Committee on Information Technology

Regular Meeting

March 21, 2019

1 Dr. Carlton B. Goodlett Place, City Hall, Room 305
San Francisco, CA 94102

Agenda

- Call to Order by Chair
- Roll Call
- Approval of Meeting Minutes from February 21, 2019
- Chair Update
- CIO Update
- Update: Citywide Employee Drone Policy
- Discussion: Proposed Surveillance Ordinance
- Cloud Acquisition Policy (Action Item)
- Public Comment
- Adjournment

3. Approval of Minutes

Action Item

4. Chair Update

5. CIO Update

Civic Bridge is a cohort-based program that connects City departments with pro bono talent teams from companies like Adobe, Bloomberg, Google, and Accenture, to tackle critical civic challenges.

CITY STAFF

+

CIVIC BRIDGE

PRO BONO TALENT TEAM

=

BETTER OUTCOMES FOR RESIDENTS AND CITY STAFF

2015

REDUCING VOLUME OF MISROUTED 311 REQUESTS

THE CHALLENGE

75% The ***volume 311 service requests have grown in the past 3 years***, thanks to the increasing popularity of the mobile app

20% The ***percent of requests that are misrouted***. Continued growth requires maturing the service model to meet the public's needs.

CIVIC BRIDGE SERVICES

A volunteer team from Google worked with 311 staff to:

- Analyze misrouted cases
- Develop dashboards to assess the problem
- Conduct user studies
- A/B test web and mobile app changes to reduce the volume of misrouted requests.

311 + Google

OUTCOMES

Deep analyses of **misrouted cases** including going on **ride-alongs** with City agencies and conducting **user studies** led to:

- ✔ **Developing dashboards** to assess the problem in a data-driven way.
- ✔ Introduced **machine learning techniques** to improve classification of tickets.
- ✔ **Shared recommendations** for reducing the volume of misrouted requests.

2017

IMPROVING EMERGENCY DISPATCHER HIRING + RETENTION

SFDEM
SAN FRANCISCO DEPARTMENT OF EMERGENCY MANAGEMENT

+

SFCED
San Francisco Center for Economic Development

THE CHALLENGE

Every 911 call should be answered within 10 seconds.
However, in 2017, a low of **66% of calls in SF met that standard.**

Since 2012:

- Call volume has increased by 18%
- The number of call-takers has decreased by 30%

Staffing sufficient call-takers is hard; it **takes ~9 months to train a dispatcher** and **40% of candidate drop-out is unrelated to performance**

CIVIC BRIDGE SERVICES

A volunteer team from the SF Center for Economic Development worked with DEM to:

- **Diagnose where candidates were dropping out** in the hiring process
- Identify opportunities to **increase the hiring pipeline**, **retain candidates**, and **train them more quickly**

OUTCOMES

Recommended and piloted improvements that could **add 80% more qualified dispatchers** through the hiring funnel without additional staff to execute. Changes include:

✔ Updating DEM's HR **website presence**

✔ Adding **night/ weekend testing**, **moving polygraph**, & creating **flexibility on missed dates**

✔ Making **training more experiential** by shortening classroom training, adding a digital training module, and making training more experiential

CIVIC BRIDGE: IMPACT

39

Number of Projects

~$3.78m USD

Total Financial Value of Services

~24,000

Private Sector Hours Contributed

24

Participating City Departments

15

Unique Pro-Bono Partners


Bloomberg


McKinsey&Company


FJORD
accenture


Google


Noodle.ai
ENTERPRISE AI


pwc


Digitalist


splunk>


HARVARD
BUSINESS
SCHOOL

Day of Service | mid-June

During a one-day event, teams of private-sector volunteers mobilize their skills to meet the needs of several City depts and agencies.

The Process

Pre-Program

Sourcing: The Office of Civic Innovation sources 1-day civic challenges from departments across SF City government

Matching: Companies vote on preferred civic challenges and OCI matches

Day-Of

Kickoff: Pro-bono teams meet City partners and review Day of Service challenges

Teamwork: Teams volunteer during a day-long session to deliver tactical deliverables

Wrap-Up: Celebration event to wrap-up the day

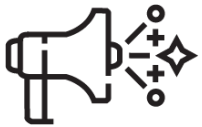
Post-Program

City department continues execution on deliverables

Types of Projects

User Research & Design | Strategy Execution | Data Collection & Synthesis | Communications & Content | Technology




