Committee on Information Technology

Special Meeting
October 27, 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 September 21, 2017
4. Chair Update
5. CIO Update
6. Program Update: DataScienceSF
7. Policy Discussion: Data Classification Standard (Action Item)
8. Program Update: City Cybersecurity Office Strategic Goals and Roadmap
9. Policy Discussion: Cybersecurity Training & Awareness Standard (Action Item)
10. Public Comment
11. Adjournment

3. Approval of Minutes

Action Item

4. Chair Update

Committee On Information Technology
October 27, 2017

CIO Update, Linda Gerull

UPDATES

Project	Status
Recruiting for City Chief Cybersecurity Officer	3 candidates to on-site interviews
Facilities Construction/Move Support	1500 Mission Medical Examiner
Closing the Digital Divide	Connectivity to Public Housing Assessment of Existing CBN
New Communities of Interest Meeting	Technology Procurement Forum Help Desk Forum SalesForce Forum

UPDATES

Project	Status
Mainframe	Moved and Upgraded
Cybersecurity Insurance	Discussion on Business Impact/Risk
Network Assessment Wave 1 Completed	✓ One South Van Ness 1455 Market (Environment) ✓ 564 6th Street (Adult Probations) ✓ 617 Mission St. (Child Support Services) ✓ 25 Van Ness (Human rights Commission)
VoIP Core Infrastructure Deployment	✓ High Level Design Finalized ✓ Equipment Received Onsite ✓ Equipment being staged in Lab ✓ SIP Trunks order placed with AT&T

Office 365 Migration Update

Completed

- The O365 Migration Project completed in August 2016
- From 2011 to 2016, DT migrated 30,000+ accounts for the 54 departments that joined the project
- In September 2017, DT implemented address book synchronization with the PUC, MTA, and CAT. This provides all CCSF email users a City-wide email address book

In Progress

- PUC, CAT, and MTA each procured their own O365 tenants earlier in 2017 and are in-progress migrating their self-hosted email accounts to O365
- Once PUC, MTA, and CAT complete their migrations the 4 tenants will be able to share calendar free/busy, Skype chat, and enable cross-tenant SharePoint Online access
- DT is working towards decommissioning the remaining Notes infrastructure by Dec 2017

AWARD WINNING

CIO 100

SFO – TaxiQ

TaxiQ is the official San Francisco International Airport (SFO) short trip app for taxi drivers operating at the airport. The previous 30-minute policy incentivized taxi operators to speed. Since the introduction of the TaxiQ system and the two-hour policy change, SFO has seen a 2 percent reduction in the number of daily short taxi trips — typically 4,000 to 6,000. The new geofence-based policy eliminates the incentive to speed, removing a hazard to the public.

6. Program Update: DataScienceSF

New Service: DataScienceSF

Data Science
Applying advanced statistical tools to existing data to generate new insights

+

Service Change
Converting new data insights into (often small) changes to business processes

Smarter Work
More efficient and effective use of staff and resources

Common Project Types

Find the needle in the haystack

Priortize your backlog

Flag "stuff" early

AB test something

Format B
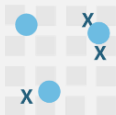
Optimize your resources
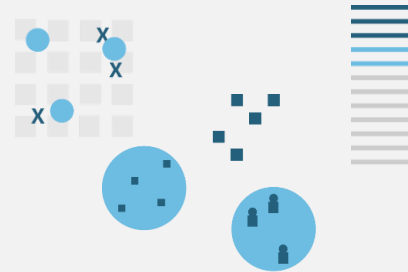
Some combination

?

Something else…

DPH WIC: Help moms and babies stay in nutrition program

Service Issue
Since 2011, DPH has seen an increase in mothers dropping out of their nutrition program. Which moms are most at risk of dropout

Data Science
Built a predictive model that identified moms and infants who are at greatest risk for dropping out

Service Change
Using the high-risk client profiles to conduct targeted interviews to identify program barriers and make service changes

Result
Expected: Reduce the dropout rate of moms, infants and children, leading to healthier outcomes

CALIFORNIA
WIC
WOMEN, INFANTS & CHILDREN
Families grow healthy with WIC

Flag "stuff" early

Visit

datasf.org/science

to learn more and apply by Nov 22!

