Regular Meeting
April 20, 2017

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

AGENDA

1. Call to Order by Chair
2. Roll Call
3. Approval of Meeting Minutes from February 16, 2017 (Action Item)
4. Chair Update
5. CIO Update
6. FY 2017-18 & FY 2018-19 Enterprise Department Requests: Review & Action (Action item)
7. FY 2017-18 & FY 2018-19 General Fund Department Recommendations
8. San Francisco City Employee Drone Policy (Action item)
9. Discussion: Citywide Data Policy
10. Public Comment
11. Adjournment

3. Approval of Minutes

Action Item

4. Chair Update

5. CIO Update

6. FY 2017-18 & FY 2018-19 General Fund Department Recommendations

COIT BUDGET UPDATE

COIT Allocation

$ millions	FY 17-18	FY 18-19	Total
Annual Project Allocation	11.7	12.8	**24.5**
Major IT Projects	18.6	20.5	**39.1**
Total	**30.3**	**33.3**	**63.6**

Note: All figures in $ millions.

ICT PLAN STRATEGIC GOALS

- Support, Maintain, and Secure Critical Infrastructure
- Improve Efficiency and Effectiveness of City Operations
- Increase Access and Transparency to Local Government

TOTAL NUMBER OF SUBMISSIONS

- Department project requests due on January 13, 2017.

	January 13 Number of Projects	April 7 Number of Projects
Enterprise Departments	19	9
General Fund Departments	117	93
Total	**136**	**102**

REVIEW METHODOLOGY

Structure

- Highest Priority Project (rank)
- Project Plan
- Coordination with Other Departments
- Funding Sources
- Performance update on existing COIT projects

MAJOR IT RECOMMENDATION

	FY 2017-18	FY 2018-19
Major IT Allocation	18.6	20.4
Funding Recommendation	18.6	19.0
F$P	-	-
Radio Replacement	8.3	8.3
Property Assessment & Tax System	10.2	10.7

Note: All figures in $ millions.

ANNUAL PROJECT ALLOCATION

- 79 Projects requesting COIT General Fund Support.

	FY 17-18	FY 18-19
Annual Allocation	11.7	12.8
COIT General Fund Requests	30.1	30.2
DIFFERENCE	(18.6)	(17.4)

Note: All figures in $ millions.

FUNDING SCENARIOS

FY 2017-18			
Total Allocation	Total Cost	GF Request	High Scenario
11.7	51.6	30.1	11.7

FY 2018-19			
Total Allocation	Total Cost	GF Request	Scenario
12.8	33.0	25.5	2.5

Note: All figures in $ millions.

7. FY 2017-18 & FY 2018-19 Enterprise Department Requests: Review & Action (Action item)

Enterprise Project Requests

Project Title	FY 2017-18 Cost	FY 2018-19 Cost
Airport Information Integration System (AIIS)	$1,500,000	$100,000
Document Management System (DMS)	$1,250,000	-
ISO27001 Information Security Management System	$500,000	$500,000
ITIL/ISO Certification	$250,000	-
Long Term Parking Guidance and Security System	$2,750,000	-
Network Improvements	$400,000	-
Property Management & Billing System (PMBS) Phase 2	$323,725	-
Public WiFi - Terminals	$4,750,000	-
Terminal Management System Upgrade	$5,750,000	$2,500,000

CCSF Drone Policy

April 20, 2017

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

Overview

- February 2, 2015 – OCA Drone Directive
- COIT Presentations:
  - September 17, 2015
  - September 15, 2016
- March 1, 2017 - Privacy Workshop
- Departments interviewed included: City Attorney's Office, SFFD, Port, Controller, Rec & Park, SFPUC, OEWD, SFO, DPW, SFPD, and the Sherriff's Office.
- Special Thank You to Startup Policy Lab!

COIT
COMMITTEE ON INFORMATION TECHNOLOGY

Agenda

1. Policy Overview
2. Authorized Use Cases
3. Implementation
4. Evaluation

Policy Overview

The City's Drone Policy requires each department wishing to use drones to issue a department policy describing the authorized uses. Department policies must prioritize the privacy and safety of residents, businesses, and visitors of San Francisco.

