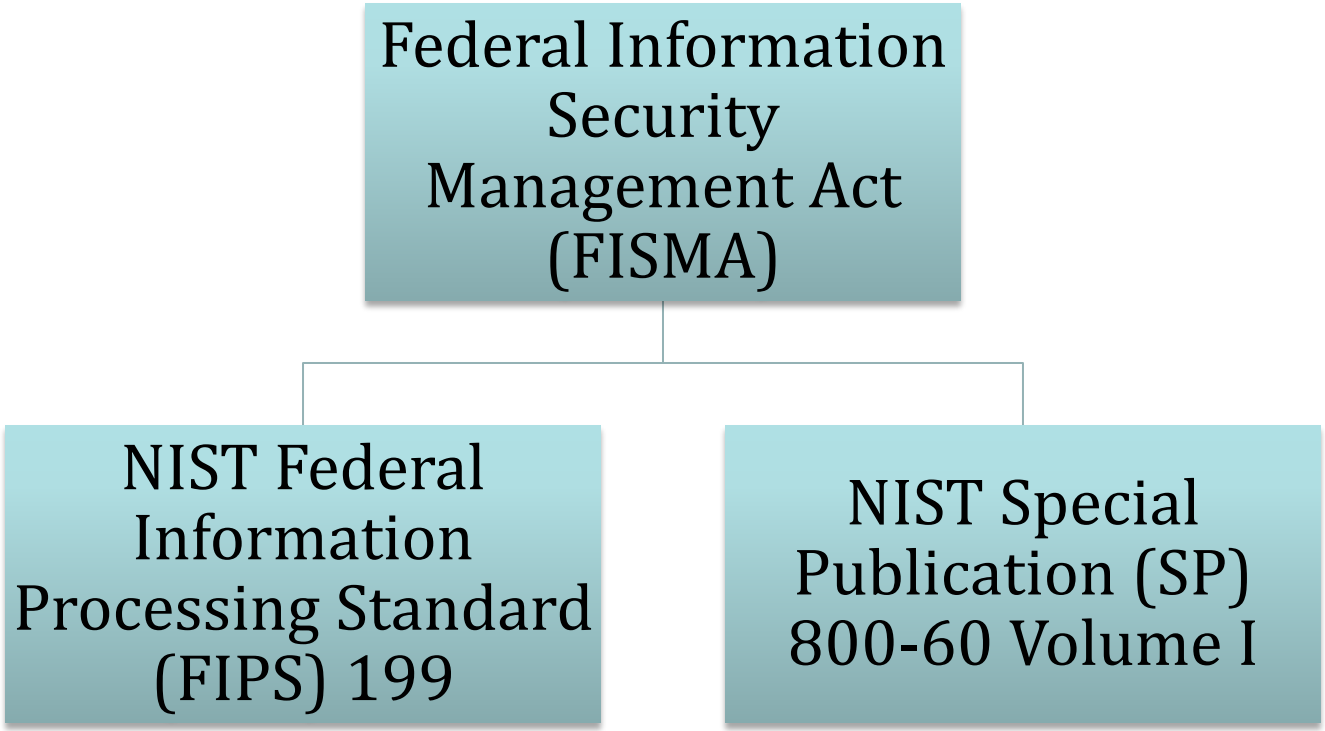
- Familiarizes developers with public safety's mission
- Provides common language
- Fosters in information sharing about apps
- Promotes interoperability
- Aids contingency and disaster recovery planning

Workshop Foundations



- What is data?
- How does data relate to cyber security?
- What data are we concerned with?

Information Security Categorization



FISMA - Security Objectives

Confidentiality

Integrity

Availability

NIST FIPS 199

- *Standards for Security Categorization of Federal Information and Information Systems*
  - Defines an information type

    A specific category of information defined by an organization, or in some instances by law, Executive Order, directive, policy, or regulation