Day of Service

Application Timeline

Application deadline: **Monday, April 1**

Application form: **http://bit.ly/CivicBridgeApplication**

6. Citywide Employee Drone Policy

Policy Objective

- Establish a standard form of conduct
- Layer increased protections for privacy and public safety in addition to FAA regulations
- Establish a sustainable framework for evaluation

Privacy Principles

- Transparency
- Data Minimization
- De-Identification
- Sustainable Privacy Program Management

Historical Background

DATE	EVENT DESCRIPTION
February 2015	OCA Drone Directive
September 2015	COIT Review – Public Safety vs Public Interest use
September 2016	COIT Review – Define Authorized Use Cases
April 2017	COIT Review – Additional Privacy Requirements
May 2017	COIT Final Review & Approval
September 2017	Public Utilities Commission Review & Approval
February 2018	SF Port Commission Review & Approval

Authorized Departments

Commission Approved

- Public Utilities Commission
- SF Port

Pending Commission Review

- Fire Department
- Recreations & Park

Post Disaster

- Controller's Office

Policy Details

- Each participating department is required to adopt a policy that reflects citywide requirements.

- Engaging in the unauthorized use of drones or activities that are inconsistent with this Policy may subject an officer or employee to discipline, up to and including termination of employment or removal from office, as well as to applicable monetary fines and penalties.

Policy Details

- Defined authorized uses with defined privacy impacts/mitigations
- Compliance with Federal Aviation Administration requirements
- Prohibited fly zones
- Public notice

Privacy Protections

- In the event of incidental collection of personal identifiable information, required to remove data
- Access control
- Data retention limit of 1-year
- Data sharing restrictions

Drone Summary 2018

- Authorized Departments: PUC & PRT

PUC Authorized Use Cases	PUC Locations
➢ Management of Extensive Watershed ➢ Environmental Monitoring and Documentation ➢ Infrastructure Construction Projects ➢ Survey of Bay and Ocean Outfalls	Alameda County: 5 flights San Francisco: 3 San Mateo County: 1 Tuolumne County: 2

-- All information is available on SF Open Data Portal --

Evaluation Criteria

- Operational Value
- Data Practices
- Privacy
- Public Notice & Safety
- Drone Policy Compliance

Lessons Learned: PUC Examples

- Evaluation conducted summer 2018
- Flights generally conducted in unpopulated areas, greatly diminishing privacy risks.
- Clear operational benefits.
- Contractor operated. Room for improvement in data practices.

Lessons Learned: Policy Updates

- Authorized Use form revisions
  - Justify drones are best alternative
  - Public notice details
  - Details on data retention and de-identification practices
- Noise restrictions
- Added public safety requirements for safe operations

Lessons Learned: Policy Updates

- Departments are advised not to retain data unless necessary. Live-streaming is preferred.
- Data Stewardship
  - "The City retains ownership and rights to City Data, including derivative works made from City Data and the licensing applied to the data. Contractors must treat City Data using the same Privacy and Data Security requirements that apply to CCSF employees."

THE STOP SECRET SURVEILLANCE ORDINANCE

Sponsor: Supervisor Peskin

Co-Sponsors: President Yee, Supervisor Walton

INTRODUCTIONS

- Lee Hepner, *Legislative Aide to Supervisor Peskin*
- Matt Cagle, *Attorney at the ACLU of Northern California*
- Brian Hofer, *Secure Justice*

HOW THE ORDINANCE WORKS

- Basic Premise + Context of the Proposed Legislation
- The Ordinance applies to “Surveillance Technology”
- 3 Straightforward Reports
  1. Surveillance Technology Policy
  2. Surveillance Impact Report
  3. Annual Surveillance Report
- Impact on Existing Surveillance Technology
- Facial Recognition Surveillance Technology
- Potential role of the Committee on Information Technology?
- Questions


Transparency and oversight of government use of surveillance technology builds safer communities.

A CONSENSUS APPROACH

BAY AREA: Santa Clara County (2016); Berkeley (Mar. 2018); Davis (April 2018); Oakland (May 2018); Palo Alto (Sept. 2018); BART (Sept. 2018)

NATIONALLY: Seattle (Sept. 2017); Cambridge, Massachusetts (Dec. 2018), Nashville, Tennessee, Somerville, MA, Lawrence, MA.

