COMMITTEE ON INFORMATION TECHNOLOGY

Budget & Performance Subcommittee
October 7, 2016

1 Dr. Carlton B. Goodlett Place, City Hall, Room 201
San Francisco, CA 94102

AGENDA

1. Call to Order by Chair
2. Roll Call
3. Approval of Minutes
4. Department Updates and Announcements
5. Strategy Update: FY 2018-22 ICT Plan (COIT)
6. Strategy Update: Shared Services (Dept. of Technology)
7. Strategy Update: Cybersecurity
    - Dept. of Technology
    - Airport
8. Strategy Update: Disaster Recovery (Public Utilities Commission)
9. Public Comment
10. Adjournment

3. Approval of Minutes

Action Item

4. Department Updates and Announcements

5. Strategy Update: FY 2018-22 ICT Plan

COIT

FY 2017-18 thru FY 2021-22 ICT Plan
Calendar

MONTH	GOAL	ACTIVITIES
June	Kick-Off Strategy Development	
July-Sept	Diagnose Current	Citywide Survey
October	Identify Ideal State Define Strategies & Tactics	Department Surveys External Survey Group Sessions
November	Define Strategies / Recommendations	Leadership Workshop
December	Final Recommendations	
January	Review Draft/Comments	
February	Final Approval	

COIT Dept IT Survey due October 21

6. Strategy Update: Shared Services

Department of Technology

7. Strategy Update: Cybersecurity

Department of Technology

Airport

Cybersecurity & Disaster Recovery

COIT Budget & Performance Subcommittee

SAN FRANCISCO
DEPARTMENT OF
TECHNOLOGY

Strategic Deepdive: Cybersecurity

Connectivity

Digital Service

Technology-as-a Service

Tech Talent

Cybersecurity

Cybersecurity is defined as the body of technologies, processes, practices and policies designed to protect the organization from the impact of attack, damage or unauthorized access of networks, computers, programs and data.

Cybersecurity Strategic Initiatives

Policy: Adopt cybersecurity framework to protect critical systems and data.

Operations: Identify, Protect, Detect, Respond, Recover using the NIST Framework.

Cybersecurity Strategic Initiatives: Policy

Policy: Adopt cybersecurity framework to protect critical systems and data.

Establish City-wide cybersecurity and policy standards.

Establish a procedure for policy implementation, audit, and compliance monitoring.

Action Items for FY 16-17

- Cybersecurity Policy approved by December 31, 2016
- Data & System Classification Standard, Awareness, & Training Policy.
- Risk Management Standard, Configuration Management, Incident Response Policy.
- Prepare for annual review of policies, make revisions based on implementation feedback.

Expand auditor's role in Cybersecurity Policy development and oversight.

Cybersecurity Strategic Initiatives: Operations

Operations: Identify, Protect, Detect, Respond, Recover using the NIST Framework	Action Items for FY 16-17
Create a Security Operations Center (SOC) with incident response capabilities to actively defend the City from attacks.	SOC analyst hired, procedures established, incident response plan in place, development of service offerings, integration of departments. Fully operationally capable.
Develop a Risk Management Program.	Publish Data Classification Standards, integrate department comments, finalize and implement Risk Management document.
Security Architecture: Ensure there is deliberate design around systems/data for security.	Initiate NIST Cybersecurity Framework Education, communicate design controls to Security Architecture Team, validate controls through Penetration Testing and Scans.
Resiliency & Recovery: Ensure all systems and data type criticality are considered in the Business Continuity Plan.	Disaster Recovery testing for eMerge, requirements gathering for IAM, FAMIS, F$P, execute testing, review and update Business Impact Analysis for eMerge and F$P.

Key Performance Indicators

of users that have completed the annual awareness training.

# of systems that are fully compliant with critical patching.

# of departments complying with monthly security status reports.

# of domain admin accounts within each department.

% of assets (both software and hardware) entered into CMDB.

# of systems covered by End-Point Protection.

# of emergency change controls.

Questions?

