



MUNICIPAL MARKET DISCLOSURE

APRIL 8-9, 2025 | COSTA MESA, CALIFORNIA

SESSION ONE

The Evolving Landscape of
Municipal Disclosure

DANIEL DEATON

Partner

Nixon Peabody LLP





When Did We Learn What Good Disclosure Looks Like?

Pension Disclosure

- What happened?
- What gave rise to the disclosure failure?
- What lessons did the SEC hope we would learn?
- What did the market learn?
- What did the SEC learn?

Disclosure Policies and Procedures

- What happened?
- What made it so that the SEC was so driven that issuers would adopt policies and procedures?
- How did the market react?
- What did the SEC learn from this?

Continuing Disclosure

- What happened?
- What efforts did the SEC take to seek to fix the problem?
- How did the market react?
- Where did we get it so wrong?

Bank Loans

- What happened?
- What efforts did investors and the SEC take to fix the problem?
- How did the market react?
- What took our market so long?

COVID Disclosure

- What happened?
- What efforts did the SEC take to help us?
- Where were we confused?
- What did we learn from it?

What Has This Trajectory Taught Us?

- Investors are supposed to react to issuers – not issuers to investors.
- Whenever we turn bonds into a transaction as opposed to a relationship with investors, we are missing the point.
- Things change – and disclosure needs to change with it.
- It's critical to have a clear sense of what the law actually requires and why it requires it.

What It Looks Like to Be An Organization That is Learning Disclosure

A Learning Organization

- Do we know what we are supposed to know?
 - High-level legal “knowing”
 - Law but also what is the SEC doing and saying
 - What is going on in the market?
 - What are the hurdles that other issuers who are similarly situated struggling with, doing about their practices, and managing areas of concern
 - ***Cautionary tale***

A Learning Organization (cont.)

- How do we know that we have the right members of the team?
 - Internal team
 - Do we have the right “ownership” team who will own the process for disclosure?
 - Do we bring together the right parts of the organization to make sure we are telling the story?
 - When was the last time it changed? (frequently if the team doesn’t change it means key areas are left out)
 - External team
 - Does our external team bring together enough legal know-how, market knowledge and other expertise to complement the internal team?
 - ***Cautionary Tale***

A Learning Organization (cont.)

❖ Do we know how to tell the credit story?

- Finances and operations
 - Are we evaluating our finances and operations freshly to ensure that we know the story as that might have changed?
 - What does internal due diligence look like?
 - Think: pension disclosure escaped disclosure, could something else do that?
- Bond Terms and Security and Source of Payment
 - Do we as the issuer think we are telling the right story about the bond terms and security and source of payment?
 - Think: bank loans escaped disclosure, could something else do the same?

A Learning Organization (cont.)

- ❖ Do we know how to tell the credit story? (Continued)
 - ❖ Perspective of an investor
 - ❖ Do we understand how an investor will look at the credit story?
 - ❖ Do we understand how that may be different than other financial stakeholders?
 - ❖ Do we have appropriate sensitivity for secondary market investors as well as primary offering investors?

How Does an Issuer Assemble Its Internal and External Disclosure Team?

Assembling the Right Team

❖ Internal disclosure team

- Do we have the big picture people?
 - Much of the credit story disclosure failures came down to not having senior management in the room empowered to frame the story of the credit.
 - Who are the right people within the organization who can frame the big picture of the credit in way that enables the disclosure working group to be confident that they are not missing an “elephant in the room” just because they are not in a place to see that big picture?
 - ***Important consideration: Big picture people are not just important for facts they may know about the credit, but their perspective and vision for the credit.***

Assembling the Right Team (cont.)

- Internal disclosure team
 - Do we have the little picture people?
 - Much of the continuing disclosure failures was the lack of little picture people.
 - There needs to be a solid group of people who are focused on:
 - Are the right people reviewing the disclosure?
 - Are the policies and procedures being followed?
 - Are we paying attention to whether others in the organization should be involved?
 - ***Important consideration: The SEC has said that the single most important element to disclosure is to know who is responsible for what. This is often times a little picture exercise, not a big picture one.***

Assembling the Right Team (cont.)

❖ Internal disclosure team

- Do we have the right subject matter experts?
 - Pension disclosure in particular became problematic in large part due to the un-involvement or uninformed involvement of the pension system.
 - Whenever a topic is discussed in the disclosure, someone who is an expert in that information needs to speak for that for the issuer.
 - But this is also about looking for the right people to cover areas that are not discussed.
 - Efficiency of the process though needs to be considered – it is important not to have so many people involved that the disclosure process becomes extremely difficult to manage.

Assembling the Right Team (cont.)

- How internal disclosure teams have changed over time:
 - After pension disclosure, involved pension systems.
 - After New Jersey and related actions, creation of disclosure practices working group.
 - After MCDC, creation or further empowerment of a disclosure coordinator.
 - After COVID, increased reliance on experts on revenues.
 - After climate change concerns, capital projects and sustainability experts.
 - After cybersecurity concerns, IT security experts.
 - Going forward, increased budget experts?
 - ***It's helpful to have an annual procedure to work with your external disclosure team to consider whether other parts of the organization should be included in some fashion into the internal disclosure team.***

Assembling the Right Team (cont.)

- External disclosure team (referring to all of the working group – bankers, municipal advisors and attorneys)
 - Does your external disclosure team help to understand what you need to know?
 - Does your external disclosure team have a sense of issues that are arising outside of your organization?
 - Does your external disclosure team have a sense of the trends that should be focused on?

What is the Point?

What is the point?

❖ Disclosure is always evolving

- Finances and operations change over time and so do the key facts investors need to know.
- The SEC changes its focus and priorities over time.
- Sometimes the law actually changes.

❖ Being a learning organization comes down to evolving with those trends

- Staying current on the legal and industry trends
- Changing practices, evaluating team members, evaluating ongoing disclosure to fit where things are today regardless of what disclosure looked like before.

QUESTIONS?

DANIEL DEATON

Partner

Nixon Peabody LLP





15-MINUTE --- BREAK

SESSION TWO

Assessment and Disclosure of Changes in Long-Range Financial and Operational Conditions and Challenges



MARGARET BACKSTROM

*Managing Director
Morgan Stanley*



JAY GOLDSTONE

*Financial Services Consultant
Self-employed*



ANNA VAN DEGNA

*Public Finance Director
City & County of San
Francisco*

Assessment and Disclosure of Changes in Long-Range Financial and Operational Conditions and Challenges

MARGARET BACKSTROM

Managing Director
Morgan Stanley





Every Organization Needs to Have a Long-range Financial Plan

Importance Of Long-range Planning

- You have a “fiduciary” duty to your organization
 - If not legally, then definitely professionally
- Without a long-term financial plan, how do you know:
 - Where you are financially
 - What the financial future looks like
 - Is your organization on financially sound ground
 - Do you need to make a course correction

Do You Have Outstanding Debt?

- You may need to inform the markets
 - This is a legal (contractual) obligation
- Is your variance material?
- What are the service implications?

Preparing The Financial Plan

- The Plan does not need to be complex
- Should contain key revenue and expenditure components
- Make sure to capture future events
- Labor Agreements
- Facilities coming online
- Known/projected changes to revenues
- Should capture at least a five-year picture
- Clearly discuss your assumptions
- Update at least annually, but monitor monthly/quarterly
- Present annually to your governing board
- **A simple PLAN is better than no PLAN**



What Do You Need To Pay Close Attention To?

Revenues

- Know your key drivers (perhaps your top 3 or 4 that could make or break your budget)
 - Property Tax
 - Sales Tax
 - Transient Occupancy Tax
 - Utility User Tax
 - Franchise Fees
 - Etc.
- Understand what moves them
- Monitor them regularly (some more regularly than others)
- Work with your department(s) who may also be monitoring them

Revenues (cont.)

- **Property Tax**
 - Who are your top 10 - 20 property tax generators?
 - Since Proposition 13, less volatile of a revenue source
- **Sales Tax**
 - Who are your top 10 – 20 sales tax generators?
 - Does it matter if one or more shut down?
- **Franchise Fees**
 - Understand your franchise ordinance and the changing technology
 - Does your ordinance reflect current/changing markets?
- **Transient Occupancy Tax**
 - How much do you rely on tourism/conventions?
 - Do you meet with your tourism authority/folks?

Revenues (cont.)

In the end...

- All revenue estimates are going to be wrong; it is just a question of by how much and in which direction
- Assessing risk tolerances – Knowing the consequences when your estimates are off
- Be consistent with agency practice/budget standards
- Use "reasonable" assumptions

Revenues (in millions) (cont.)

