City and County of San Francisco

Committee on Information Technology

Budget and Performance Subcommittee

Regular Meeting

March 03, 2023

Agenda

1. Call to Order by Chair
2. Roll Call
3. General Public Comment
4. Approval of the Meeting Minutes from February 3, 2023
5. Department Updates and Announcements
6. FY 2023-24 & FY2024-25 Budget Project Presentations
7. Proposed Schedule to Review General Fund Project Requests
8. Adjournment

Item Number 3

General Public Comment

Item Number 4

Approval of the Meeting Minutes from February 3, 2023

Action Item

Item Number 5

Department Updates and Announcements

Discussion

Item Number 6

FY 2023-24 & FY2024-25 Budget Project Presentations

Discussion

Airport Cyber-Security Program

SFO

Project: SFO CyberDefense

Committee on Information Technology
Budget & Performance Subcommittee
March 3, 2023

San Francisco International Airport (AIR)
Jonathan Kaplan, Airport CISO (acting)

Safety and Security is our First Priority

Airport Cyber-Security Program

1. What is the problem we are trying to solve?
2. What is the scope of this problem/opportunity?
3. What does success look like?
4. What is needed to be successful?
5. What business constraints are present?
6. How long will this take?

What problem we are trying to solve?

Take corrective action to address critical and high-risk vulnerabilities identified by NCC Group during the FY 2020/21 network assessment and penetration test of SFOnet.

Success looks like:

1. Keep track of everything sitting on our networks.
2. Monitor, detect and respond to anomalous activity on our networks.
3. Strengthen command and control systems for critical IT components.
4. Strengthen MFA methods for critical IT components.
5. Enhance cloud security.

Scope:	SFOnet
Timeframe:	$1.5M through FY2025/26

Business Constraints:
TSA Regulatory Framework

Department of Homeland Security (DHS)

- Transportation Security Administration (TSA)
  - 49 CFR Part 139: Certification of Airports
  - 49 CFR 1542.101: Airport Security Program (ASP)
  - 49 CFR Part 15 and 1520: Sensitive Security Information (SSI)

Historically, information security and cyber-security decisions were left to the discretion of the regulated entity…

National Amendments to the Airport Security Program

49 CFR 1542.101: Airport Security Program (ASP)

- ✈ TSA NA-21-05: Incident Reporting
  effective January 10, 2022

- ✈ TSA NA-22-01: Self-Assessments and Incident Response
  effective July 31, 2022

  - ✓ Self-Assessment Checklist (October 2022)
  - ✓ Remediation Plan (January 2023)

What is the scope of these new requirements?

Scope of TSA NA-22-01

"… the regulated entity must apply the measures contained in each applicable security program to all IT and OT systems that they are responsible to operate and maintain, irrespective of whether the systems are necessary for carrying out security program responsibilities."

TSA cyber-security requirements apply to all information technology and operation technology managed by SFO.

TSA NA-22-01:

Everything everywhere all at once…

Expand GRC capabilities:

- Resources needed to manage multiple concurrent assessments.
- Update Remediation Plan with results of each assessment.
- Support agreements must be updated to address findings.
- Assessment team may not bid against remediation contracts.
- Additional funding will be required to implement findings.

Scope:	Critical Operational Technology
Timeframe:	initial estimates, four to five years

TSA NA-22-01:
Everything everywhere all at once…

Expand Incident Response capabilities:

- Keep track of everything sitting on our networks.
- Monitor, detect and respond to anomalous events.
- Strengthen command and control systems.
- Strengthen MFA methods for critical IT/OT systems.

Align City's cyber-security and ESF-18 initiatives with Airport's federal responsibilities under 49 CFR Part 139 and 1542.

Thank you

SFO cyber-security strategy

1. In accordance with TSA NA-22-01, complete a self-assessment of critical and non-critical operational technology that, if compromised, could adversely impact Airport Operations or the Airport Security Program.