Joe Voje
Chief Security Officer
City & County of San Francisco

SFO San Francisco International Airport

SFO Cybersecurity Strategy

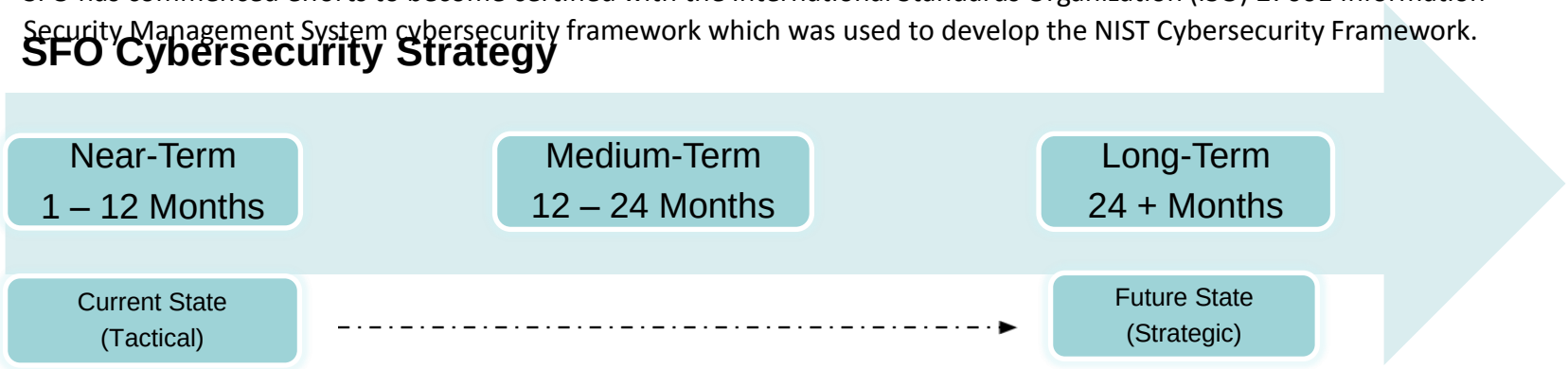
"Tactically Strategic "

Compliance with the City and County of San Francisco Cybersecurity Policy

San Francisco International Airport (SFO) fully supports the adoption of The Cybersecurity Framework, developed by the National Institute of Standards and Technology (NIST) in order to provide the methodology to secure CCSF information resources.

SFO has commenced efforts to become certified with the International Standards Organization (ISO) 27001 Information Security Management System cybersecurity framework which was used to develop the NIST Cybersecurity Framework.

SFO Cybersecurity Strategy



SFO Mission	We provide an exceptional airport
SFO Vision	Reaching for #1
Overall Goals	7 new goals
Objective	32 New Key Objectives
Initiatives	165 initiatives to support the objectives

Airport Goals

Goal 3: Be the Industry Leader in Safety and Security *(incl. physical & cyber)*

IT Policies

IT Policy 1: Underpin SFO's safety, security and cyber-security programs with state-of-the-art technology solutions.

IT Actions

Policy	Actions (include…)
Underpin SFO's safety, security and cyber-security programs with state-of-the-art technology solutions.	Implement new badge and surveillance (video) solutions. Procure SMS, mobile P.139 & Notice of Violation solutions. Achieve international cyber-security standards accreditation. Upgrade video surveillance systems.

San Francisco International Airport 5-Year Strategic Plan 2017-2021

SFO 5-Year Strategic Plan Mission, Vision and New Goals	SFO 5-Year Strategic Goal and Cybersecurity Initiatives
SFO Mission: "We provide an exceptional airport in service to our communities" SFO Vision: Reaching for #1 Overall Goals: 7 new goals Objectives: 32 New Key Objectives Initiatives: +160 initiatives to support the objectives New Goals: 1. Revolutionize the Passenger Experience 2. Achieve Zero by 2021 **3. Be the Industry Leader in Safety and Security** 4. Nurture a Highly Competitive and Robust Air Service Market 5. Be a World Class Dream Team 6. Deliver Exceptional Business Performance 7. Care For and Protect our Airport and Communities	**3. Be the Industry Leader in Safety and Security** *Safety and security is SFO's first priority. Our valued passengers, employees, airlines and tenants depend on the airport safety and security systems to provide a safe and secure travel environment. We are committed to exceeding all aviation safety and security regulations. We hold ourselves to high standards that align with our Core Values. Through the use of advanced technology, implementation of best practices and industry expert assessments, we continue to advance our safety and security profile.* **Cybersecurity Strategic Initiatives supporting this goal:** a. 3.2.3. Complete procurement for Single Sign-On Implementation. b. 3.3.1. Complete ISO27001 Information Security Management System Staff Augmentation RFP for ISO27001 Lead Implementer, original contract modification, Airport Commission approval and begin identification of scope and gap analysis. c. 3.3.2 Complete current fourteen (14) assessments & remediation of external security assessment and address all critical, (mandatory) items.