GENERAL FUND REVENUES	Fiscal Year 2025 Adopted Budget	Fiscal Year 2026	Fiscal Year 2027	Fiscal Year 2028	Fiscal Year 2029	Fiscal Year 2030
Property Tax	\$ 808.9	\$ 844.4	\$ 880.6	\$ 918.5	\$ 957.5	\$ 998.2
Sales Tax	393.5	392.8	403.0	416.6	430.7	445.3
Transient Occupancy Tax	172.8	176.4	185.1	194.4	204.0	214.2
Franchise Fees	123.7	120.8	117.0	120.4	126.8	134.7
Property Transfer Tax	10.1	10.9	11.3	11.8	12.3	12.8
Licenses and Permits	28.0	23.3	29.3	24.1	30.2	24.9
Cannabis Business Tax	19.4	18.2	19.0	19.7	20.4	21.1
Fines, Forfeitures and Penalties	31.2	31.6	32.1	32.6	33.1	33.5
Revenue from Money and Property	81.8	78.3	79.8	81.3	82.9	84.6
Revenue from Federal and Other Agencies	12.2	10.8	10.8	10.8	10.8	10.8
Charges for Services	281.7	267.5	276.0	284.1	288.9	295.8
Other Revenue	1.6	1.6	1.6	1.6	1.6	1.6
Transfers In	111.6	98.0	100.3	102.4	104.5	106.7
BASELINE GENERAL FUND REVENUES	\$ 2,076.5	\$ 2,074.7	\$ 2,146.1	\$ 2,218.4	\$ 2,303.8	\$ 2,384.4

Expenditures

- Again, know your key drivers (perhaps your top 2 or 3 that could make or break your budget)
 - Salary
 - Overtime
 - Pension Payments
- Know which departments could have the biggest impact
 - Public Safety
- Understand your labor agreements
- Are any new facilities coming online in the near future?
- Are there any significant projects under construction?

Expenditures (cont.)

- Salaries
 - Memorandum of Understanding
 - Is someone from Finance at the table?
 - Do you use your financial plan to evaluate proposals?
 - Are you paying attention to the impact on salary related costs?
- Overtime
 - Harder to control
 - Public Safety is the primary violator of the overtime budget
- Benefits
 - What is happening to your pension liability?
 - What is happening to your OPEB liability?
 - Do you even understand how these liabilities are calculated?

Expenditures (in millions) (cont.)

GENERAL FUND EXPENDITURES	Fiscal Year 2025 Adopted Budget	Fiscal Year 2026	Fiscal Year 2027	Fiscal Year 2028	Fiscal Year 2029	Fiscal Year 2030
Salaries & Wages (Current Negotiated MOUs; Annualized Positions; Step Increases; DROP Payments)	\$ 925.7	\$ 986.9	\$ 988.9	\$ 989.1	\$ 989.4	\$ 989.6
Salaries & Wages (Assumed General Wage Increases at 2.73% annually)		0.1	24.9	50.5	76.7	103.6
Retirement Actuarially Determined Contribution (ADC) ¹	357.2	364.3	369.7	381.4	328.6	332.7
Estimated Increase in ADC due to Investment Losses ²		0.0	0.0	0.0	0.0	0.0
Estimated Amortization of Proposition B Unfunded Liability		0.0	0.0	0.0	0.0	0.0
Employee Flexible Benefits	104.6	106.9	107.4	107.4	107.4	107.4
Other Post Employment Benefits (OPEB)	32.2	31.6	30.9	30.3	29.7	29.1
Workers' Compensation	33.0	39.2	42.7	46.5	50.6	55.0
Supplemental Pension Savings Plan (SPSP)	10.9	10.9	10.9	10.9	10.9	10.9
Other Fringe Benefits	39.7	40.8	41.6	41.9	42.3	42.8
Personnel Expenditures	\$ 1,503.2	\$ 1,580.6	\$ 1,617.1	\$ 1,658.1	\$ 1,635.6	\$ 1,671.2

Expenditures (cont.)

- Non-Personnel
 - Contractual Services
 - Debt Service
 - New facilities
 - Emergencies

Expenditures (in millions) (cont.)

GENERAL FUND EXPENDITURES	Fiscal Year 2025 Adopted Budget	Fiscal Year 2026	Fiscal Year 2027	Fiscal Year 2028	Fiscal Year 2029	Fiscal Year 2030
Supplies	\$ 31.5	\$ 39.5	\$ 40.3	\$ 41.1	\$ 42.0	\$ 42.8
Contracts & Services	387.6	394.0	409.0	420.7	438.1	449.3
Information Technology	59.2	60.2	61.0	61.7	65.4	71.9
Energy and Utilities	70.9	74.5	78.5	83.1	88.9	96.0
Reserve Contributions	0.0	63.2	24.3	24.7	24.8	30.5
Charter Section 77.1 - Infrastructure Fund Contribution	21.1	8.8	11.1	16.7	22.6	28.8
Other Expenditures	87.5	112.2	122.4	129.2	158.4	163.2
Non-Personnel Expenditures	\$ 657.7	\$ 752.3	\$ 746.6	\$ 777.2	\$ 840.3	\$ 882.6
BASELINE GENERAL FUND EXPENDITURES	\$ 2,160.9	\$ 2,332.9	\$ 2,363.7	\$ 2,435.3	\$ 2,475.9	\$ 2,553.8

Expenditures (in millions) (cont.)

Table 1.1 - Fiscal Year 2026-2030 Financial Outlook
Summary of Key Financial Data (\$ in Millions)

	Fiscal Year 2026	Fiscal Year 2027	Fiscal Year 2028	Fiscal Year 2029	Fiscal Year 2030
Property Tax	\$844.4	\$880.6	\$918.5	\$957.5	\$998.2
Sales Tax	\$392.8	\$403.0	\$416.6	\$430.7	\$445.3
Transient Occupancy Tax	\$176.4	\$185.1	\$194.4	\$204.0	\$214.2
Franchise Fees	\$120.8	\$117.0	\$120.4	\$126.8	\$134.7
All Other Revenue Categories	\$540.4	\$560.3	\$568.5	\$584.7	\$592.0
BASELINE GENERAL FUND REVENUES	\$2,074.7	\$2,146.1	\$2,218.4	\$2,303.8	\$2,384.4
Salaries & Wages (Current MOUs)	\$986.9	\$988.9	\$989.1	\$989.4	\$989.6
Salaries & Wages (Assumed General Wage Increases at 2.73% Annually)	\$0.1	\$24.9	\$50.5	\$76.7	\$103.6
Retirement Actuarially Determined Contributions (ADC)	\$364.3	\$369.7	\$381.4	\$328.6	\$332.7
All other Personnel Expenditures	\$229.4	\$233.6	\$237.1	\$241.0	\$245.3
Non-Personnel Expenditures	\$680.4	\$711.2	\$735.8	\$792.9	\$823.3
Charter Section 77.1 - Infrastructure Fund Contribution	\$8.8	\$11.1	\$16.7	\$22.6	\$28.8
BASELINE GENERAL FUND EXPENDITURES (LESS RESERVE CONTRIBUTIONS)	\$2,269.8	\$2,339.4	\$2,410.5	\$2,451.1	\$2,523.2
BASELINE (SHORTFALL)/ SURPLUS (LESS RESERVE CONTRIBUTIONS)	(\$195.0)	(\$193.4)	(\$192.2)	(\$147.3)	(\$138.8)
Reserve Contributions	\$63.2	\$24.3	\$24.7	\$24.8	\$30.5
BASELINE (SHORTFALL)/ SURPLUS	(\$258.2)	(\$217.6)	(\$216.9)	(\$172.1)	(\$169.4)

Expenditures (in millions) (cont.)

GENERAL FUND EXPENDITURES	Fiscal Year 2025 Adopted Budget	Fiscal Year 2026	Fiscal Year 2027	Fiscal Year 2028	Fiscal Year 2029	Fiscal Year 2030
---------------------------	---------------------------------	------------------	------------------	------------------	------------------	------------------

NEW FACILITIES	\$ 9.3	\$ 13.9	\$ 14.6	\$ 20.9	\$ 21.4
PLANNED COMMITMENTS	\$ 61.8	\$ 71.0	\$ 75.9	\$ 80.9	\$ 85.5

(AMOUNT TO BE MITIGATED) / AVAILABLE RESOURCES ³	\$ (329.3)	\$ (302.6)	\$ (307.4)	\$ (273.9)	\$ (276.3)
---	------------	------------	------------	------------	------------

Assess the Risk Tolerance

- What if you are off by 5%, 10%, 20%, etc.?
- Make sure you understand what is causing the variance
- How easily can you make a mid-term budget adjustments?