2. Create a well-defined and repeatable process for gathering the technical details needed to identify and assess the severity of technological risks associated with critical Information Technology and Operational Technology that support Airport Operations or the Airport Security Program.

3. Contract with third-party subject matter experts to augment our ability to conduct cyber-security assessment of mission-critical OT systems such as baggage handling and access control.

SFO cyber-security strategy

4. Prioritize and execute remediation plans through appropriate contracting vehicles in accordance with guidance from Contracting Administration Unit.

5. Establish capability and governance to quickly identify a major cyber-security that could adversely impact Airport Operations or the Airport Security Program, and isolate critical IT and OT systems needed to maintain necessary capacity and operational requirements under 49 CFR Part 139 and 1542.101.

6. Revise Airport Cyber-security Incident Response Plan to reduce the risk of operational disruption, or significant business or functional degradation of necessary capacity, should an aviation partner be operationally compromised as a result of a cybersecurity incident.

TSA National Amendment 22-01

"The Transportation Security Administration (TSA) is issuing this National Amendment (NA) to the Airport Security Program (ASP), TSA-NA-22-01, due to the ongoing cybersecurity threat to transportation systems and associated infrastructure to prevent against the significant harm to the national and economic security of the United States that could result from the 'degradation, destruction, or malfunction of systems that control this infrastructure.'"

TSA is quoting National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems (July 29, 2021)

San Francisco
Water Power Sewer
Services of the San Francisco Public Utilities Commission

COIT

Budget Project Presentation
FY 2023/24

March 3rd, 2023

Ramsey Williams
Chief Information Security Officer
San Francisco Public Utility Commission

San Francisco Water Power Sewer
Services of the San Francisco Public Utilities Commission

Department Goals & Potential

Citywide & Regional Benefits:

SFPUC Mission Statement:

Provide our customers with high quality, efficient and reliable water, power and Serwer services

SFPUC's Cybersecurity Program's Regional Benefits

2.7 million water customers through 26 water agencies in four bay area counties
San Francisco, Alameda, Santa Clara, and San Mateo
San Francisco's wet weather (rain) and clean water (sewer) systems
385 MW of greenhouse gas-free hydroelectric generation (Tuolumne county)
8.5 MW of solar generation capacity (San Francisco)
160 miles of clean energy transmission lines from Yosemite to the Bay Area

Mayor's Executive Directive 21-02 alignment:

Item #2 – Managed Detection & Response
Item #3 – Risk Management

ICT FYI 2022-26 Strategic Goal:

ICT: Information Communication Technology Plan
Cybersecurity protection require constant vigilance (p26)

San Francisco Water Power Sewer
Services of the San Francisco Public Utilities Commission

Why Cybersecurity Matters

Top 3 Cybersecurity Drivers @ SFPUC

Protecting Critical Water, Power and Sewer Services

Increased risk to operations due to a cybersecurity intrusion resulting from weakness in cybersecurity controls within the operational environments.

Protecting Reputation, Brand & Trust

Increased risk to credit rating used long-term infrastructure bonds due to a cybersecurity intrusion resulting from lack of focus on IT system management fundamentals.

Regulatory Compliance

Risk of penalties due to non-compliance to industry or government regulations.

Protecting Data

Increased risk of manicous intent due to inadvertent disclosure of sensitive data; failing to meet the expectation related to protection of data.

Protecting Revenue

Risk of financial impacts due to implications of a cybersecurity breach.