Nothing is possible with out a fantastic team…☺

Blake
Harvard DataSmart Fellow
…and PowerBI Ninja

Jason
Open Data Program Manager
…and the ♥ of DataSF

Erica
ShareSF Program Manager
…and expert truffle hunter

Joy
Chief Data Officer
…and recent succulent propagator

Janine
Open Data Services Engineer
…and budding bird watcher

Kim
Data Scientist
…and R extraordinaire

16

Data, for the love of the City

Thank you! Questions?
@datasf | datasf.org |datasf.org/blog

Data ♥'s Policy

Data Classification Standard *COIT*

Joy Bonaguro

Chief Data Officer

City and County of San Francisco

Agenda

- Why a Data Classification Standard?
  - Formalizes existing practice
  - Information security
  - Data sharing and open data
  - Best practice
- Overview of Process
- Data Classification Standard
- Discussion and adoption

Why a Data Classification Standard?

Formalizes existing practice: Data is already being classified during the annual inventory into 3 categories

Formalizes existing practice: Data is already being classified during the annual inventory into 3 categories

Datasets by Data Classification →
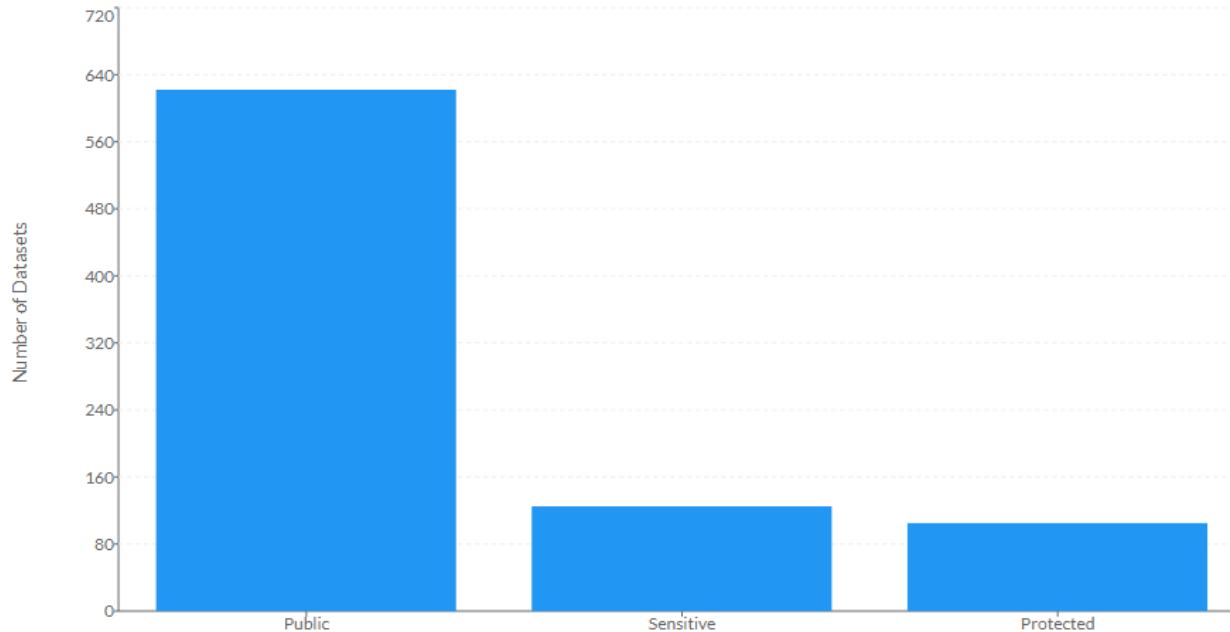
Classification scheme introduced in first data inventory in 2014

22

Information security: Classification is required by the Cybersecurity Policy to identify risky data and systems

City-wide Cybersecurity Policy

The City and County of San Francisco is dedicated towards building a strong cybersecurity program to support, maintain, and secure critical infrastructure and data systems. The following policy is intended to establish key elements to a citywide cybersecurity program.

ROLES AND RESPONSIBILITIES

1. **Department Heads** shall:

   b. To the extent possible, attempt to budget and staff the cybersecurity function for systems procured, operated, or contracted by their respective departments to ensure that all systems and the data contained by them are protected in accordance with the category / classification of the data and systems.

2. **Department Cybersecurity Security Officers / Liaisons** shall:

   a. Ensure information resources are properly protected through risk treatment strategies that meet the acceptable risk threshold for the category / classification of the information resource.

5. **Chief Data Officer** shall:

   a. Work with the City CISO to develop and maintain an information classification system and support departments in their data classification efforts.

Information Security: Why does classification matter?