CALIFORNIA: 2018 California SB 1186 (Hill) (requiring local governing body oversight of surveillance tech acquisitions and use)

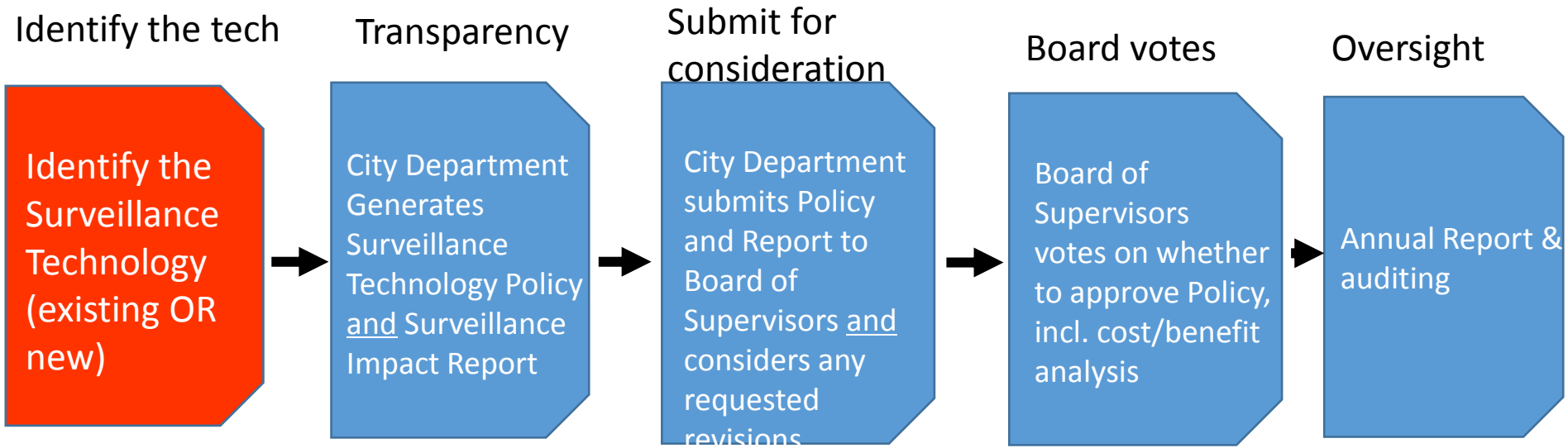
- ***Board File No. 180511*** *– Resolution Supporting SB 1186– passed by 10-1 vote*

THE PROCESS

A Department must obtain Board of Supervisors approval of the Surveillance Technology Police prior to:

- **Seeking funds** for Surveillance Technology
- **Acquiring or borrowing** new Surveillance Technology
- Using new or existing Surveillance Technology in a manner not specified in an approved Surveillance Technology Policy
- **Entering into an agreement** with a non-City entity to use Surveillance Technology

HOW THE ORDINANCE WORKS



WHAT IS “SURVEILLANCE TECHNOLOGY”?

“Surveillance Technology” means any technology – hardware or software – that is primarily intended to collect, store, or use personal information.

“**Surveillance Technology**” includes:

- Cell site simulators
- Automatic license plate readers
- Security cameras
- Wearable body cameras
- DNA capture technology
- Biometric software (face, voice, iris and gait-recognition software/databases)
- Software designed to monitor social media services
- Radio Frequency I.D. (RFID) Scanners

REASONABLE EXEMPTIONS

“Surveillance Technology” specifically exempts:

- Office hardware (TVs, computers, credit card machines, copy machines, telephones, printers)
- City databases (ex. human resource, permit, license & business records)
- IT security systems
- Physical access control systems and employee ID management systems
- Infrastructure and mechanical control systems (ex. devices that control street lights, traffic lights, electrical, natural gas, or water or sewer functions)