Training

- FAA Remote Pilot Certificate
- Signed compliance with CCSF Drone Policy

Safety Practices

- Prohibited zones

Policy Overview

Privacy

Departments shall collect information using a drone, or use drone-collected information, only to the extent that such collection or use is pursuant to an authorized purpose only.

Data Security

- Departments are advised not to maintain archives of raw, unprocessed drone data once the business purpose is accomplished.
- To the extent departments do retain drone-collected data, Departments must restrict access to the raw drone footage to authorized staff only.
- Distribution of raw drone data is restricted to authorized departments only, defined by this policy. In all other circumstances, the City may not exchange raw, unprocessed drone-collected data between departments or disclose such data to the public except for exigent public safety needs or as required by law.
- Absent a specific Department policy, 1-year data retention standard

Authorized Use Cases

- Fire Department
- Office of the Controller
- Recreation & Parks Department
- Public Utility Commission
- Port

Authorized Use Cases – Fire Department

Incident Response:

- Building fires: identify: rescues, hot spots, hazards, structural integrity, exposures, fire progression, 5 sided view of the building, and review fire operations post-incident.
- Search and Rescue for water and cliff rescue response: Video and Thermal imaging can help identify victims in the water or stuck on a cliff. Drones can deliver flotation devices to victims in the water.

Disaster Response:

- Surveys of high occupancy sites (schools, hospitals)
- Surveys critical infrastructure
- Identify Fires, Building Collapse and victims.
- Assist in prioritizing incidents & allocation of resources

Training:

- Operator proficiency, identify drone capabilities and limitations
- Reviewing ground, water and cliff operations training evolutions

Authorized Use Cases – Fire Department

Authorized Use Cases – Parks Department

- Construction Management: Inspection of SFRPD project sites for contract and environmental compliance.
- Disaster Response & Recovery: Inspection of properties, facilities, and assets during and after disasters.
- Environmental Monitoring: Flora and fauna type and health, spills and leaks, erosion.
- Event Management: Monitor large events to document pre/post event conditions, and event operations.
- Inspections: Surveys and assessments of SFRPD properties, facilities, and assets.
- Mapping: Digital elevation models, land use maps, 3D models, contours.
- Marketing: Capture videos and still photographs.
- Search & Rescue: Reconnaissance and assist during an emergency, both for water and land operations.
- Security: Overflights and boundary patrols of SFRPD properties and assets.

Implementation

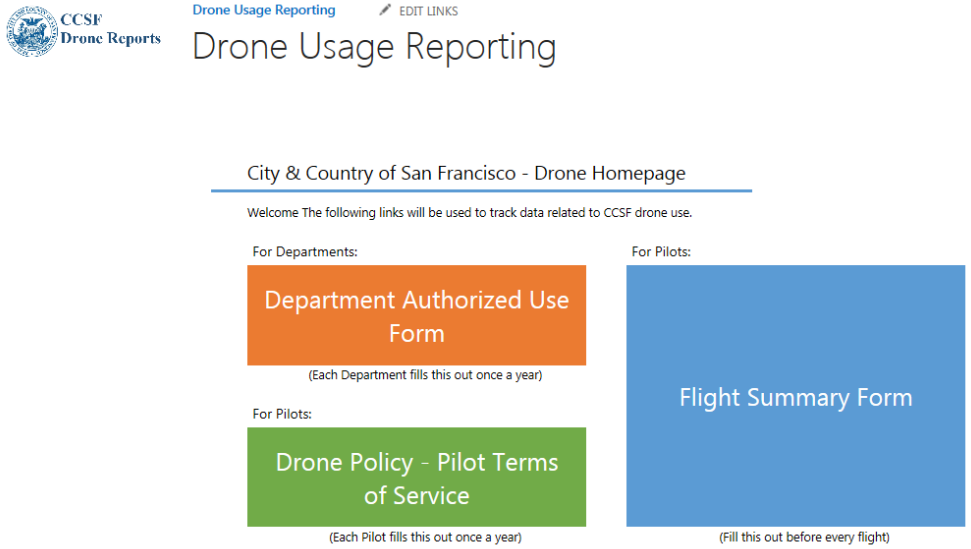
Notification

- Departments must notify the public of intended drone operations at the site of operations through signage in readily viewable public areas.