- Responsible risk management requires that you match security protections with risk
  - Identify which systems need additional protection
  - Identify which systems may be overprotected
  - Tailor incident response based on impact of the data loss
- Develop plans and requirements for acquisition
  - Evaluation criteria
  - Data security terms in contracts

Classification supports informed data sharing and helps prioritize data for publication by identifying data that can easily be shared or published versus data that requires additional controls

San Francisco Administrative Code

🔖CHAPTER 22D:
OPEN DATA POLICY

(c) **City Departments.** Each City department, board, commission, and agency ("Department") shall:

   (1)   Make reasonable efforts to make publicly available all data sets under the Department's control, provided however, that such disclosure shall be consistent with the rules and technical standards drafted by the CDO and adopted by COIT and with applicable law, including laws related to privacy;

   (2)   Review department data sets for potential inclusion on DataSF and ensure they comply with the rules and technical standards adopted by COIT;

   (3)   Designate a Data Coordinator (DC) no later than three months after the effective date of Ordinance No. 285-13, who will oversee implementation and compliance with the Open Data Policy within his/her respective department. Each DC shall work with the CDO to implement the City's open data policies and standards. The DC shall prepare an Open Data plan for the Department which shall include:

Data Sharing: Why does classification matter?

- Flags data to help employees make responsible choices
- Helps reduce barriers for sharing data that is less risky
- Facilitates confidential data sharing by using the same language and similar controls for data that poses similar risks

For all these reasons, it's a best practice

Process to Develop the Standard

Overview of the process

Research best practices → APRB Review & Decision Tree → Create working group → Draft Standard → APRB Review → COIT Adoption
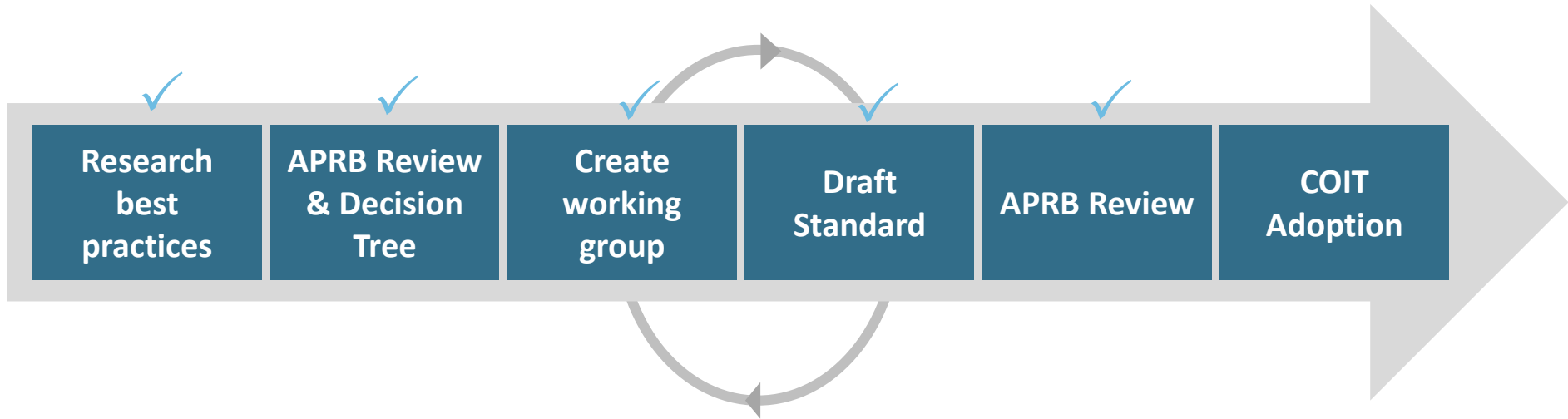
SME work group members

Overview of the Standard

Requirements

1. **Classify data** as part of the annual data inventory process...

2. **Review classification** of data on a regular basis, but no less than annually as part of the annual data inventory process set out in the Data Policy.

3. **Review and modify** the data classification as appropriate when the data is de-identified, combined or aggregated.

This standard does not alter public information access requirements. California Public Records Act or the San Francisco Sunshine Ordinance requests and other legal obligations may require disclosure or release of data from any classification.