  - Establishes levels of impact

Quantifying Impact to Security Objectives

Low

Moderate

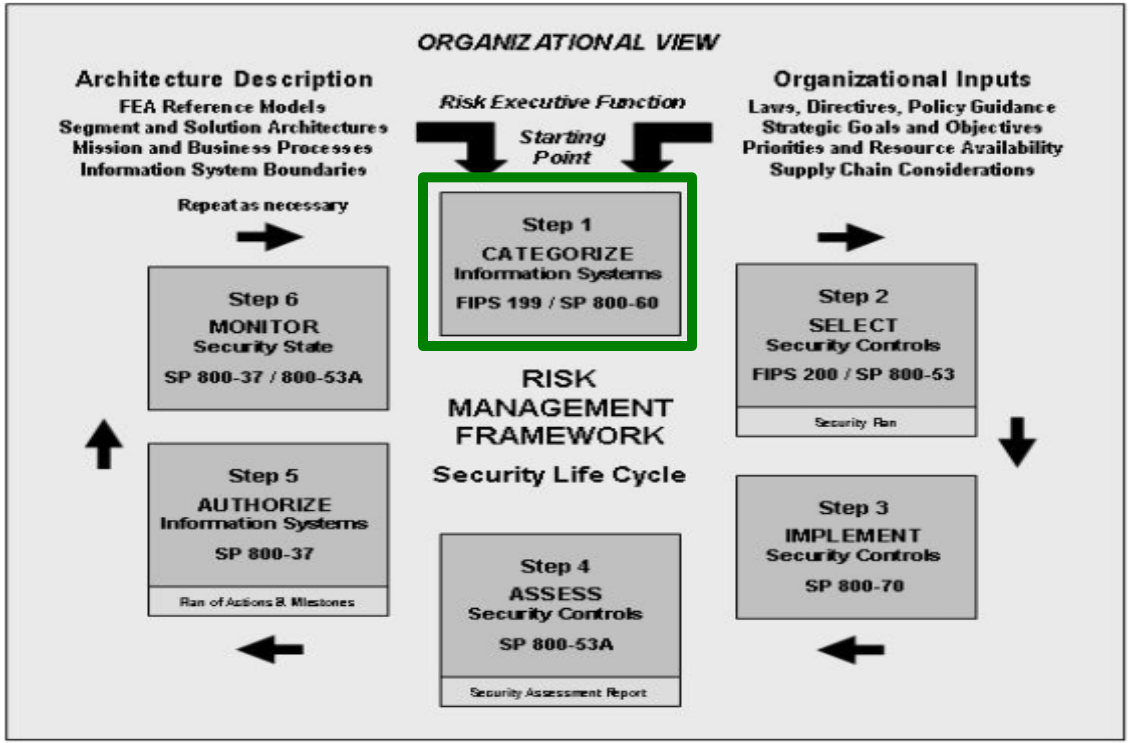
High

- Mission
- Assets
- Financial Loss
- Harm to Individuals

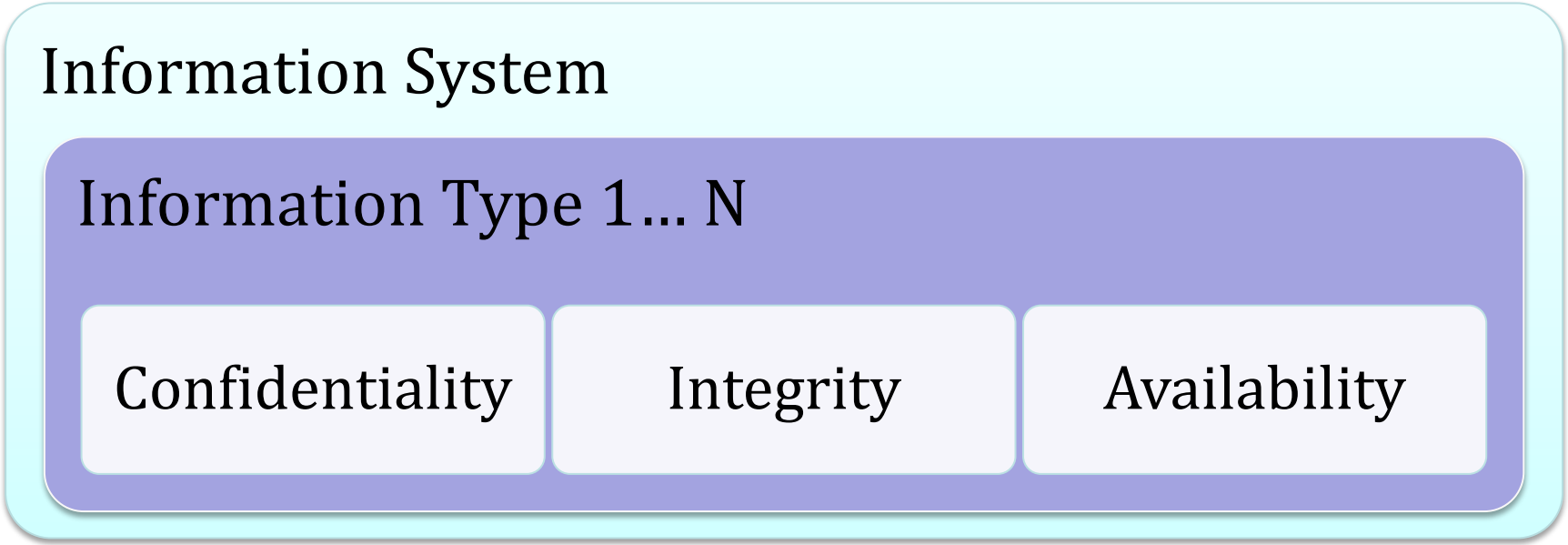
Information Security Categorization

SC information type = { (confidentiality impact),
(integrity, impact),
(availability, impact) }

NIST Risk Management Framework