So Now You Have An Idea Of Where You Are And Where You're Going

- What do you do now?
 - Annually present this plan/forecast to your governing board
 - Post it on your website (investor page)
 - Update at least annually
 - Monitor monthly/quarterly
- Recognize your obligation to publicly disclose (specifically to investors) any “material” variances
 - EMMA



When and How Should You Disclose What You Know?

Outline

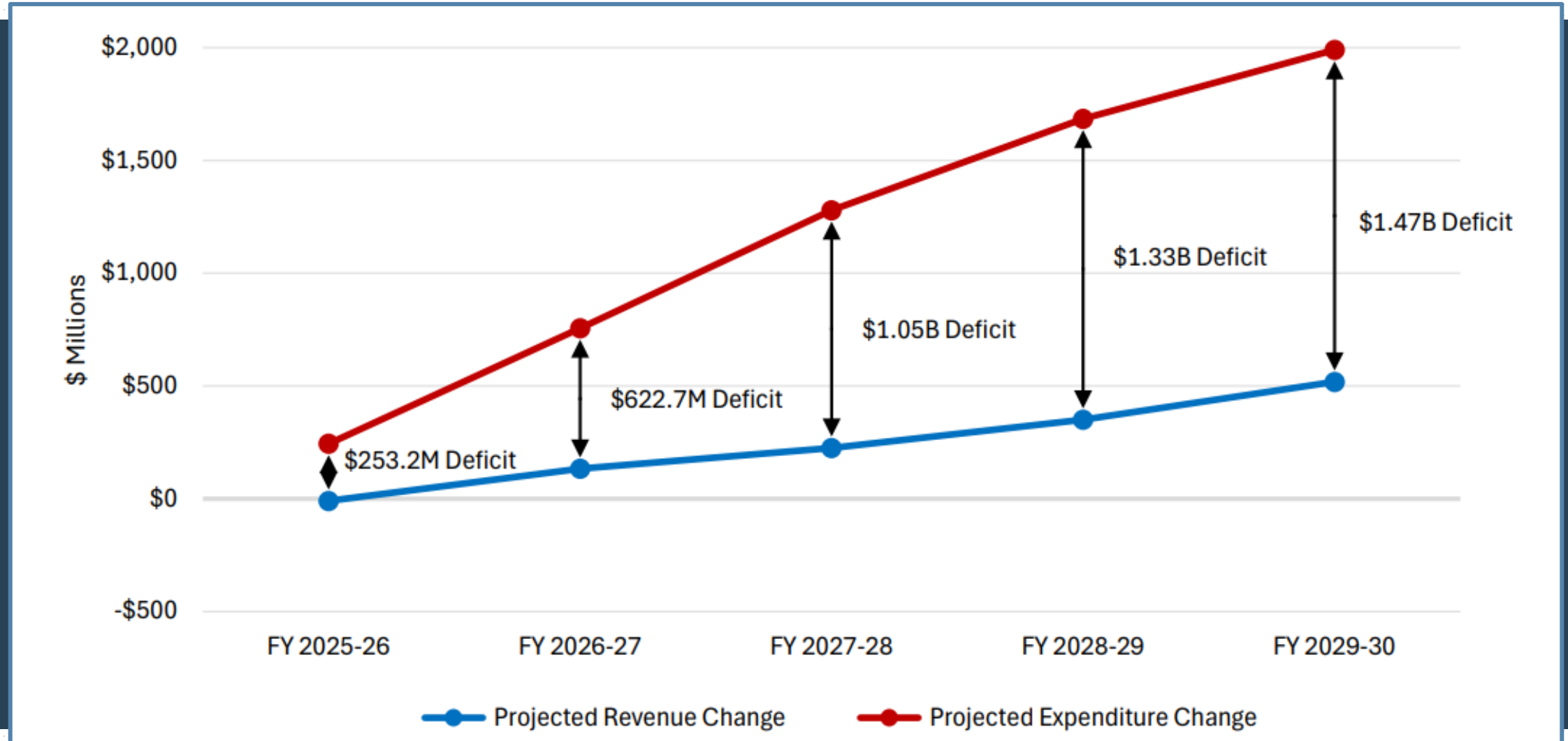
- Background on San Francisco
 - Financial Planning
 - Fiscal Reports
 - Frequency of reporting
- New Issuance Disclosure
- Ongoing Investor Communications

San Francisco – Financial Planning

- The 5-Year Financial Plan
 - Required under Prop A charter amendment (November 2009)
 - Impact of current service levels and polices on revenues and expenditures
- Longer Term Planning
 - Pension (10-year projections) and OPEB
 - Capital and Deferred Maintenance

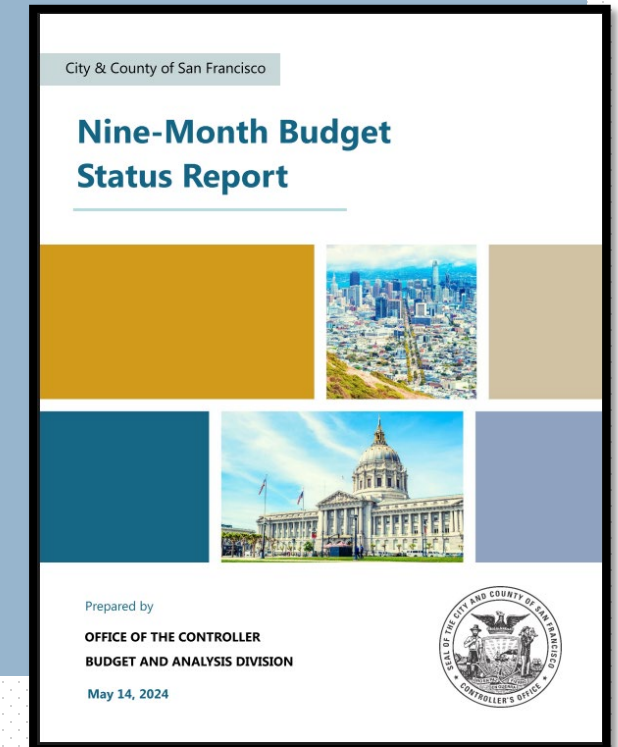
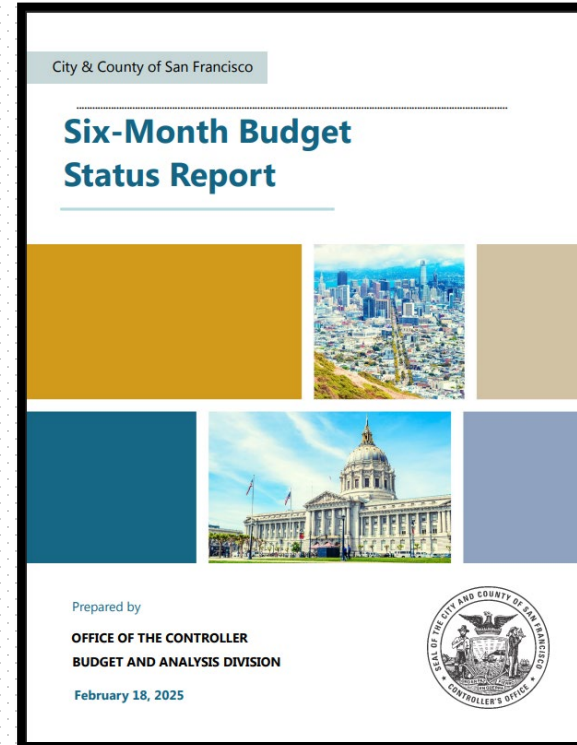
San Francisco – Financial Planning (cont.)

Projected Growth in General Fund Expenditures & Revenues



San Francisco – Fiscal Reports


- Regular reporting cycle
 - Five-Year Financial Plan with periodic updates
 - Annual Comprehensive Financial Report
 - Budget Status Updates
 - Six-Month Report
 - Nine-Month Report
 - Budget and Revenue Letter



Pandemic Example #1

- During extraordinarily high levels of uncertainty, more frequent updates may be needed/helpful
 - 3-month report published in November of 2020

Changes from Adopted Budget (\$ in M)	FY 2020-21
FY 2019-20 estimated fund balance	21.3
Citywide Revenue	-143.5
Baseline Offsets	46.4
Departmental Revenues and Expenses	-51.3
November 2020 Local Ballot Measures	11.3
Surplus/ (Shortfall)	-115.9



OFFICE OF THE CONTROLLER
CITY AND COUNTY OF SAN FRANCISCO

Ben Rosenfield
Controller
Todd Rydstrom
Deputy Controller

TO: Mayor London Breed
President Norman Yee and Members of the Board of Supervisors

FROM: Ben Rosenfield, Controller

DATE: November 10, 2020

SUBJECT: **FY 2020-21 3-Month Budget Status Report**

EXECUTIVE SUMMARY

The Controller's Office provides periodic budget status updates to the City's policy makers during each fiscal year, as directed by Charter Section 3.105. The level of uncertainty of both City revenues and expenditures is historically high due to the operational and economic effects brought on by the COVID-19 pandemic.