San Francisco Water Power Sewer
Services of the San Francisco Public Utilities Commission

Cybersecurity Priorities/Projects

1. Identity, Access & Directory Services
2. Operational Technology (OT) Security
3. OT/IT Asset Management
4. Data Governance
5. Network Management
6. Endpoint Management
7. Offline Backup
8. Mobile Device Management
9. Email Security

San Francisco Water Power Sewer
Services of the San Francisco Public Utilities Commission

Conclusion

- Strategic Planning: 2-year roadmap
  - Re-evaluate: Older solutions, program opportunities
  - Enhanced Focus: Agencywide (Emphasis on Operational Environments)
  - In alignment with:
    - Office of Cybersecurity (DT)
    - Committee on Information Technology (COIT)
    - Executive Directives (our Mayor)
    - Citywide Cybersecurity Exercise (DEM): Partnering with Emergency Planning

San Francisco Water Power Sewer
Services of the San Francisco Public Utilities Commission

Q&A

Questions

Item Number 7

Proposed Schedule to Review General Fund Project Requests

Action Item

Recap of City's Guiding Vision & ICT Goals

"Government services that are available and universally accessible in times of crisis and beyond."

ICT Goals

1. Online and Accessible City Services Residents Can Use
2. Integrated City Operations that are Efficient and Cost-Effective
3. IT Infrastructure You Can Trust

Recap of Evaluation Criteria

(1) Problem Definition: *User research, Alternatives*

(2) Strategic Alignment and Benefits: *Strategic Priority, Impact*

(3) Development Plan and Change Management: *Role of Business Prototyping*

(4) Architecture Review

(5) Department Capacity: *Staffing, Project History*

COIT Submitted Requests

82 projects submitted; 53 requesting GF support

	FY 2023-24	FY 2024-25	FY 2025-26	FY 2026-27	FY 2027-28
Total Cost (High)	113.6	91.0	27.3	6.5	2.7
Total GF Requested	**41.8**	**34.4**	**20.5**	**6.4**	**2.6**

All figures in $ millions

Summary of Projects by Recommendation

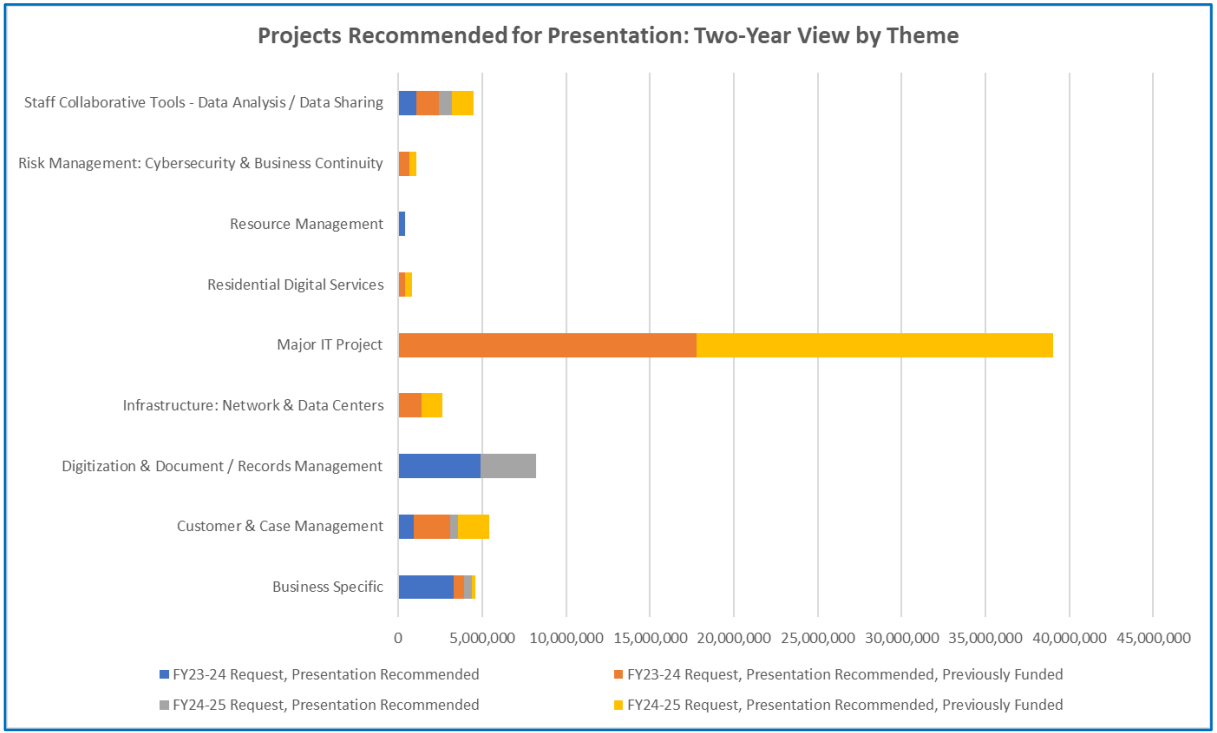
53 requesting GF support, 22 recommended to present at this time