Classification

Data class	Description	Potential adverse impact
Level 1 Public	Data available for public access or release.	None - Low
Level 2 Internal Use	**Data that is normal operating information, but is not proactively released to the public.** Viewing and use is intended for employees; it could be made available Citywide or to specific employees in a department, division or business unit. Certain data may be made available to external parties upon their request.	Low
Level 3 Sensitive	**Data intended for release on a need-to-know basis.** Data regulated by privacy laws or regulations or restricted by a regulatory agency or contract, grant, or other agreement terms and conditions.	Low - Moderate
Level 4 Protected	**Data that triggers requirement for notification** to affected parties or public authorities in case of a security breach.	Moderate
Level 5 Restricted	**This data poses direct threats to human life or catastrophic loss of major assets and critical infrastructure** (e.g. triggering lengthy periods of outages to critical processes or services for residents).*	High

*Before classifying data as Level 5 Restricted, you should speak with leadership in your department and the City's Chief Information Security Officer. Only in rare instances will data be classified at this level. For example, in the federal NIST guidance, homeland security, national defense and intelligence information is classified as "high" impact.

Data Classification Procedure

(Appendix A)
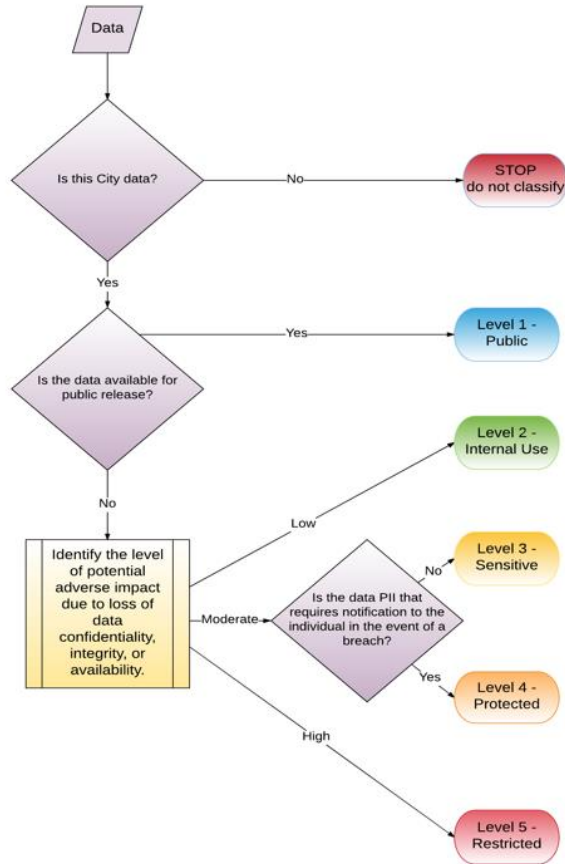
Proposed Implementation and Rollout

- Update the existing 3 level classification (public, sensitive, protected) with the new levels

- Incorporate into existing annual inventory process with additional guidance

- For departments that have only completed a system inventory, have them classify the range of data held in the system and offer assistance and consulting to finish dataset inventory

Plan Progress

Our open data legislation requires 1) an inventory of City datasets and 2) publishing plans from each department. March 31, 2015 was the target date for all departments to complete the dataset inventory. We accept department submissions on a rolling monthly basis and ask for annual revisions of the inventory. Publishing plans were due contingent on inventory completion and will be updated every year.

52 Departments

36 Inventories Complete

27 Plans Complete

Read the Publishing Plans

View Progress by Department

Inventory status

■ Complete ■ Incomplete ■ Partial Complete

Publishing plan status

■ Complete ■ Incomplete
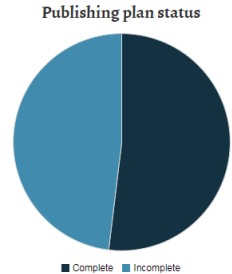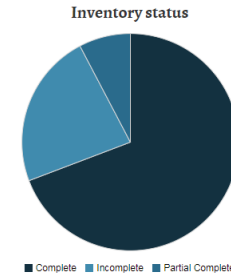
Data, for the love of the City

THANK YOU

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

CYBERSECURITY
Strategic Goals and Roadmap

SAN FRANCISCO
DEPARTMENT OF TECHNOLOGY

2017-2018 Strategic Plan
Strategic Area of Focus

3. CYBERSECURITY

Secure the City's infrastructure, network, and data by establishing strong policies and practices while integrating superior cybersecurity tools.