In summary, our projection of General Fund revenues and expenditures indicates a General Fund shortfall of \$115.9 million in the current fiscal year. This is predominantly comprised of weakness in key tax and fee revenues driven by a slower economic recovery than was anticipated in the adopted budget. This weakness is partially offset by a higher than projected balance available from the prior year. Required reserve deposits in the prior year are expected to be higher than previously expected, as detailed in the appendix to this report, and could be used to offset a portion of the current year projected shortfall or retained for challenges in future fiscal years.

The level of uncertainty regarding city revenues and expenditures remains extraordinarily high, driven by the economic and financial impacts of the public health emergency. We will continue to provide regular budget updates throughout the year as conditions change.

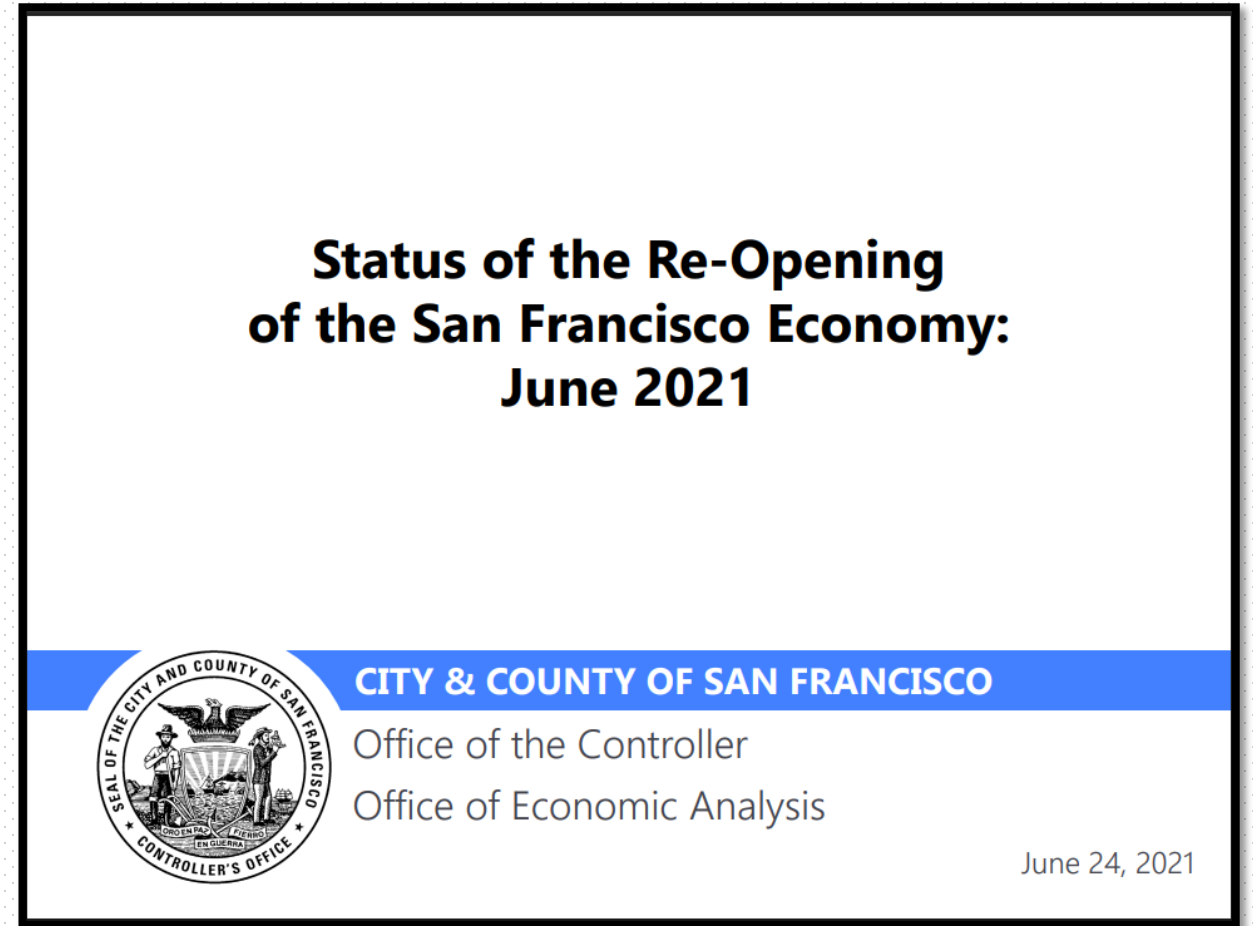
Table 1. FY 2020-21 Projected General Fund Variances to Budget (\$ million)

Changes from Adopted Budget	FY 2020-21
A. FY 2019-20 estimated fund balance (pre-audit)	21.3
B. Citywide Revenue	(143.5)
C. Baseline Offsets	46.4
D. Departmental Revenues and Expenditures	(51.3)
E. November 2020 Local Ballot Measures	11.3
F. COVID Emergency Response	-
Surplus / (Shortfall)	(115.9)

CITY HALL • 1 DR. CARLTON B. GOODLETT PLACE • ROOM 316 • SAN FRANCISCO, CA 94102-4694
PHONE 415-554-7500 • FAX 415-554-7466

Pandemic Example #2

- Monthly reports published from June 2021 through July 2023
- Bi-monthly reports published currently



Types of Investor Disclosure

- New Issuance Disclosure
- Official Statement / Appendix A
- Ongoing Investor Disclosures
- Annual Continuing Disclosure Report
- Investor Relations Website

New Issuance Disclosure

- Appendix A
 - City Financial Challenges upfront
 - Budgetary Risks section
 - Threat of Recession
 - Impact of Commuting Pattern Changes on Business Taxes
 - Office Vacancy in San Francisco; Impact on Property Taxes and Other Revenues
 - Business Tax Litigation
 - Impact of the State of California Budget on Local Finances
 - Impact of Federal Government on Local Finances
 - Etc.,.....