- All drone operations must be submitted at least 24 hours in advance through the Open Data portal.

Implementation

- SharePoint & Open Data



Evaluation

- Drone Oversight Committee
  - Mayor's Office
  - City Administrator
  - Committee on Information Technology

Timeline

Evaluation Period

- Date of COIT Approval until June 30, 2018

Review Focus Areas

- Impact evaluation
- Privacy practices and data retention
- Review additional authorized use cases

Data ♥'s Policy

Proposal: Data Policy

COIT

Joy Bonaguro
Chief Data Officer
City and County of San Francisco

Agenda

- Why a data policy
  - Framework for existing work
  - Challenges & Opportunities
  - Maturity framework
  - Best practices
- Data Policy Goals & Overview
- Overview of Process

A Merry collection of standards and required processes

Data Coordinators
Roles & Responsibilities

Contract terms

Open data release toolkit

Data sharing agreements

Inventory process

Metadata standard

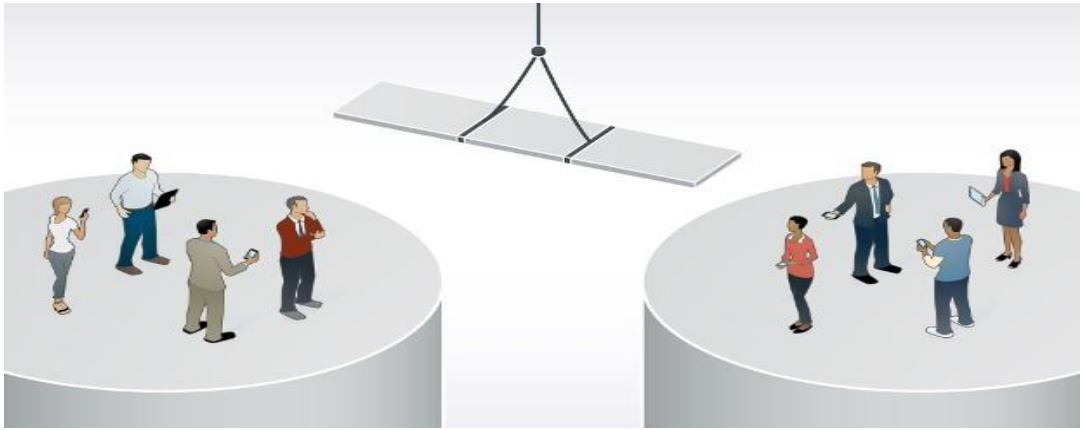
Licensing standard

In need of a tree to unite them

Challenges

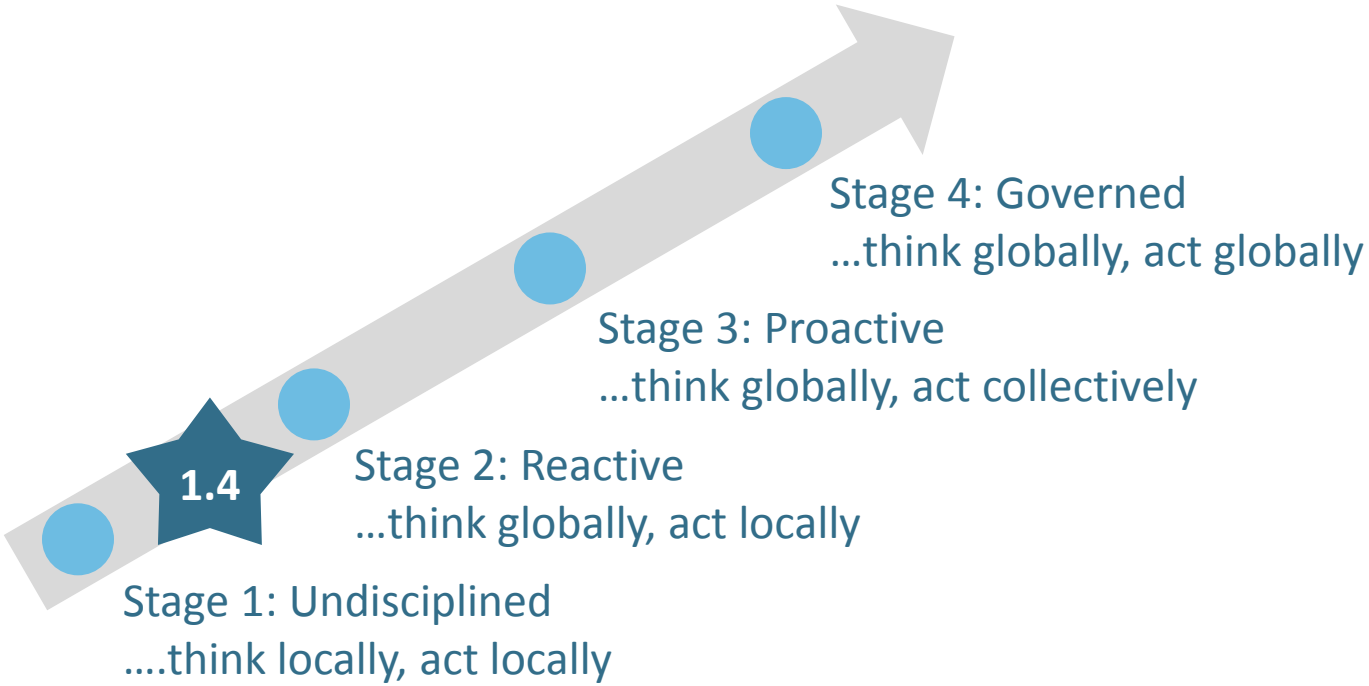
- Data silos; fragmented data governance and stewardship
  - Complex, time-consuming data integration or sharing
  - Complex regulatory control and data compliance
  - Data management and standards missing or inconsistent

Opportunities



- ✓ Data interoperability – reduce time to deliver and implementation costs
- ✓ Increase trust in government data security & use

APRB Data Maturity Quick Assessment: Results



Inspired by other jurisdictions

2014

SPARCS

Data Governance Policy and Procedure Manual

Bureau of Health Informatics
Office of Quality and Patient Safety
NYS Department of Health

Version 1.0 (Sep. 2014)

University of Colorado