San Francisco International Airport

Near-Term
1 – 12 Months

Elementary actions that will have an immediate positive cyber security impact without "breaking the bank"

Step 1 **Use the 2014 CCSF CAU IT audit recommendations** *No cost other than staff time*	**Step 2** **Conduct vulnerability assessments** *Costs to retain an external subject matter expert*
Use the 2014 CCSF CAU IT audit which included 25 recommendations across four milestones that SFO rolled up into 6 remediation action items: 1) Improved Password Policy (stronger passwords and disabled accounts 2) Implement a comprehensive process to address critical operating systems and third-party application vulnerabilities using a centralized patch management system 3) Reduce number of users with administrative privileges 4) Secure configuration of systems 5) Improve overall architecture and implementation of internal and external network boundary points 6) Protect unauthorized movement of data across networks	Identify and risk rank critical systems in order to conduct vulnerability assessments and generate remediation action items: 1) Identify and risk rank critical information systems in preparation for vulnerability assessments 2) SFO chose to use an industry recognized set of 20 Critical Security Controls updated regularly by the Center for Internet Security:

Critical Control		Effect on Attack Mitigation
1	Inventory of Authorized and Unauthorized Devices	Very High
2	Inventory of Authorized and Unauthorized Software	Very High
3	Secure Configuration for hardware and software on laptops, workstations, and servers	Very High
4	Continuous vulnerability assessment and remediation	Very High
5	Malware Defenses	High
6	Applications Software Security	High
7	Wireless Device Control	High
8	Data Recovery Capability	Moderately High to High
9	Security Skills Assessment and Appropriate Training to Fill Gaps	Moderately High to High
10	Secure Configuration for Network Devices such as Firewalls, Routers, and Switches	Moderately High
11	Limitation and Control of Network Ports, Protocols, and Services	Moderately High
12	Controlled Use of Administrative Privileges	Moderate to Moderately High
13	Boundary Defense	Moderate
14	Maintenance, Monitoring, and Anlysis of Security Audit Logs	Moderate
15	Controlled Access Based on the Need to Know	Moderate
16	Account Monitoring and Control	Moderate
17	Data Loss Prevention	Moderately Low to Moderate
18	Incident Response Capability	Moderately Low to Moderate
19	Secure Network Engineering	Low
20	Penetration Tests and Red Team Excercises	Low

SFO San Francisco International Airport

Mid-Term
12 – 24 Months

Mid-Term 12 – 24 Months
In the Mid-term cybersecurity is "Proactively Reactive"

Objective:

1) Implement Information Systems Service Management System
2) Implement Information Security management System (ISMS)

The "What" (Action):

1) Critical systems identified and are assessed annually
2) Increase/Elevate capabilities
3) Cybersecurity Awareness Training in place and has senior management support
4) Continue to identify vulnerabilities
5) Consolidated Reports (for total visibility)
6) Continue to develop CCSF COIT & CISO cybersecurity policies/standards/procedures
7) Holistic cybersecurity architecture begins to take form in the organization. Holistic in the sense that the strategy includes threat actors, advanced telemetry of the network and a defensive strategy that continuously adapts to the adversaries capability and threat landscape
8) Governance - cybersecurity committee launches
9) Establish cybersecurity processes and practices
10) Recurring annual reviews of critical systems
11) Select, configure and deploy a Managed Security Service Provider (MSSP)
12) Partnership with SFO Enterprise Architect
13) Address CLETS/SLAN/SCADA systems
14) ISO20000 (Service Management)
15) Stakeholders engaged in design

The "How":

1) Continue to measure systems against the CSA audit checklist or have CSA conduct a new audit & checklist
2) Cybersecurity is considered part of change management process (beginning, during and at the end of the process)
3) Refresh system rankings and keep this list current and up-to-date ("evergreen")
4) Review and refresh if necessary the vulnerability assessment criteria
5) Conduct ongoing vulnerability assessments on critical systems
6) Remediation for Penetration test and vulnerability assessment items continues
7) Fill open cybersecurity positions
8) Find Cybersecurity Champions in the business
9) Choose a Cybersecurity Framework (ISO27001 and/or NIST Cybersecurity Framework)
10) Cybersecurity Awareness Training in place and has senior management support

San Francisco International Airport

Long-Term
24+ Months

Long-Term 24 + Months
In the Long-term cybersecurity is "Proactive"

Objective:

1) ISO20000 (Information Systems Service Management) is in place, operational and has been independently certified
2) ISO27001 (information Security Management System) is in place, is operational and is ready to be or has been independently certified
3) Goal of: ""Embedded"" Cybersecurity as Cultural Norm"

The "What" (Action):

1) Develop and implement cybersecurity processes
2) Cybersecurity as an agenda item for all projects and discussions
3) Vulnerability Assessment and remediation is a part of SFO culture
4) Threat analytics is in place to provide airport management with "real-time" cybersecurity posture
5) NIST Cybersecurity Framework overlay
6) Holistic cybersecurity architecture continues to mature and evolve

The "How":