REASONABLE EXEMPTIONS

"**Surveillance Technology" specifically exempts (pt. 2):**

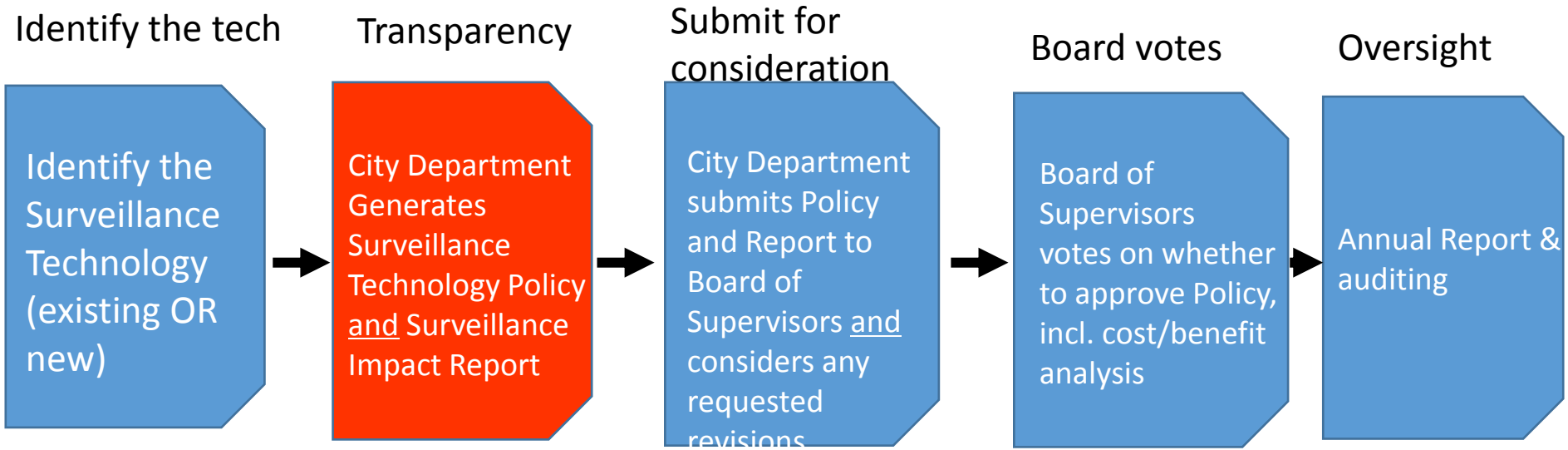
- Personal communication devices and email systems
- Parking ticket devices
- Police Dept CAD, records/case management, Live Scan, DMV, 9-1-1 dispatch and emergency service systems
- Computers, software, hardware or devices used to monitor the safety and security of City facilities and their occupants

PROCESS EXEMPTION

??EXIGENT CIRCUMSTANCES??

In the case of an emergency involving imminent danger of death or serious injury, Departments may temporarily acquire or use Surveillance Technology solely to respond to the emergency.

HOW THE ORDINANCE WORKS



THE “SURVEILLANCE TECHNOLOGY POLICY”

The “Surveillance Technology Policy” is a basic statement & set of rules governing how a City Department uses that Surveillance Technology.

The Policy must include:

- A **description of the technology itself** (manufacturer, model number, service provider, etc.)
- The **purpose of the Surveillance Technology**, including the types of data that may be collected by the technology
- **Authorized uses** of the technology, and **prohibited uses** of the technology
- The **length of time** that data will be retained
- **Access controls** and categories of individuals authorized to use the technology.

THE “SURVEILLANCE TECHNOLOGY POLICY”

The Surveillance Technology Policy also includes:

- An explanation of **data sharing** practices
- Information about required **training** for users
- A procedure for **receiving public input**, complaints, and questions

THE “SURVEILLANCE TECHNOLOGY POLICY”

Review sample Surveillance Technology Policies…

THE “SURVEILLANCE IMPACT REPORT”

A “Surveillance Impact Report” is submitted at the same time as the Surveillance Technology Policy and includes:

- How the Surveillance Technology works (e.g., a product description)
- The **purpose** of the Surveillance Technology
- The **general location(s)** that the Surveillance Technology may be deployed
- Any **potential impact on civil liberties and civil rights**, including safeguards to protect civil liberties and civil rights
- The **fiscal costs**, including purchase price, personnel and ongoing costs, and current or potential sources of funding
- Any evidence of **unanticipated costs**, or abuses of civil rights or civil liberties through use of the technology

County of Santa Clara
Office of the Sheriff

Body Worn Camera (BWC)
Anticipated Surveillance Impact Report

Attachment: BWC - Anticipated Surveillance Impact Report (84164 : Body Worn Cameras)

I. Information Describing the BWC System and How It Works

The BWC system consists of three main components: The camera itself, the docking station, and the Evidence Management System (EMS) software.

Camera

The first and most visible component of the BWC system is the camera itself, which is usually about the size and shape of a pack of standard playing cards. The camera is designed to be affixed to a deputy's uniform and is powered by an internal rechargeable battery. The deputy can start and stop recording by pressing a button on the face of the camera. The camera does not contain a screen, so video recorded by the camera cannot be displayed on it.