Boulder | Colorado Springs | Denver | Anschutz Medical Campus

ADMINISTRATIVE POLICY STATEMENT

Policy Title: Data Governance

APS Number: 6010 **APS Functional Area:** Information Technology

Brief Description:	To ensure that data is managed as a material asset the University has established a data governance program with the goals of ensuring that data provides value, meets compliance requirements, and risks are managed appropriately. Given that poor handing of data poses a risk to the University it is necessary to define roles and responsibilities for certain types of data.
Effective:	January 17, 2013[1]
Approved by:	President Bruce D. Benson
Responsible University Officer:	Vice President of Employee and Information Services
Responsible Office:	Office of the Vice President of Employee and Information Services
Policy Contact:	Chief Information Security Officer
Supersedes:	N/A
Last Reviewed/Updated:	January 17, 2013
Applies to:	University wide

Reason for Policy: Define roles and responsibilities to enable the University to exercise positive control over the processes and methods used to handle data and assure that university employees and administrative processes have appropriate access to reliable, authentic, accurate, and timely data. Data governance authority rests ultimately with the President and Chancellors; this policy defines roles and responsibilities to assist the President and Chancellors.

I. **INTRODUCTION**

The policy covers *university records*, data where federal or state regulations exists, and data where external contract requirements exists regardless if the data is stored on a University owned or managed system or on a third party hosted service. Excluded from the scope of this policy is intellectual property that is educational materials.