1) Existing CSA audit checklist is used or new CSA audit is conducted regularly for use
2) Cybersecurity is top-of-mind in all project planning
3) Refresh system ranking and keep this list current and up-to-date ("evergreen")
4) Review and refresh if necessary the vulnerability assessment criteria
5) Conduct ongoing vulnerability assessments on critical systems
6) Annual pen tests and remediation plans continue
7) Remediation for Penetration test and vulnerability assessment items continues
8) Open cybersecurity positions are addressed as required
9) Continue to cultivate cybersecurity champions
10) Cybersecurity Framework is in place and being audited annually
11) Cybersecurity Awareness Training in place and has senior management support

Ongoing Airport Cybersecurity Efforts

SFO Cybersecurity compliance and evolution - ISO and NIST

- 2016 - 2019 – deploy ISO27001 framework and maintain compliance
- Simultaneously evaluate SFO environments using NIST Cybersecurity Framework implementing additional cybersecurity controls as appropriate
- Continue to adapt cybersecurity program to align with CCSF cybersecurity program and meet Federal aviation and transportation security requirements

Long-Term
24 + Months

Future State
(secure, compliant & evolving)

SFO San Francisco International Airport

Definitions					
Required - Priorities 1 and 2.					
Recommended - Priorities 3 and 4.					
System	Required Complete	Required Incomplete	Recommended Complete	Recommended Incomplete	Notes
Legacy SLAN Remediation Complete 12/31/16	19		12		Video cameras
AIDMS Remediation Complete Completion Date 12/31/16	13		3		Access and Identity Mgt System
CAD Remediation Complete Completion Date 12/31/16	9		3		Computer Aided Dispatch (SFO SOC)
Electrical Metering Remediation Remediation Complete 5/9/16	41		26		
Safe Mobile Application Remediation Complete 2/15/16	16		0		
Safe Mobile Audit Remediation Remediation Complete 3/18/16	18		0		
Water Treatment Plant Completion Date 11/18/16	17		10		
Mechanical Maintenance Completion Date 12/31/16	8		12		
Baggage Handling System Completion Date 12/30/16	23		40		
Airfield Lighting Remediation Completion Date 12/31/16	13		5		
Radio Systems Comm. Center	17		9		
Airinc/Vmuse System	16		3		SFO Muti-Use Terminals
Simplex Fire System Comm. Center	4		0		
Access Control Lenel/MDI/QS	0		0		
Pelco/PSIM Video Surveillance, Aviation Security CSC Assessment	0		0		
Totals	214		123		

8. Strategy Update: Disaster Recovery

Public Utilities Commission

SF Public Utilities Commission (SFPUC)

Agenda

- SFPUC Strategic Plan
- SFPUC IT COO Plan
- SFPUC DOCs
- Radios
- Handoff to Brad Taylor for IT COO implementation

SF Public Utilities Commission (SFPUC)

Strategic Plan

- Reliable Service and Assets
  - Ensure SFPUC can mitigate, respond to, and recover from threats and disasters
- Organizational Excellence
- Effective Workforce
- Financial Sustainability
- Stakeholder and Community
- Environmental Stewardship

SF Public Utilities Commission (SFPUC)

IT COO Plan

- Part of the SFPUC Continuity of Operations Plan
- **2011:** Version 1 app'd by SFPUC IT Steering Committee. Supp Budget approved for FY14/15 and FY15/16
- Daily + data geographic backup
- Networks – Finishing full SFPUC microwave link.
  PRTG Network Monitoring – view

SF Public Utilities Commission (SFPUC)

IT COO Plan

- Apps classified with status
  - Mission Critical (RTO: 0-3 Days with 4 hour target)
    - IT Infrastructure systems to support COO (e.g. AD)
    - Power scheduling
    - Customer Call Center
    - Control systems
    - Email
    - Vehicle GPS
    - Learning Management
    - Maximo – work management

SF Public Utilities Commission (SFPUC)

COO Plan

- Apps classified with status
  - Mission Critical continued (RTO: 0-3 Days with 4 hour target)
    - Gatebook – Water distribution drawings
    - Geographic Information Systems
    - Laboratory Information Management system
    - Position Control – employee info
    - eTime – timekeeping for payroll

SF Public Utilities Commission (SFPUC)

COO Plan

- Other classifications
  - Critical (RTO: 0-7 Days) – which we will promote to Mission Critical
    - Smart metering – SaaS agreement
    - Citrix
    - Customer Care & Billing
  - Essential systems (after 7 days)

Drills – Formal IT COO plan drills in November

BTW – Information Security breach drill this FY

SF Public Utilities Commission (SFPUC)

DOCs

- 3 <emergency> Department Operations Centers (DOC)
- Southeast Plant, Headquarters: 3rd and 2nd floor
  - Features
    - High Band radio, Low Band radio, radio consoles
    - Satellite internet (email), phones and TV
    - Audio Visual/ conference room videoconference
    - Personal videoconferencing
    - Ready with network hubs and wireless printing
    - Backup power
  - DOC Drills – November: Assessment without utility power. Functionality drill will follow

SF Public Utilities Commission (SFPUC)

Radios

- In SF, mostly use City radio system
- Currently, outside of SF – Low Band
- Project funded to replace Low Band. Options:
  - Lease space on a Commercial UHF non standard radio system
  - Extend the new City Motorola radio system
  - Extend the MTA Harris radio system
  - A proprietary system
  - Other

Questions?