Some models come with a separate camera and battery pack, in which case the camera is approximately the size and shape of a tube of lipstick and is designed to be affixed to the user's glasses. The camera is connected to a battery pack worn on the user's belt with a cable. These models allow the camera to more closely capture the same field of view that is seen by the user, since the camera moves with the user's head and is aligned with the user's eyes.

Examples of various styles of BWCs

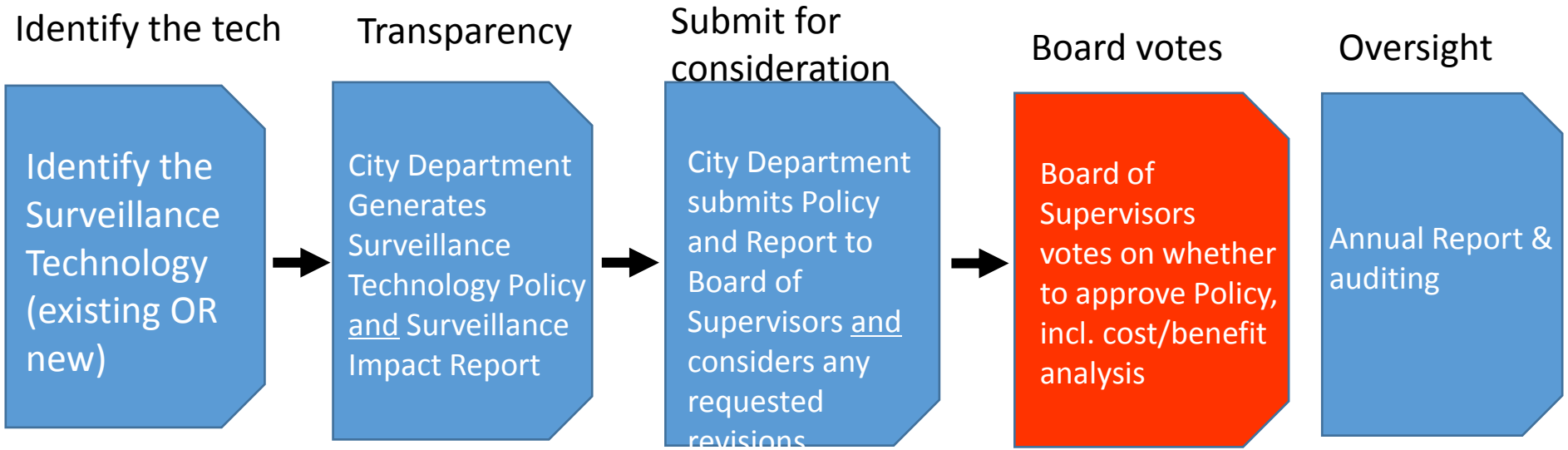
Docking Station

The second component of the camera is the docking station, which serves two purposes simultaneously: recharging the camera's battery and retrieving captured video from the camera. Both tasks are done automatically when the camera is inserted into the docking station. When the camera has finished delivering its stored videos to the EMS, the videos are deleted from the camera. Docking stations are permanently installed in appropriate work areas, and typically hold between one and ten cameras.

EMS

The third component of the system is the Evidence Management System (EMS). All video footage is uploaded to the EMS via the docking station. The EMS is typically located in cloud-based data centers for security, scalability, and ease of administration. Users can add metadata to existing videos such as associated case numbers, incident type, incident dispositions, etc. to make the videos easier to find. However, once uploaded to the EMS, the videos themselves cannot be altered by the user. Users can view

HOW THE ORDINANCE WORKS



STANDARD FOR BoS APPROVAL

In making its decision, the Board of Supervisors must find:

1. Benefits > Costs

2. Adequate Safeguards Exist Against Civil Liberties and Civil Rights Abuses

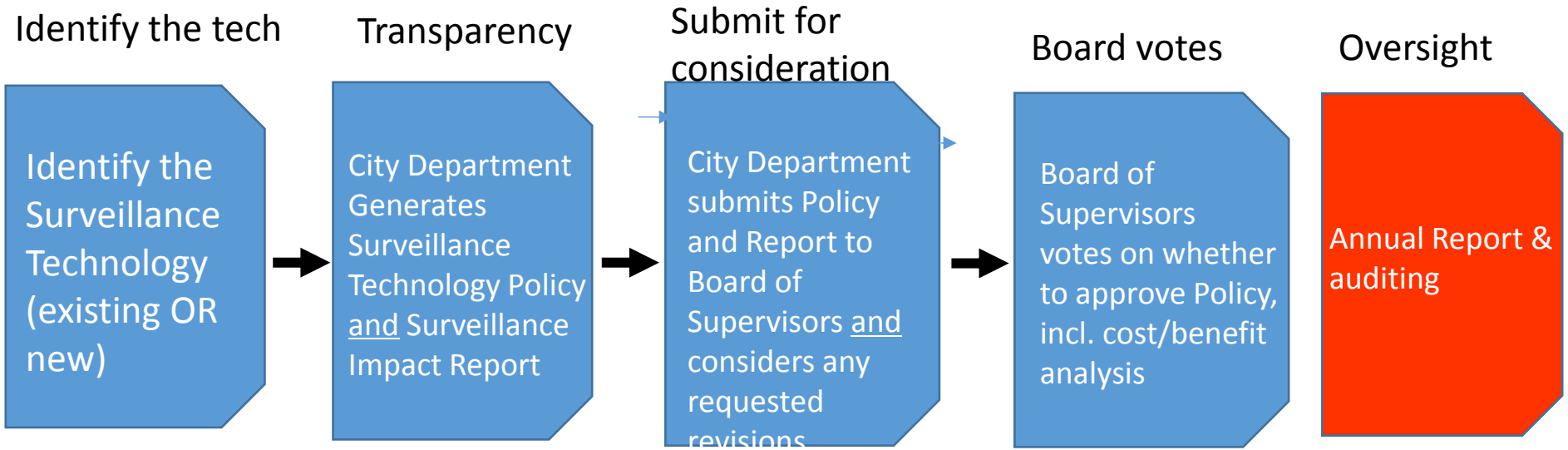
3. No Anticipated Disparate Impact on Any Community or Group

BRINGING EXISTING TECH INTO COMPLIANCE

For *existing* Surveillance Technology, City Departments have **120 days** to submit a proposed Surveillance Technology Policy and Surveillance Impact Report to the Board of Supervisors, subject to a **one-time 90-day extension**.

The Board of Supervisors has **180 days** from the date of submission to approve the Surveillance Technology Policy, otherwise use of the Surveillance Technology must cease.

HOW THE ORDINANCE WORKS



THE “ANNUAL SURVEILLANCE REPORT”

A Department that uses Surveillance Technology must submit to the Board of Supervisors an **Annual Surveillance Report**, which includes:

- How often data acquired through the Surveillance Tech was **shared** with outside entities
- A summary of **complaints or concerns** from the public
- If there was any **internal deviation** from the Surveillance Technology Policy, a general description of any actions taken in response
- Total annual **costs**, including personnel and other ongoing costs
- Any **requests for modification** of the Surveillance Technology Policy

ANNUAL AUDIT

- The Controller shall audit annually any Department use of Surveillance Technology for compliance with the approved Surveillance Technology Policy.

- The audit shall include a review of any difference between the full cost of the Surveillance Technology equipment and the total annual costs set forth in the Annual Surveillance Report.

- The Controller may recommend changes to the Surveillance Technology Policy to the Board of Supervisors.

PROHIBITION ON FACE RECOGNITION TECH

"The propensity for facial recognition technology to endanger civil rights and civil liberties substantially outweighs its purported benefits, and the technology will exacerbate racial injustice and threaten our ability to live free of continuous government monitoring."

"It shall be unlawful for any Department to obtain, retain, access, or use: 1) any Face Recognition Technology; or 2) any information obtained from Face Recognition Technology."