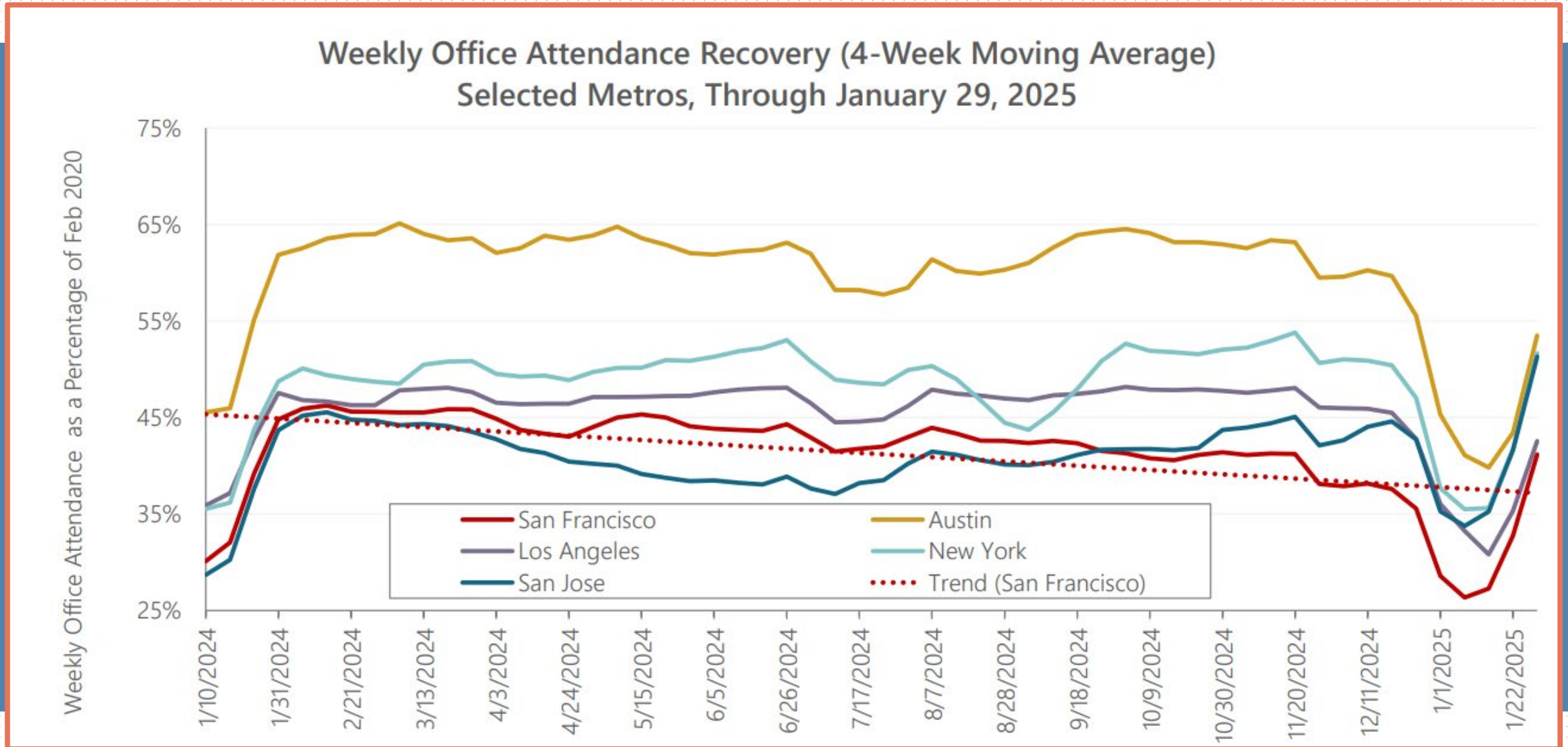
Appendix A

New introductory paragraph, followed by highlights from recent reports

City Financial Challenges

The City continues to face material financial challenges, including actual and projected revenue losses, resulting from a variety of factors, including continuing remote work by a significant portion of the workforce (which has led to vacancies and declining property taxes for certain office buildings, lower real estate property transfer taxes, and reductions in taxes based on employees physically located in the City), continued weakness in the local hospitality and convention industries (resulting in declines in hotel and sales taxes from pre-pandemic levels), reduced funding to the City in State budgets, potential losses from litigation challenging the City's business taxes, uncertainty about receipt of outstanding FEMA reimbursements and general economic conditions. The City has experienced the largest increase in office vacancy among major urban office markets in the United States, from 5.6% in the fourth quarter of 2019 to 34.5% in the third quarter of 2024. As further described in APPENDIX A hereto, the conditions discussed above have contributed to projected budget deficits (absent corrective actions) in the hundreds of millions of dollars in future fiscal years, rising to approximately \$1.47 billion in fiscal year 2029-30.

Appendix A – Post Pandemic Impacts



Ongoing Investor Disclosures

- Annual Continuing Disclosure Report

II. Recent Events

Public Health Emergency – COVID-19

On February 11, 2020 the World Health Organization (“WHO”) announced the official name for the outbreak of a new disease (“COVID-19”) caused by a strain of novel coronavirus, an upper respiratory tract illness which has since spread across the globe. The spread of COVID-19 is having significant adverse health and financial impacts throughout the world, including the City and County of San Francisco (“City”). The WHO has declared the COVID-19 outbreak to be a pandemic, and states of emergency have been declared by the Mayor of the City, the Governor of the State and the President of the United States.

As of March 1, 2021, there were over 34,000 confirmed cases of COVID-19 in the City, and health officials expect the number of confirmed cases to continue grow. The outbreak has resulted in the imposition of restrictions on mass gatherings and widespread closings of businesses, universities and schools (including the San Francisco Unified School District) throughout the United States. On June 8, 2020 the National Bureau of Economic Research announced that the U.S. officially entered into a recession in February 2020. In addition, capital markets in the United States and globally have been volatile.

Investor Relations Website

Controller's Office of Public Finance



Disclaimer & Conditions of Use

By accessing any of the information on this website, the reader acknowledges that they have read the disclaimer.

[Read our disclaimer here](#)

Investor Relations Website (cont.)

Market Disclosure and Reports

[Primary Market Disclosure \(Official Statements\)](#) → [Annual Secondary Market Disclosure](#) →

[Outstanding Debt & Long Term Obligations](#) → [City Credit Ratings](#) →

[Annual Comprehensive Financial Reports \(ACFR\)](#) → [Special Tax District Reports](#) →

[Citywide Fiscal Reports](#) → [Search all Controller's Office reports](#) →

Find audits, budgets, whistleblower complaints, performance reports, and Civil Grand Jury status reports.

Investor Relations Website (cont.)

Annual Budget and Appropriation Ordinance



Five-Year Financial Plan Update



View the [Five-Year Financial Plan: FY 2025-26 through FY 2029-30](#)

View the [March 29, 2024, Update to the Five-Year Financial Plan](#)

View the [Five-Year Financial Plan Update: FY2024-25 through FY 2027-28](#)

Six-Month Budget Status Report



Revenue Letter



Nine-Month Budget Status Report



DISCUSSION

QUESTIONS?



MARGARET BACKSTROM
Managing Director
Morgan Stanley



JAY GOLDSTONE
Financial Services Consultant
Self-employed



ANNA VAN DEGNA
Public Finance Director
City & County of San
Francisco



LUNCH

SESSION THREE

Technology Topics: Disclosable Risks and Opportunities



PAULINA HARO

*Senior Project Advisor
Governmental
Accounting Standards
Board*



DONALD HESTER

*Cybersecurity Advisor
Cybersecurity and
Infrastructure
Security Agency*



DIANE QUAN

*Partner
Hawkins Delafield
& Wood LLP*



KRYSTAL TENA

*Associate Director
S&P Global Ratings*

Introduction

- Current disclosure guidance
- Issuer perspective; strategic planning
- Investor perspective and expectations
- Discussion - application of guidance and advice
- Federal Data Transparency Act

Basis of SEC Regulation

- Municipal securities are exempt from registration with the SEC
- Continued applicability of the Anti-Fraud Rules
 - Obligation to avoid material misstatements and omissions in disclosures
 - Includes official statements, annual reports, annual comprehensive financial reports and voluntary statements
- SEC rules for public companies as guidance

Applicable Guidance

- SEC Final Rule: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure – Adopted on July 26, 2023; effective September 5, 2023
- SEC Statement: The Importance of Disclosure for our Municipal Markets – Issued May 4, 2020

Final Rule on Cybersecurity Disclosure

GENERAL

- Requires public companies to:
 - Report material cybersecurity incidents
 - Provide disclosure on cybersecurity risk management and governance
- Guidance for municipal entities

Final Rule on Cybersecurity Disclosure

MATERIAL CYBERSECURITY INCIDENT

- Disclose any cybersecurity incident issuer determines to be material, including
 - material aspects of the nature, scope, and timing of the incident
 - material impact or reasonably likely material impact of the incident on the issuer, including its financial condition and results of operations

Final Rule on Cybersecurity Disclosure

MATERIAL CYBERSECURITY INCIDENT (cont.)

- “Cybersecurity incident” means an unauthorized occurrence, or a series of related unauthorized occurrences, on or conducted through a registrant’s information systems that jeopardizes the confidentiality, integrity, or availability of a registrant’s information systems or any information residing therein.
 - To be broadly construed
 - Includes a series of events that are material, even if the individual incident is not

Final Rule on Cybersecurity Disclosure

MATERIAL CYBERSECURITY INCIDENT (cont.)

- “Information systems” means electronic information resources, owned or used by the registrant, including physical or virtual infrastructure controlled by such information resources, or components thereof, organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of the registrant’s information to maintain or support the registrant’s operations.

Final Rule on Cybersecurity Disclosure

MATERIAL CYBERSECURITY INCIDENT (cont.)

- Includes incidents on systems of a third-party service provider (e.g., cloud service providers)
- Suggests policies and procedures that take into account third-party oversight and reporting
- For such disclosure
 - based on the information available to registrant
 - no requirement for additional inquiries outside of the regular channels of communication with third-party service providers pursuant to those contracts and existing disclosure controls and procedures

Final Rule on Cybersecurity Disclosure

MATERIAL CYBERSECURITY INCIDENT (cont.)

- Materiality determination remains unchanged
 - Case law has established that information is material if there is a “substantial likelihood that, under all the circumstances, the omitted factor would have assumed actual significance in the deliberations of a reasonable [investor]”
 - “Reasonable” investor is an objective standard

Final Rule on Cybersecurity Disclosure

MATERIAL CYBERSECURITY INCIDENT (cont.)