SF Public Utilities Commission (SFPUC)

Continutity of Operations - Overview

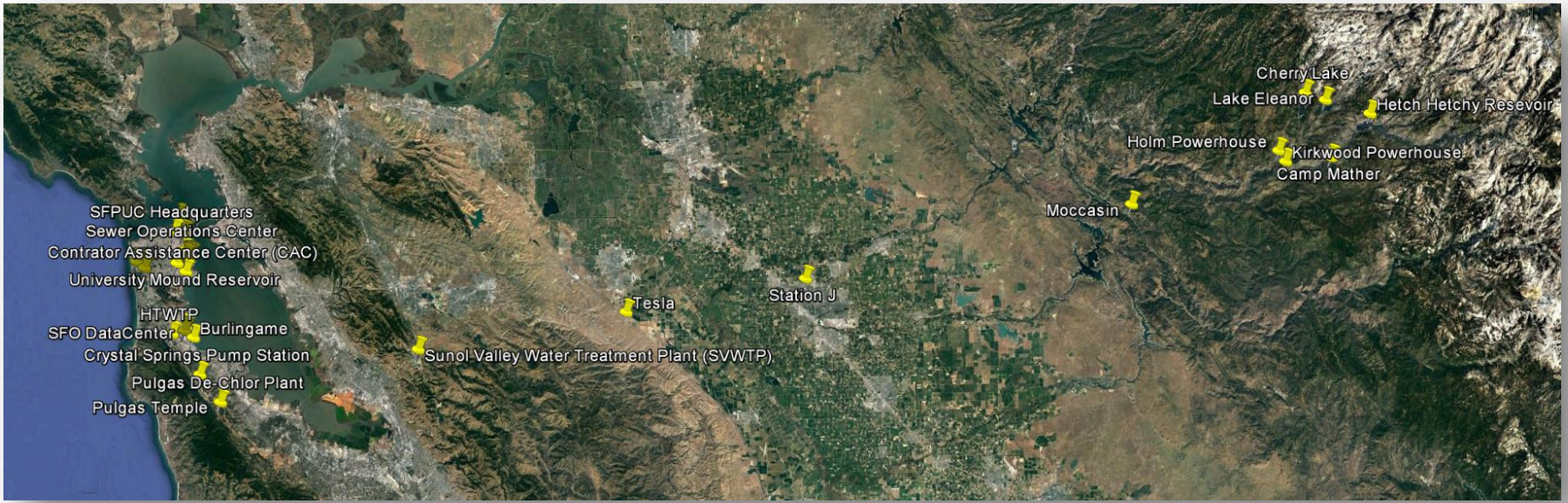
Overview/Justification

- The COO initiative provides the ability for key systems to be operational during/immediately after a major event such as a large earthquake and provides continuity of operations for various events impacting a single site, multiple sites, or an entire region.

Impact

- Enables critical system and services to be recovered and restored through local, site wide, or regional disaster events.

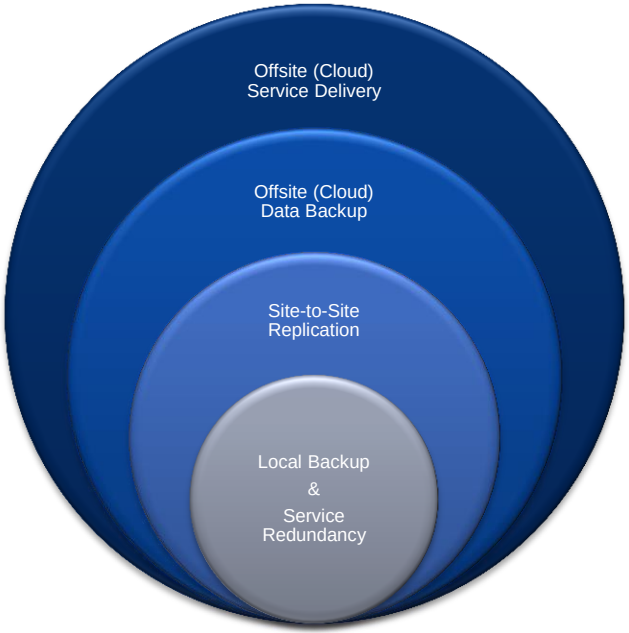
COO Solution – Scope of SFPUC



COO Solution – Defense In Depth

Layered Protection Scheme

To ensure continuity of operations across a broad spectrum of events we need to plan for local, site-wide, multi-site, as well as regional events.