3.1 POLICY: Adopt cybersecurity framework to protect critical systems and data.	**3.1.1** - Establish Policies **3.1.2** - Policy Execution	
3.2 OPERATIONS: Identify, Protect, Detect, Respond, and Recover using the NIST Framework.	**3.2.1** - Security Operations Center **3.2.2** - Cybersecurity Risk Mgmt. Program **3.2.3** - Security Architecture	**3.2.4** - Resiliency **3.2.5** - Advanced Endpoint Protection **3.2.6** - Mobile Device Management DT
3.3 COIT CYBERSECURITY PROJECTS: Successfully implement COIT projects, specifically Identity and Access Management, Business Continuity/Disaster Recovery, Active Directory, and Third-Party Patching Solution.	**3.3.1** - Identity & Access Management* **3.3.2** - Citywide Active Directory*	**3.3.3** - Third-Party Patch Mgmt. Program* **3.3.4** - Business Continuity/Disaster Recovery*

SAN FRANCISCO
DEPARTMENT OF
TECHNOLOGY

Policy & Framework Roadmap

Project	Results
Cybersecurity Training	• Adopted by 42 Departments • 84% adoption rate
Cybersecurity Awareness	• Cyber Awareness Month 3 learning events (Symantec, FBI) • Developed cyber awareness website
City Cybersecurity Training & Awareness Policy	• Based on NIST Policy templates • Presented to review board • Ready for COIT approval

AVOID THE RANSOMWARE NIGHTMARE!
BE CYBER AWARE   #CyberAware
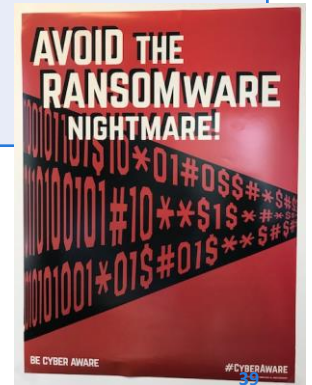
Cyber Operations Roadmap

Project	Results
Security Operations Center	• Conducting regular scans, advising departments • Incident Response: ransomware, 26 suspicious logins
Compliance	• PCI compliance - Coalfire, scans • CJIS certification of operations staff in progress • Patch management – evaluating servers, tool sets for patch management and policy
COOP & Disaster Recovery 	• DT Business Impact Analysis – essential processes, dependencies, priorities, staffing needs • Recovery Plan developed, table top exercise completed • Established a website for departments DPR3 efforts • Assisted with DEM emergency response and testing

COIT Cybersecurity Roadmap

Project	Results
Identity & Access Management	• FSP DR tests completed • Continued FSP post go-live support • IAM DR phase 1 test completed
Active Directory Upgrade	• Onboarding SF Fire and DPA completed • Engaging MicroSoft for upgrade assessment
New Project Privileged Access Management	• Access keys only for designated staff on request • All access logged, no one person "owns" the key • Products demos in progress

SAN FRANCISCO
DEPARTMENT OF
TECHNOLOGY

CYBERSECURITY
Strategic Goals and Roadmap
Look Ahead

Offer to Departments:

Device/system scanning services

Defined dashboards to quickly assess threats and situations

Mobile device management

Device encryption

Patch management

Early detection and cyber advisory services

SAN FRANCISCO
DEPARTMENT OF
TECHNOLOGY

Citywide Cybersecurity Awareness & Training Policy

Why is Cybersecurity Awareness Important?

The Risk:

- A large citywide, connected network

- The human factor in cyber risk management

- Loss of data, interruption of services, system failure

- Non-compliance with laws and regulations

- Evolving cybersecurity threats

Policy Goals/ Objectives

➢ Improve user awareness of risks.

➢ Ensure users understand their responsibilities for protecting information and systems.

➢ Develop user knowledge and skills so they can perform their jobs securely.

➢ Ensure that CCSF complies with federal, state and local government regulations for data and system security (HIPAA, CJIS, PCI).

Policy Actions

- New employees take cybersecurity training during onboarding

- System users take yearly training: On-line course, instructor led workshop, or other approved training.

- Training records retained by to the Cybersecurity Liaison and available to departmental human resources (HR) staff.

- Records retained for a minimum of 2 years from last date of completion, or longer depending on departmental requirements.

Roles and Responsibilities

City Chief Information Security Officer (CISO) – *Plan and produce yearly training*

Department Heads – *Promote and ensure compliance in their department*

Departmental Cybersecurity Liaisons – *organize, conduct and track training*

Departmental HR – *maintain training records*

City Services Auditor - *assess compliance with this standard*

Users - *complete required annual training and participate in cybersecurity awareness events*

Compliance

A department may restrict access to information systems of any user who fails to comply with the annual awareness training requirement, until the requirement is met.

10. Public Comment