II. **POLICY STATEMENT**

The program shall be managed and monitored collaboratively by University Counsel, Chief Information Security Officer, and the Council of Data Owners. Roles and responsibilities for data governance are as follows:

[1] The title of "IT Security Principals" was replaced with the title of "Information Security Officers" effective May 1, 2014.

1

City of Boston
Open and Protected Data Policy

doit

Martin J. Walsh, Mayor
Jascha Franklin-Hodge, Chief Information Officer

Open and Protected Data Policy Version: 1.0 Effective: 07/01/2015

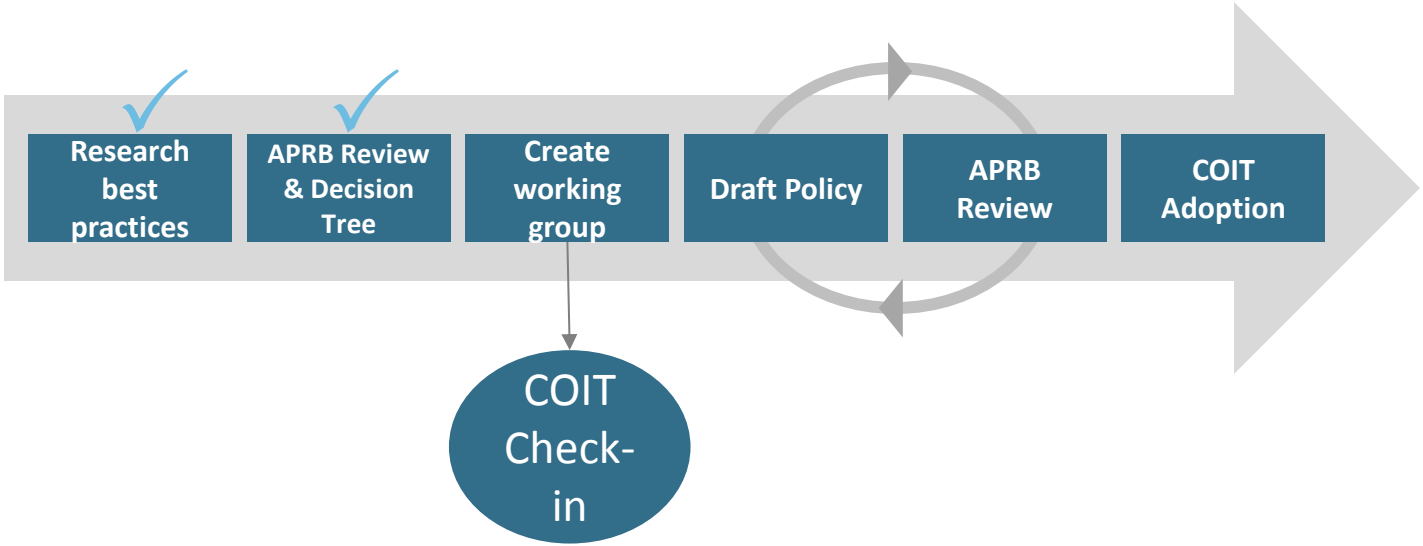
Policy Goals

- Treat data as a valuable resource
- Define and classify data
- Improve data management
- Ensure data practices respect the priorities and interests of the whole community
- Reduce costs and increase productivity and quality

Data policy overview

- Data Management
  - Data Inventory
  - Data Classification (practicing and required by cyber policy)
  - *Data Life-Cycle Management*
- Open Data
  - Publishing Plans
  - Publishing Open Data
  - Publishing Priority of Open Data
  - Open Data Licensing Standard
- Confidential Data
  - Data Protection
  - Data Sharing
- Roles & Responsibilities
  - Chief Data Officer
  - Data Coordinators
  - Data Custodians
  - Data Stewards
- Others?

Policy Making Process



Questions for COIT

- Proceed?
- If so, recommendations on working group membership
  - Program and technical

THANK YOU

@datasf | datasf.org |datasf.org/blog

10. Public Comment