Layered Protection Scheme

1º → Local data loss or hardware failure in a given location.

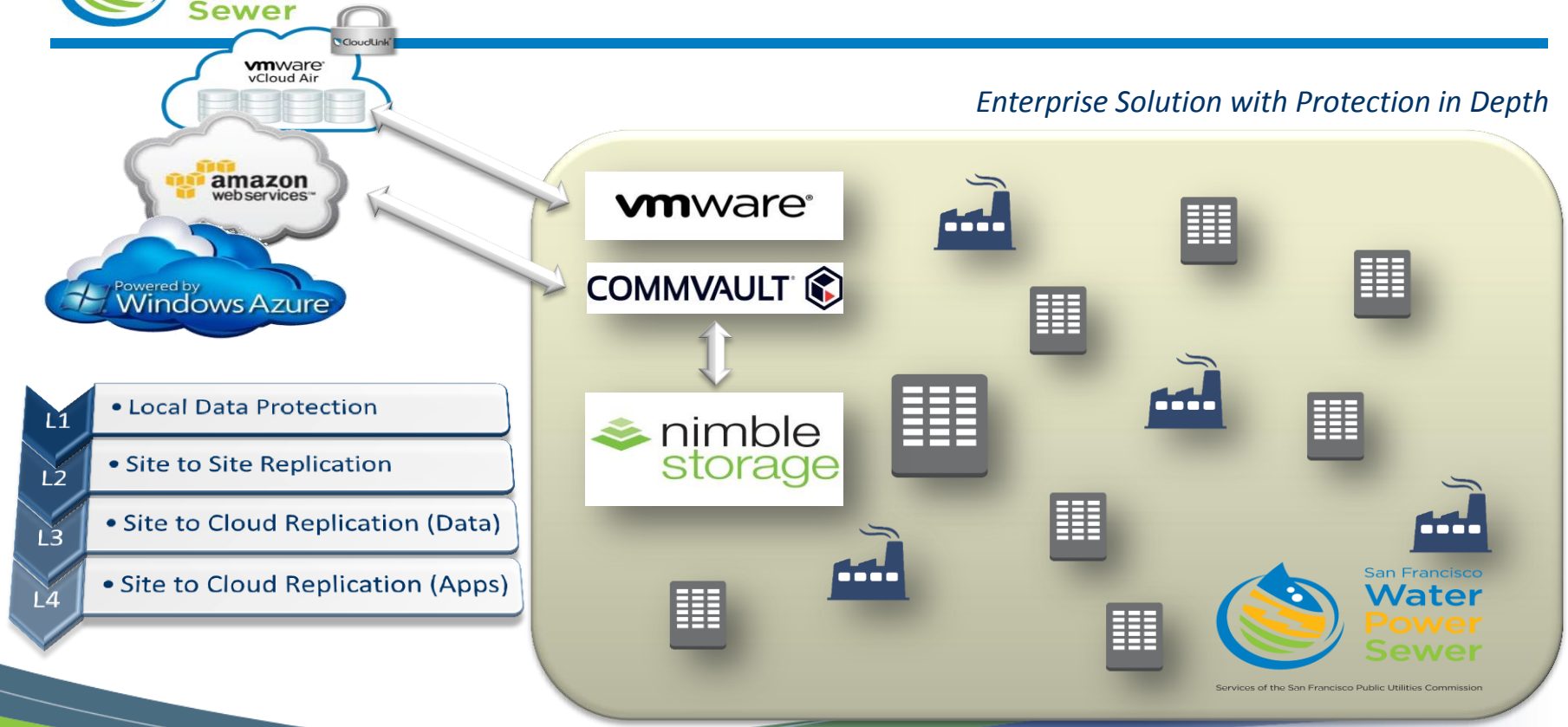
2º → Site failure or partial site failure; failover to secondary site.

3º → Multi-site failure with recovery to remaining viable site.

4º → Regional disaster; cutover to (offsite) cloud hosted services.