- Materiality depends upon a balancing of both the indicated probability that the event will occur and the anticipated magnitude of the event
- A misstatement or omission may be material if it affects rating, yield, risk of early redemption, etc., even if it does not present a risk of default
- Confidentiality, business concerns, and political sensitivity are not exceptions to application of disclosure rules

Final Rule on Cybersecurity Disclosure

MATERIAL CYBERSECURITY INCIDENT (cont.)

- Departs from original proposal in that public companies are not required to disclose incident remediation status, whether it is ongoing, or whether data was compromised
 - While some incidents may still necessitate disclosure – for example, discussion of data theft, asset loss, intellectual property loss, reputational damage, or business value loss – registrants will make those determinations as part of their materiality analyses

Final Rule on Cybersecurity Disclosure

MATERIAL CYBERSECURITY INCIDENT (cont.)

- Registrant need not disclose specific or technical information about its planned response to the incident or its cybersecurity systems, related- networks and devices, or potential system vulnerabilities in such detail as would impede the registrant's response or remediation of the incident

Final Rule on Cybersecurity Disclosure

MATERIAL CYBERSECURITY INCIDENT (cont.)

- Determine the materiality of an incident without unreasonable delay following discovery
- Public companies are required to file a statement with the SEC within four business days of such determination
 - Note period begins with materiality determination, not breach
 - Municipal issuers not subject to similar timing constraints
 - Abide by internal processes and procedures

Final Rule on Cybersecurity Disclosure

MATERIAL CYBERSECURITY INCIDENT (cont.)

- Disclosure may be delayed if the United States Attorney General determines that immediate disclosure would pose a substantial risk to national security or public safety
 - Similar to no confidentiality exception to Anti-Fraud Rules
 - Municipal issuers do not have an obligation to speak absent a contractual undertaking or if there is an offering

Final Rule on Cybersecurity Disclosure

MATERIAL CYBERSECURITY INCIDENT (cont.)

- The final rules do not separately create or otherwise affect a registrant's duty to update its prior statements
 - Except with respect to previously undetermined or unavailable information
 - Duty to correct prior disclosure that the registrant determines was untrue (or omitted a material fact necessary to make the disclosure not misleading) at the time it was made
 - Duty to update disclosure that becomes materially inaccurate after it was made (for example, when the original statement is still being relied on by reasonable investors)

Final Rule on Cybersecurity Disclosure

RISK MANAGEMENT AND STRATEGY

- Describe processes, if any, for assessing, identifying, and managing material risks from cybersecurity threats in sufficient detail for a reasonable investor to understand those processes
- Describe whether any risks from cybersecurity threats, including as a result of any previous cybersecurity incidents, have materially affected or are reasonably likely to materially affect the registrant, including its business strategy, results of operations, or financial condition and, if so, how

Final Rule on Cybersecurity Disclosure

GOVERNANCE

- Describe the governing board's oversight of risks from cybersecurity threats
- Describe management's role in assessing and managing the registrant's material risks from cybersecurity threats (e.g., use of committees and process for information board)

SEC 2020 Statement on Importance of Disclosure







- Related to COVID-19 pandemic; applies to voluntary statements generally
- SEC recommends that the disclosure on financial and operating conditions be accompanied by
 - meaningful cautionary language, description of facts or assumptions affecting the reasonableness of reliance on and the materiality of the information provided
 - cautionary language on how certain information may be incomplete or unaudited
 - forward-looking statements
- Consistency with internal reports

THREAT LANDSCAPE & CISA RESOURCES



Donald E. Hester
CISA Cybersecurity Advisor – Northern California
Region 9 (AZ, CA, HI, NV, AS, CNMI and GU)
Cell: +1 (202) 315-8091 | Teams +1 (202) 984-3677
Email: donald.hester@cisa.dhs.gov

Cyber Threat Continuum

	HACKTIVISM	CRIME	INSIDER	ESPIONAGE	TERRORISM	WARFARE
THREATS						
ACTIONS	Hackers might use computer network exploitation to advance their political or social causes.	Individuals and sophisticated criminal enterprises steal personal information and extort victims for financial gain.	Insider threat actors typically steal proprietary information for personal, financial, or ideological reasons.	Nation-state actors might conduct computer intrusions to steal sensitive state secrets and proprietary information from private companies.	Terrorist groups might seek to sabotage the computer systems that operate our critical infrastructure.	Nation-state actors might attempt to sabotage military and critical infrastructure systems to gain an advantage in the event of conflict.



ODNI Annual Threat Assessment

Cyber Crime

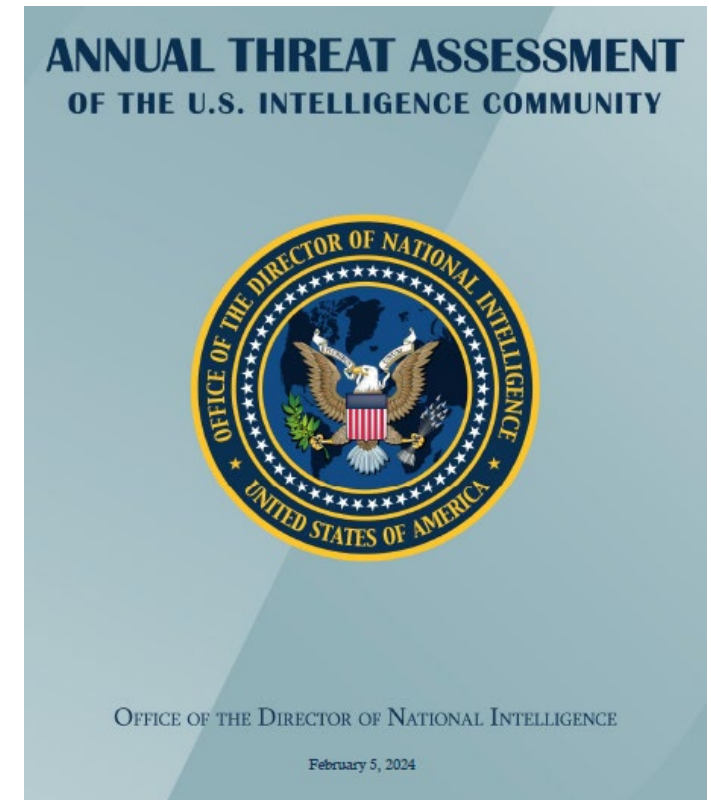
“Transnational organized criminals involved in ransomware operations are improving their attacks, extorting funds, disrupting critical services, and exposing sensitive data.”

Disruptive Technology

“New technologies—particularly in the fields of AI and biotechnology—are being developed and are proliferating at a rate that makes it challenging for companies and governments to shape norms regarding civil liberties, privacy, and ethics.”

Health Security

“National health system shortfalls, public mistrust and medical misinformation, and eroding global health governance will impede the capacity of countries to respond to health threats.”



2024 ODNI Annual Threat Assessment

Foreign Threat Actors



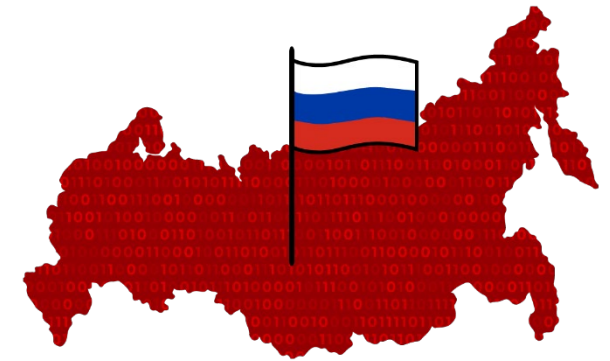
PEOPLE'S REPUBLIC OF CHINA

“China remains the most active and persistent cyber threat to U.S. Government, private-sector, and critical infrastructure networks.”



IRAN

“Iran’s growing expertise and willingness to conduct aggressive cyber operations make it a major threat to the security of U.S. and allied and partner networks and data.”