Security Categorization



Information Security Categorization

SC information type = { (confidentiality, impact),
(integrity, impact),
(availability, impact) }

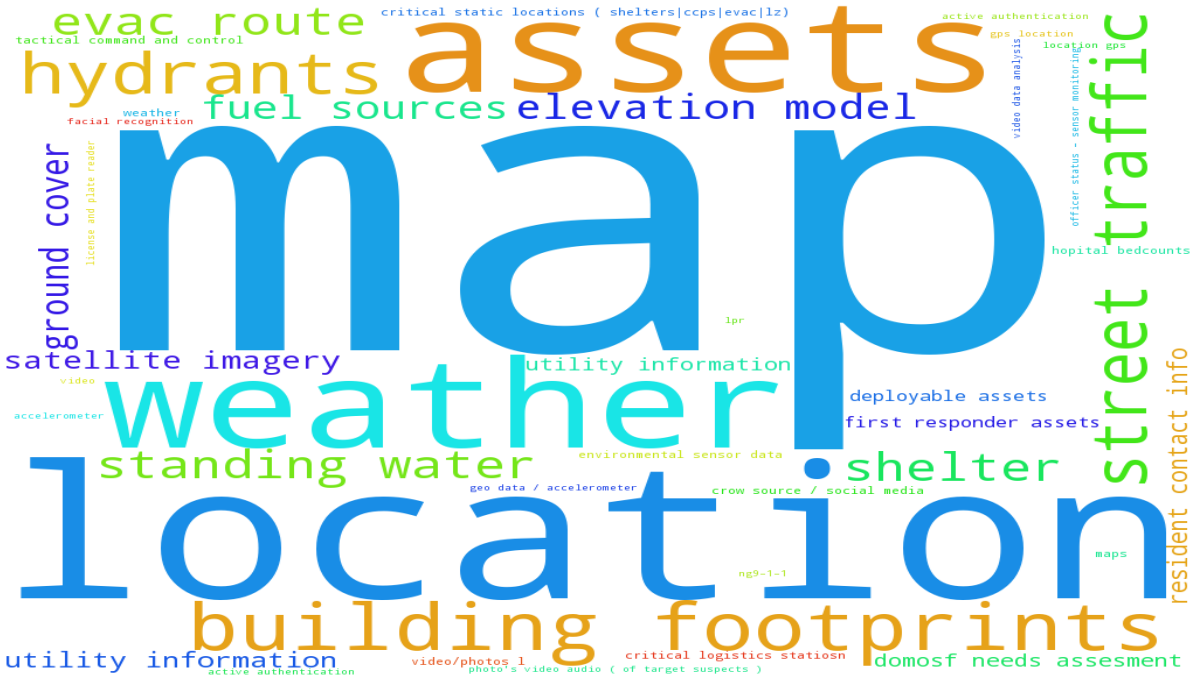
- Characterization of information
- Assessment of impact to the loss of security objectives: confidentiality, integrity, and availability
- Impact to operations, assets and individuals