COO Solution – The Big Picture

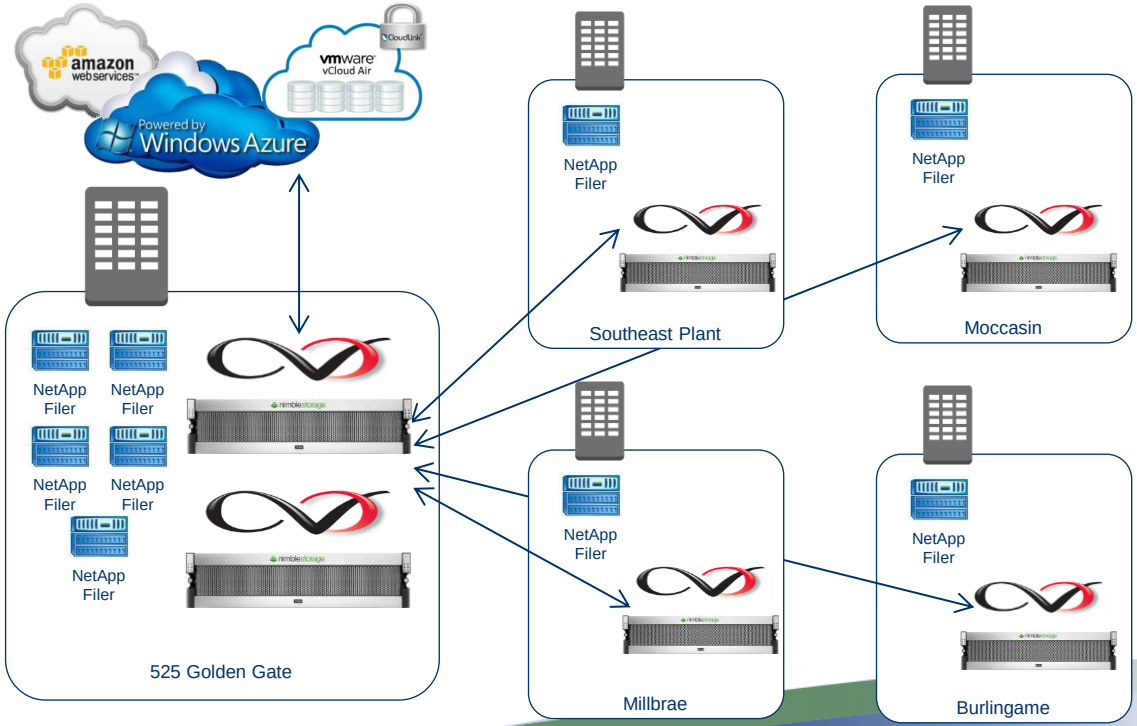
Enterprise Solution with Protection in Depth