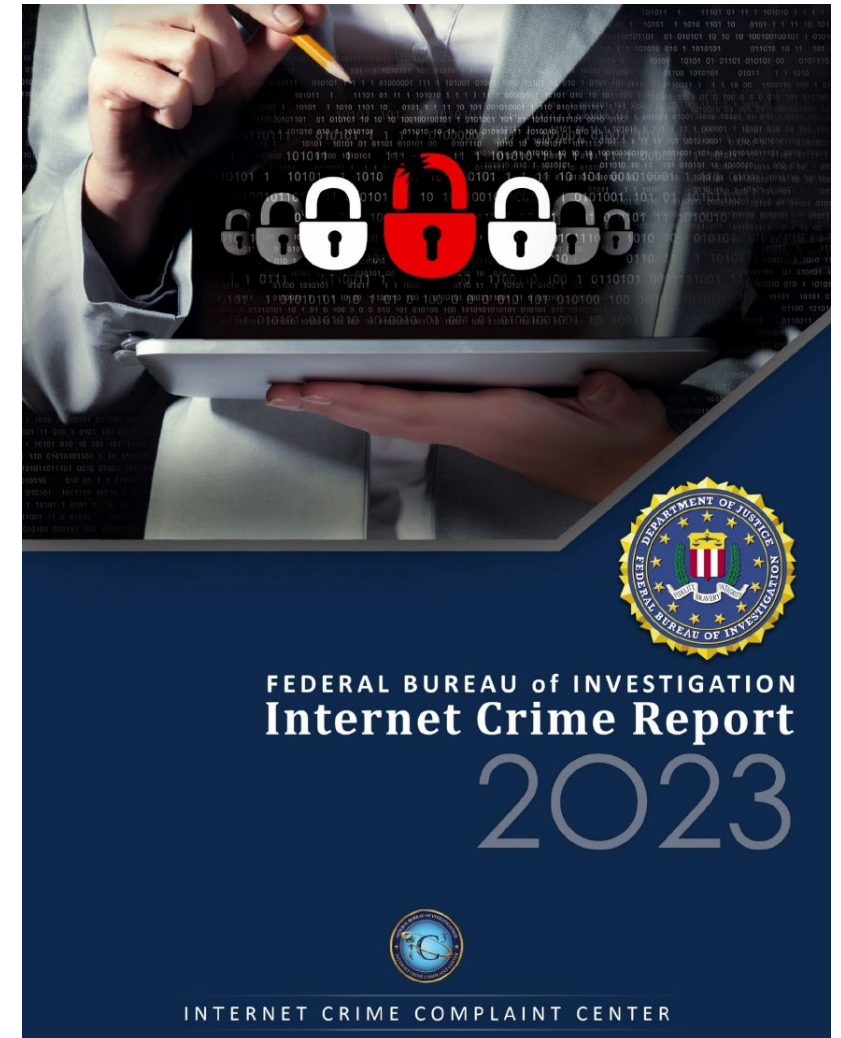
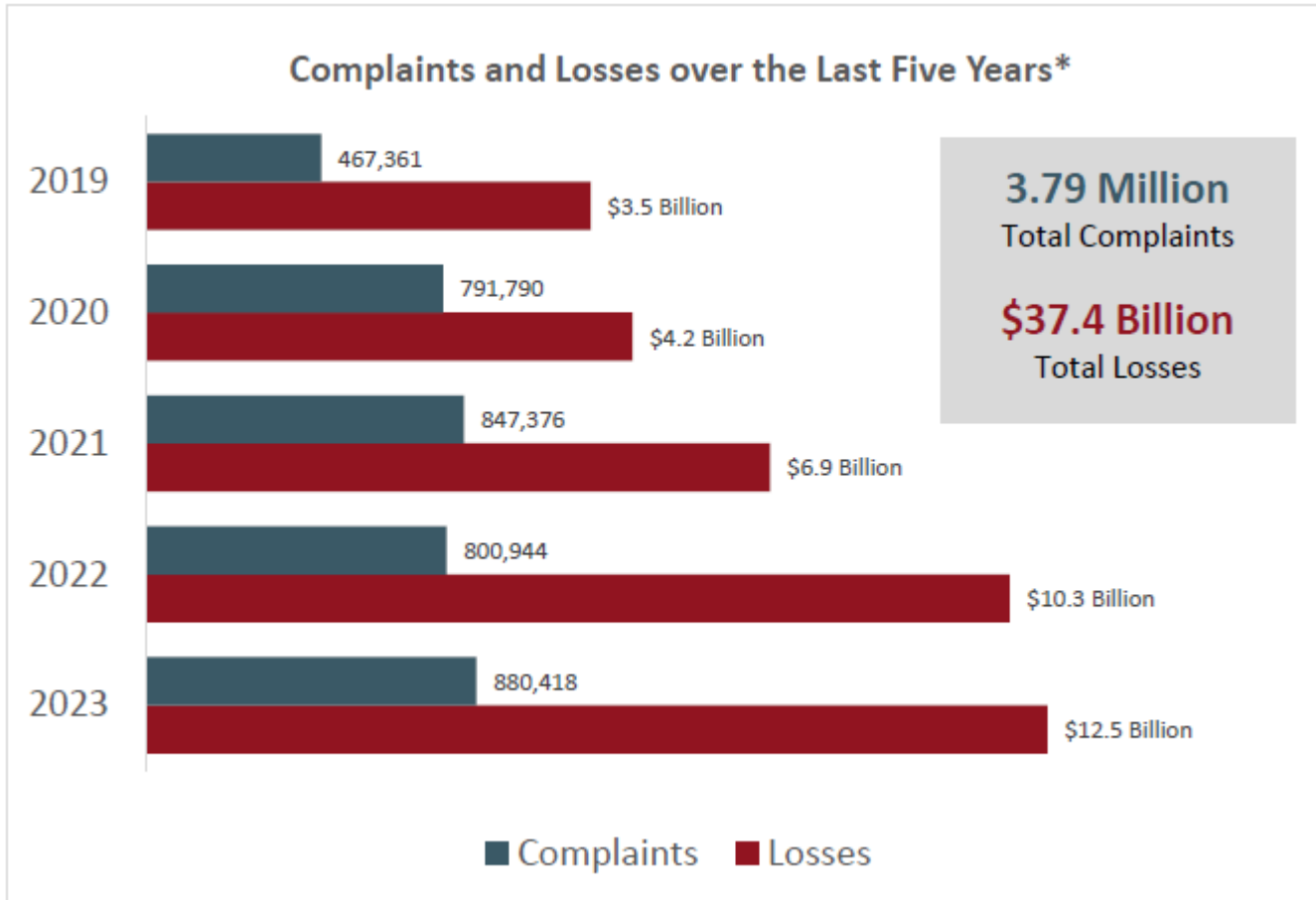


RUSSIA

“Russia will pose an enduring global cyber threat even as it prioritizes cyber operations for the Ukrainian war.”