Workshop Organization

- Thought experiment
  - Perfect App
  - Perfect Device
- Scenario driven
- Group driven

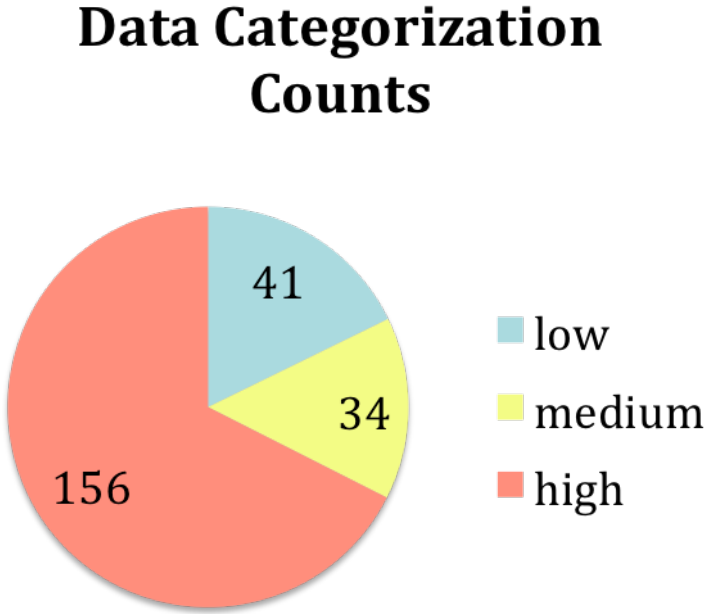
Disaster Scenarios

- Explosion at a chemical plant
- Personal injury with hazards
- Medical Emergency
- Search in a national park
- Rioting in an urban area
- Undercover officer
- Structure fire
- Wild fire
- Hurricane
- Active shooter
- Police officer vehicle stop


map
location
assets
weather
building footprints
evac route
hydrants
fuel sources
elevation model
street traffic
ground cover
satellite imagery
utility information
standing water
shelter
deployable assets
first responder assets
resident contact info
domosf needs assesment
critical static locations (shelters|ccps|evac|lz)
tactical command and control
weather
facial recognition
hopital bedcounts
video
accelerometer
environmental sensor data
geo data / accelerometer
crow source / social media
maps
ng9-1-1
video/photos_1
critical logistics statiosn
photo's video audio (of target suspects)
active authentication
gps location
location gps
video data analysis
officer status - sensor monitoring
license and plate reader
1pr

Workshop Results

- 110 data types identified
- 77 data types classified
- 4 data type groups



Data Type Groups

- Operations Data
- Situational Awareness Data
- Sensor Data
- Publicly Sourced Data

Operations Data

- Tactical Command and Control
- Incident action plans
- Deployable Assets
- GIS Intel Location
- White boarding

Operations Data

- **Confidentiality** — High
- **Integrity** — High
- **Availability** — High

Operations Data

	Low	Medium	High
Confidentiality	7	6	**27**
Integrity	1	5	**34**
Availability	2	6	**32**

Situational Awareness

- Building blueprints
- Weather
- Map data
- Hospital capacity
- DoT information

Situational Awareness Data

- **Confidentiality**
- **Integrity**
- **Availability**

Low

High

High

Situational Awareness Data

	Low	Medium	High
Confidentiality	**19**	5	4
Integrity	1	6	**21**
Availability	2	2	**24**

Sensor Data

- Environmental sensor data
- Location GPS
- Equipment sensors
- Officer status monitoring

Sensor Data

- **Confidentiality** — High
- **Integrity** — High
- **Availability** — High

Sensor Data

	Low	Medium	High
Confidentiality	1	1	**5**
Integrity	1	1	**5**
Availability	2	1	**4**

Publicly Sourced Data

- Directly from social media
- Social media pre-processors






Publicly Sourced Data

- **Confidentiality** — Low
- **Integrity** — Low
- **Availability** — Low

Thank You!

Michael Ogata
NIST
michael.ogata@nist.gov