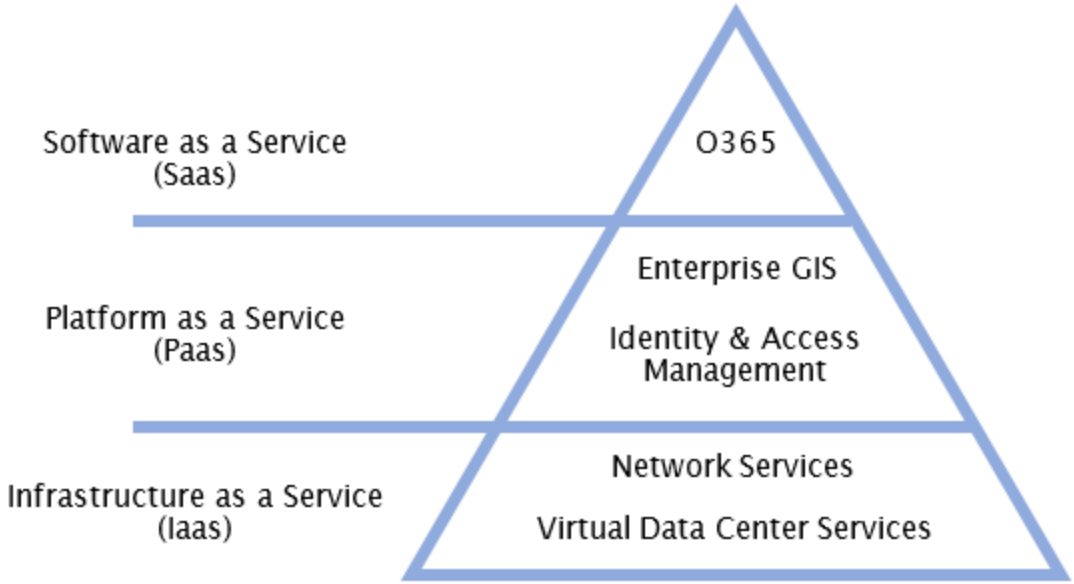

QUESTIONS?

8. Cloud Acquisition Policy

Background on “Cloud Services”

Software as a Service (SaaS): SaaS is a software licensing and delivery model by which software and/or applications are licensed on a subscription basis and centrally hosted by the software provider.

Background on “Cloud Services”



Overview

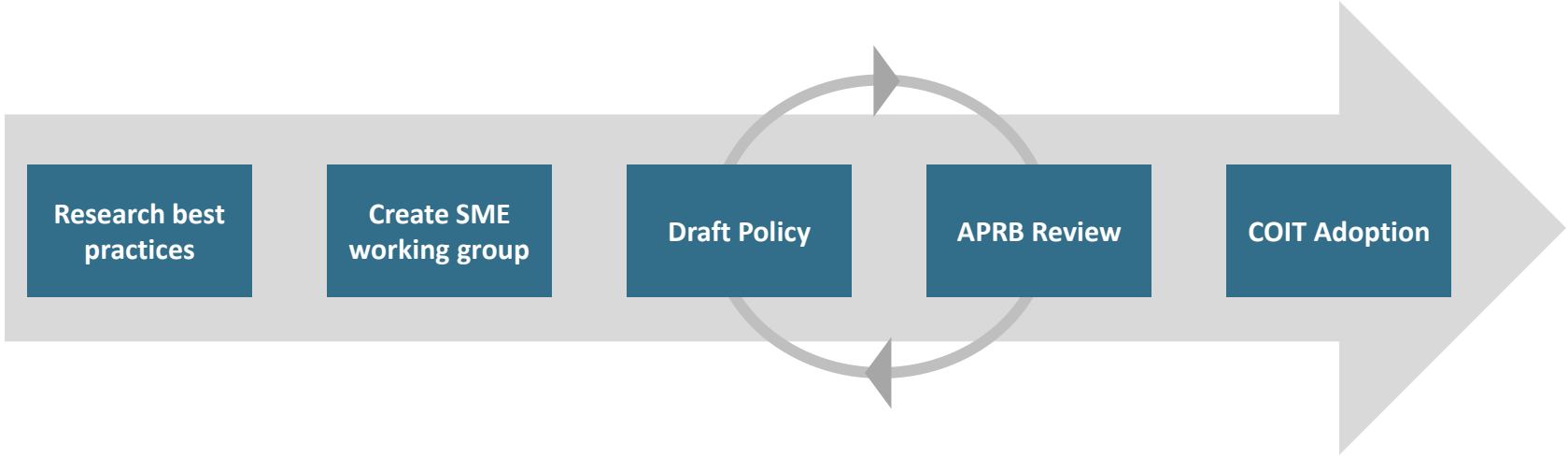
- Previous "Cloud Computing Policy" passed in 2011

- Mixes elements of a Cloud First strategy and risk management tactics

Version 2 Policy Objectives

- Address shadow IT & risks
- Clarify roles & responsibilities during procurement
- Share reference material

Policy Development Process



Process Overview

EVENT	DESCRIPTION
Architecture Policy & Review Board	APRB policy prioritization & draft policy statements (Jan 2018)
SME	3 meetings and 1 digital meeting (June – December) SME Participants: ASR, DT, DPH, DSO, HSA, OCA, PUC
Tech Community	2 week comment period
Architecture Policy & Review Board	Final review & recommendation to COIT