Recommendation	FY23-24 GF Request	FY24-25 GF Request	Total 5-Yr GF Request	Total 5-Yr Cost
Further Review, Potential Presentation	3.6	0.8	4.4	4.4
No Presentation Recommended at this Time	3.2	1.9	5.5	5.8
Presentation Recommended	10.6	5.0	15.6	18.1
Presentation Recommended (Previously Funded)	24.4	26.7	80.2	89.4
Subtotal of Projects Recommended for Presentation	**35.0**	**31.8**	**95.8**	**107.5**
Grand Total	41.8	34.4	105.8	117.7

All figures in $ millions

Summary of Projects Recommended to Present

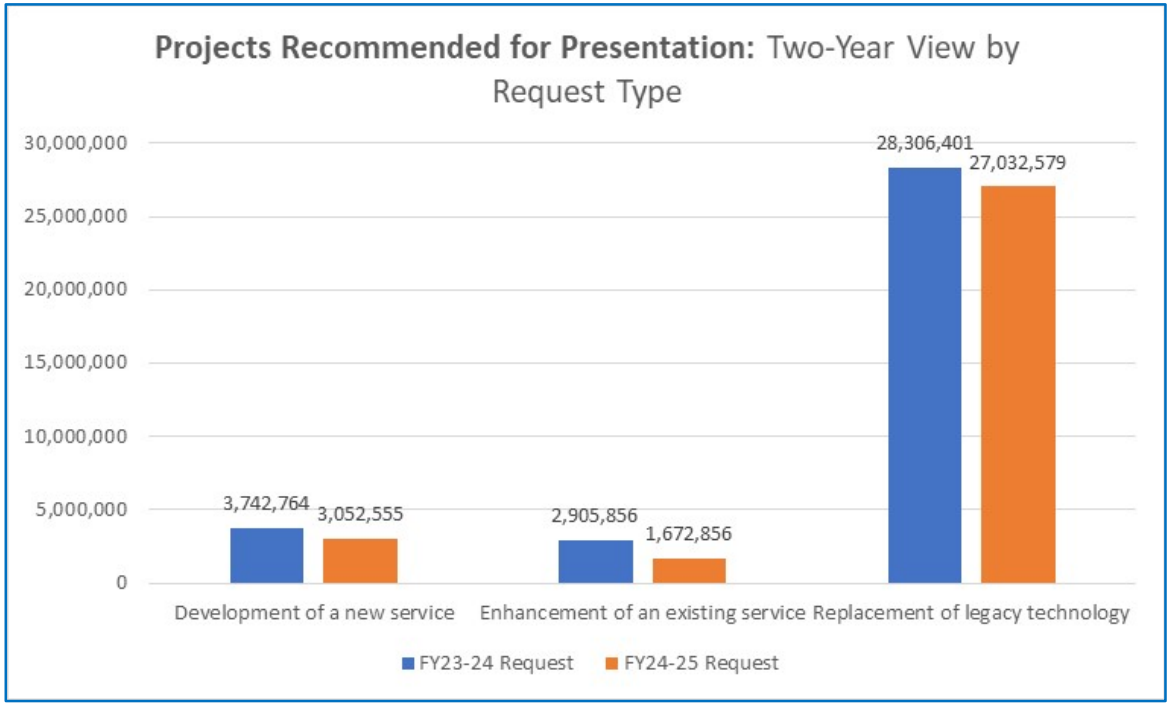
Recommendations span all 9 themes; Emphasis on Major IT, Digitization, Customer/Case Mgmt, Business Specific & Data Analysis/Sharing



All figures in $ millions

Summary of Projects Recommended to Present

Replacement of legacy technology is the dominant request type at 81% and 85% of requests by amount for FY24 and FY25 respectively.