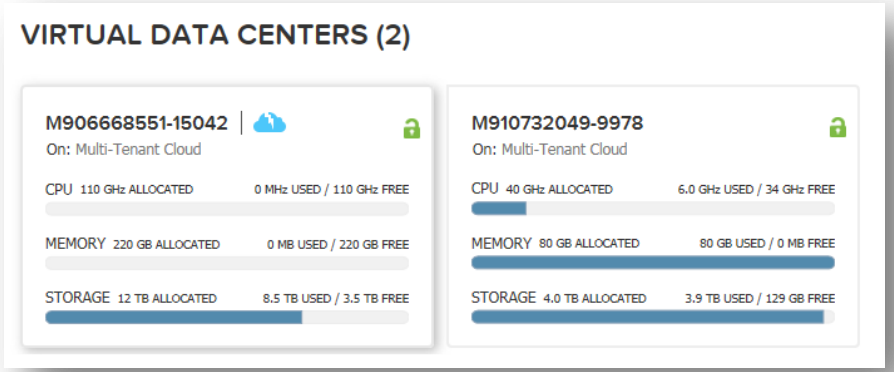
COO Solution – Current Implementation

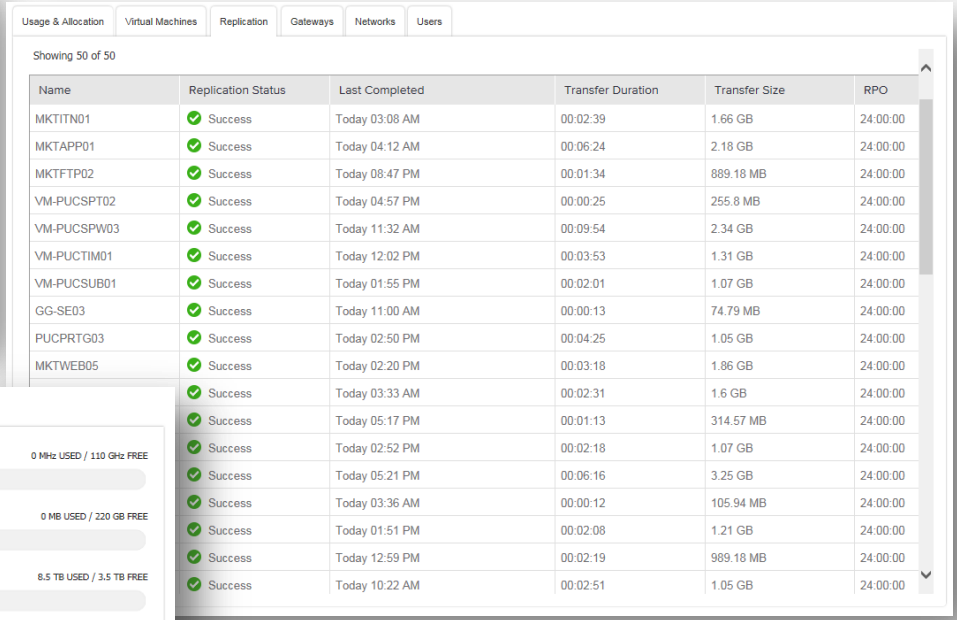
Major COO Infrastructure Components

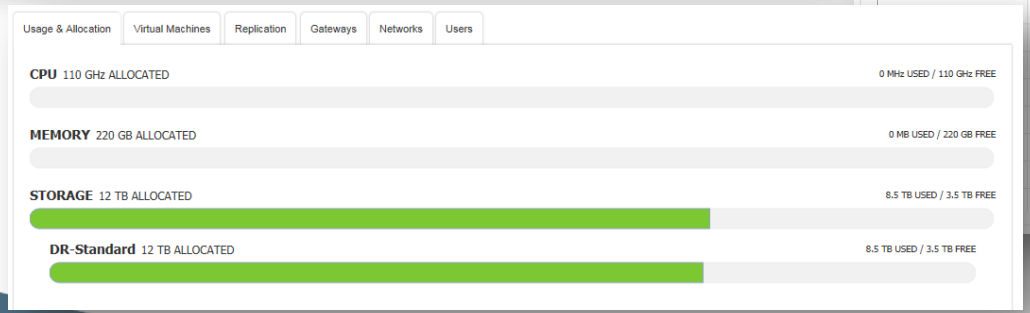
1. CommVault CommCell
   - Primary @ 525GG
   - Secondary @ Cloud
2. CommVault Media Agents
   - 525 Golden Gate
   - Southeast Plant
   - Millbrae
   - Burlingame
   - Moccasin
3. Disk-to-Disk Backup Arrays
4. CommVault CloudConnect
   - Google Nearline
   - Amazon S3 → Glacier
5. VMware Replication
   - vCloudAir DRaaS
   - Las Vegas Data Center



COO Solution – Cloud Utilization



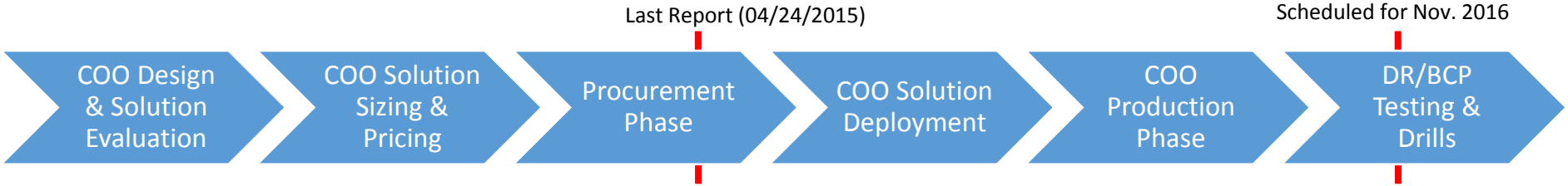




SFPUC – Continuity of Operations

Current State

Description of Implementation:



List of Stakeholders or Collaborating Departments

- SFPUC Enterprises – Water, Power, WasteWater, and Business Administration
- IT Technical Operations
- IT Enterprise Applications
- IT Business Applications
- SFPUC Business Technology Council

SFPUC – Continuity of Operations

Dashboard

Project Name: Continuity of Operations Sponsoring Department: SFPUC			
Project	**Status**	**Trend**	**Comment**
Scope	Scope Completed	On Plan	Solution spec'd and sized; procurement & implementation phases completed.
Schedule	Implementation Complete	On Plan	Procurement process slowing overall progress; anticipated completion of procurement by Q1.
Budget	On Plan	Downward	Expected overall budget savings ~ 20% below.

Project	Implementation of enterprise data protection and service availability solution to support continuity of operations in the event of service disruption at the local, site, or regional level.

COIT $ Approved	
Total Project Cost:	$2.1M
Total COIT Approved:	$2.1M
Dollar Amt Received:	--
Dollar Amt Spent:	**$1.8M**

Project Information			
GFS/NGFS Both	Start Date	% of Project Completed	End Date Planned
NGFS	02/2015	95%	**11/2016**

Risks and Issues	
Standardization is key across all business units and operating procedures.	Still working on getting some stakeholders to "let go" of their existing DR/BCP tools and technology.

Status	Planning for mid-November DR/BCP drills and testing.

9. Public Comment