Policy Details

Departments are required to:

- Conduct a formal evaluation
- City employees may not provision cloud products without approval from Department IT Manager
- Use existing contracts where appropriate

Policy Details: Risk Mitigation

Departments are required to:

- Conduct risk assessment and use COIT Data Classification Standard
  - Data classified as levels 3-5 should have extra review.
- Verify data rights
- Define data retention standards
- Consider interoperability of the service

Roles & Responsibilities

Department CIO's and IT Managers:

- Review all uses of cloud services within their departments and provide approval for use where appropriate.

Department IT Security Officers:

- Conduct risk assessments for cloud products.

Department of Technology & Office of Contract Administration:

- Support departments to use appropriate procurement method for cloud services.

Appendix

Data Classification Standard

DATA CLASS	DESCRIPTION
Level 1	Data available for public access or release.
Level 2	Data that is normal operating information, but is not proactively released to the public.
Level 3	Data intended for release on a need-to-know basis. Data regulated by privacy laws or regulations.
Level 4	Data that triggers requirement for notification to affected parties or public authorities in case of a security breach.
Level 5	This data poses direct threats to human life or catastrophic loss of major assets and critical infrastructure.

PCI- DSS

Presenters:
-Office of Treasurer & Tax Collector
-Department of Technology

PCI Compliance

Agenda

- Overview
- Recent Accomplishments
- SAQ Status Summary
- Follow up & Planning

PCI Compliance

Overview

- What is PCI-DSS?
- Consequence of Non-compliance
- List of Departments Accepting Credit cards

PCI Compliance

What is PCI-DSS

- **Payment Card Industry-Data Security Standard** is a **set** of security guidelines designed to ensure that ALL organizations who handle credit cards maintain a secure environment
- Regulated by the major card brands: Visa, MasterCard, Discover, American Express, JCB
- 6 controls group; 12 requirements
- *Over 250 controls…*

Consequence of Non-Compliance

Non-compliance can result in serious consequences for the city including:

- Reputational damage
- Loss of customers (loss of tender type)
- Litigation
- Substantial fines and other financial costs
- Loss of the ability to process payment card transactions

PCI Compliance

Departments Accepting Credit Cards	-Animal Care and Control (ACC) -Arts Commission (ART) -Assessment Appeals Board (PAB) -Assessor/ Recorder (ASR) -Building Inspection (DBI) -BOS ASSESSMENT APPEALS -County Clerk -DEPARTMENT OF ELECTIONS -Dept Public Health (DPH) -Dept of Public Works (DPW) -District Attorney-Recreation and Parks- -Entertainment Commission (ENT) -Ethics Commission (ETH) -Film Commission (ECN)	-Fire Department (FIR) -GSA -Give2SF -Health Services System (HSS) -Library (LIB) -Medical Examiner -Municipal Transportation Agency (MTA) -Office of Short Term Rentals - City Planning -PORT -Public Utilities Commission (PUC) -SFGov TV -Superior Court -Treasurer and Tax Collector (TTX)

PCI Compliance

Recent Accomplishments:

- Established an Electronic Payment Governance Charter (committee consist of 8 members from different City agencies)
- Established PCI Policy (posted on TTX website @ https://sftreasurer.org/banking)
- Completed Mandatory PCI-Safety Awareness Training
- Completed Citywide Cash Handling Training
- Completed 2018 SAQs for all departments (PCI assessments)
- Completed required remediations (except for MTA & Rec/Parks)

PCI Compliance

Work in progress:

- MTA-Level 1 Merchant -ROC (Report on compliance)-Extension granted through 5/31/19
- REC & Parks-Level 3 Merchant-SAQ (Self Assessment Questionnaire) and remediations-Extension granted through 9/30/19

PCI Compliance

NOT a PROJECT but a PROGRAM!

-Add other departments requesting to accept credit cards as a form of payment
-Complete department assessments (SAQ) for YEARLY submission
-Continued monitoring of the network and remediate as needed
-Perform required device inventories and quarterly internal and external scanning
-Conduct mandatory annual trainings
-Maintain and update Citywide policy as needed
-Regular meetings/discussions with our credit card processors, gateway providers, and PCI consultants
-Continue to build awareness citywide!

10. Public Comment