All figures in $ millions

Presentation Recommendations (Excel File)

Proposed Presentation Schedule

Budget & Performance Sub-Committee

March 17th
Expanded Hours
(9am-12pm)

Public Safety: **DAT, SHF, POL, JUV**

Emergency Management: **DEM**

March 31st
Expanded Hours
(9am-12pm)

Public Finance:
ASR, TTX

Tech Infrastructure, Cyber-Security: **DT**

Residential Digital Services: **DS**

Replacement of Legacy Tech, Service Enhancement/ Dev:
BOS, DHR

April 7th
Expanded Hours
(9am-12pm)

Draft Funding Recs

COIT

April 20th (10am-12pm)

Final Funding Recs

Questions

Adjournment

Appendix

Five-Year Financial Forecast

From FY 2023-24 through FY 2027-28, City departments anticipate initiating 82 projects for a total of projected cost of $241.0 million.

COIT ALLOCATION	FY2023-24	FY2024-25	FY2025-26	FY2026-27	FY2027-28
No. of Projects	82	41	11	5	4
Projected Cost	$113.6	$91.0	$27.3	$6.5	$2.7

COIT Allocations Forecast

	FY 2023-24	FY 2024-25	FY 2025-26
Annual Allocation	15.8	26.2	22.7
Major IT Allocation	22.6	16.1	23.9
Total	**38.4**	**42.3**	**46.6**
Previously Committed	**28.5**		

All figures in $ millions

Note: During the FY22-23 cycle, a total of $28.5 M in allocations were made against the FY23-24 budget. This included $5.8 M in annual allocations. If maintained, these allocations would leave a total of $10M for the FY23-24 annual allocation. A total of $22,642,272 in Major IT allocations was made. The FY23-24 Major IT allocation falls short of covering these decisions by 42K. Assuming FY23-24 total funds can be used towards either allocation type, a total of $9.9 M in funds would remain.

Future Major IT costs: Ongoing, COIT-funded Major IT projects anticipate costs of 17.4M and 14.6M in FY24-25 and FY25-26.

Project Themes for GF Requests

THEME	PROJECT COUNT	YEAR 1 GF ASKS	YEAR 2 GF ASKS
Business Specific	11	4.8	1.6
Customer & Case Management	11	4.2	2.9
Digitization & Document / Records Mgmt	4	5.9	3.4
Infrastructure: Network & Data Centers	8	3.1	1.6
Major IT Project	4	17.8	21.3
Residential Digital Services	3	0.6	0.5
Resource Management	1	0.4	0.0
Risk Management: Cybersecurity & Business Continuity	8	2.5	1.0
Staff Collaborative Tools - Data Analysis / Data Sharing	3	2.5	2.2
TOTAL	53	41.8	34.4

All figures in $ millions

Major IT Allocation Projection

	FY 2023-24	FY 2024-25	FY 2025-26	FY 2026-27	FY 2027-28
GF Requests ($)	17.8	21.3	18.4	4.7	1.0
Major IT Allocation	22.6	16.1	23.9	20.0	20.0
Difference	**4.8**	**(5.2)**	**5.5**	**15.3**	**19.0**

All figures in $ millions

Annual Allocation Projection

	FY 2023-24	FY 2024-25	FY 2025-26	FY 2026-27	FY 2027-28
Number of GF Requests	49	27	4	2	2
GF Request ($)	24.0	13.2	2.1	1.7	1.7
Annual Allocation	15.8	26.2	22.7	31.2	36.3
Difference	**(8.2)**	**13.0**	**20.6**	**29.5**	**34.6**

All figures in $ millions