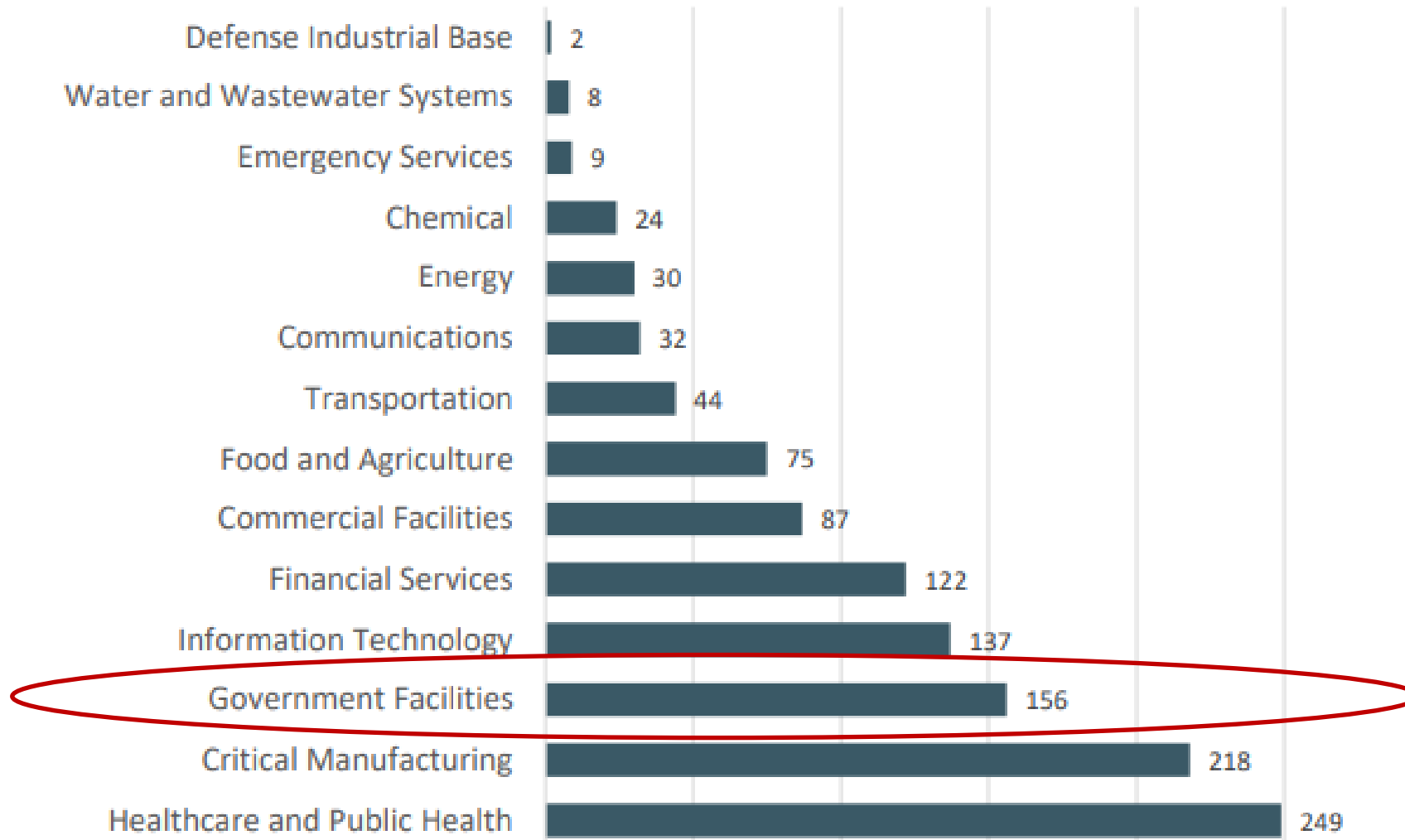


IC3 Internet Crime Report 2023



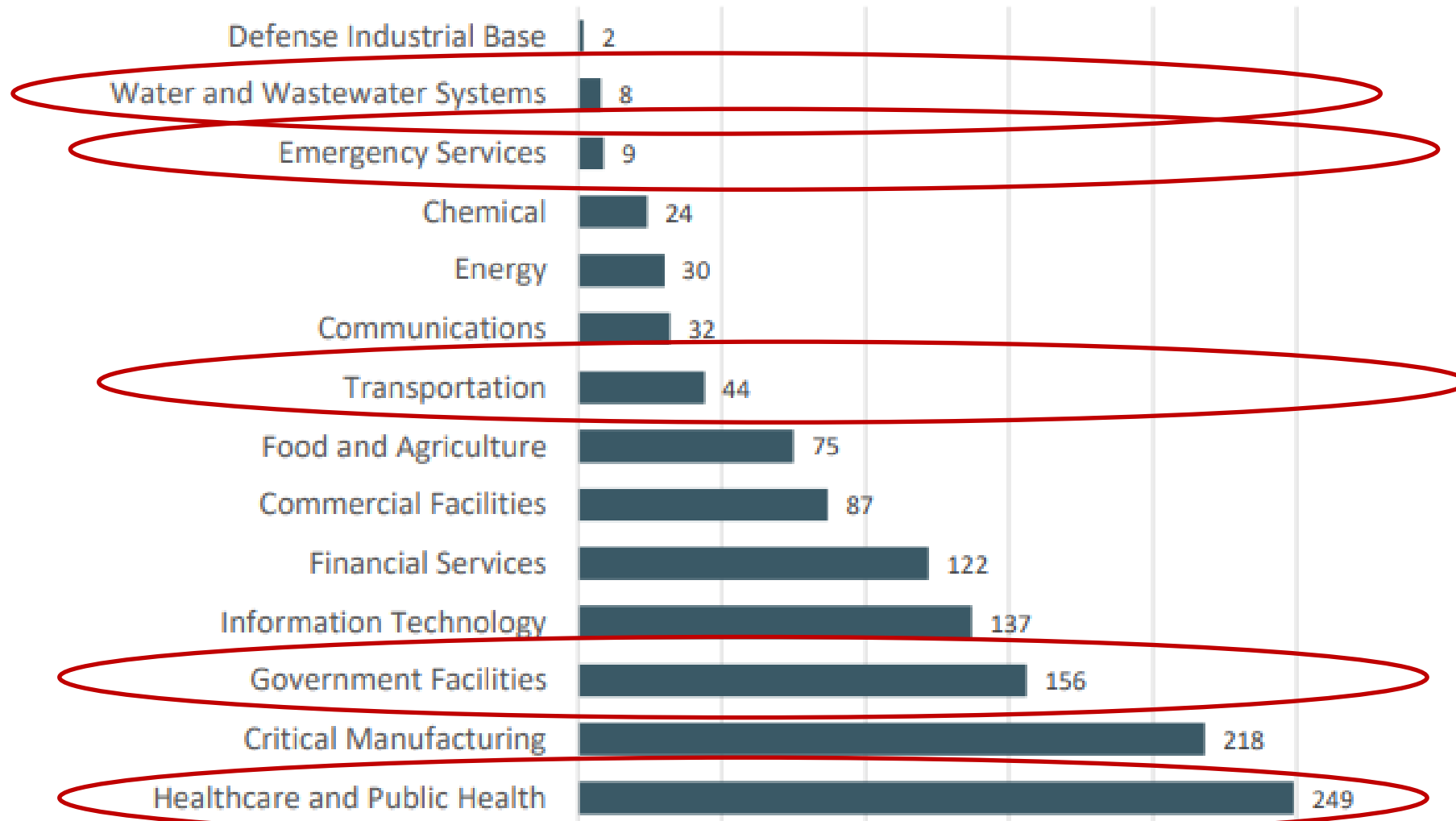
Sectors Affected by Ransomware

Infrastructure Sectors Affected by Ransomware

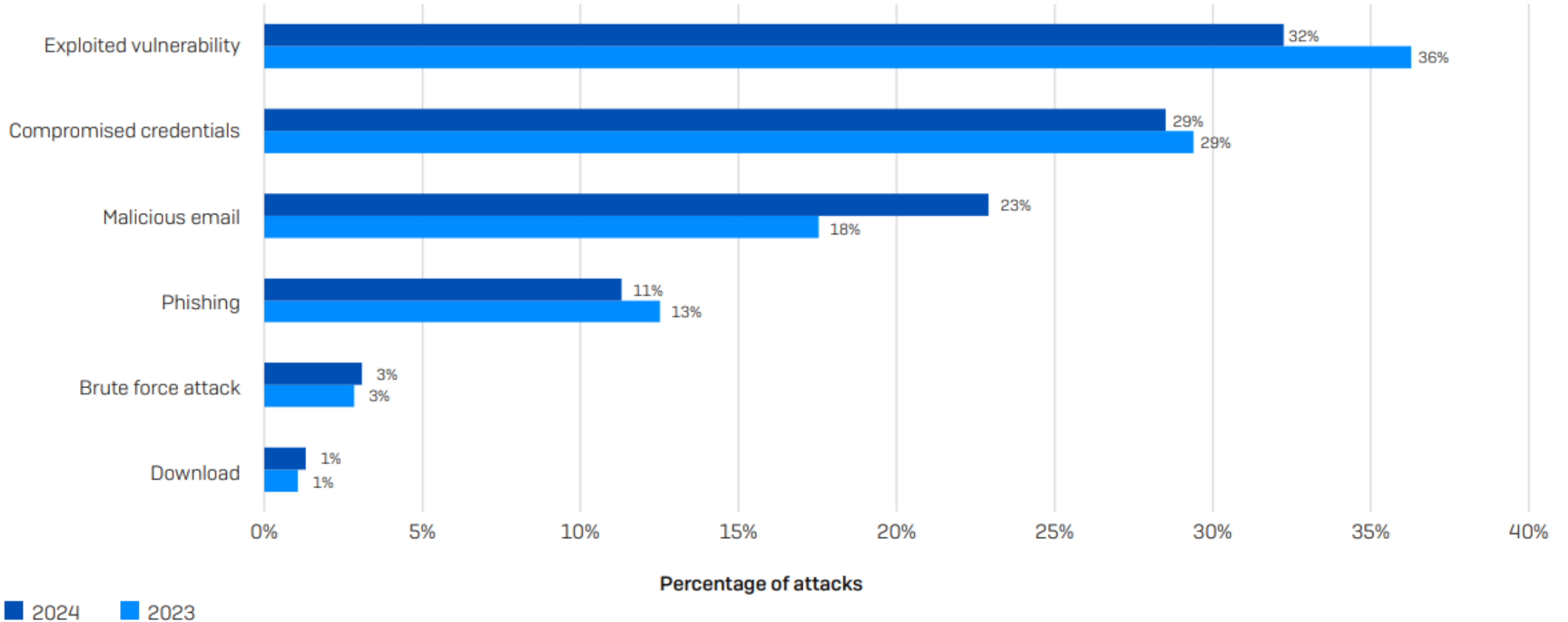


Sectors Affected by Ransomware

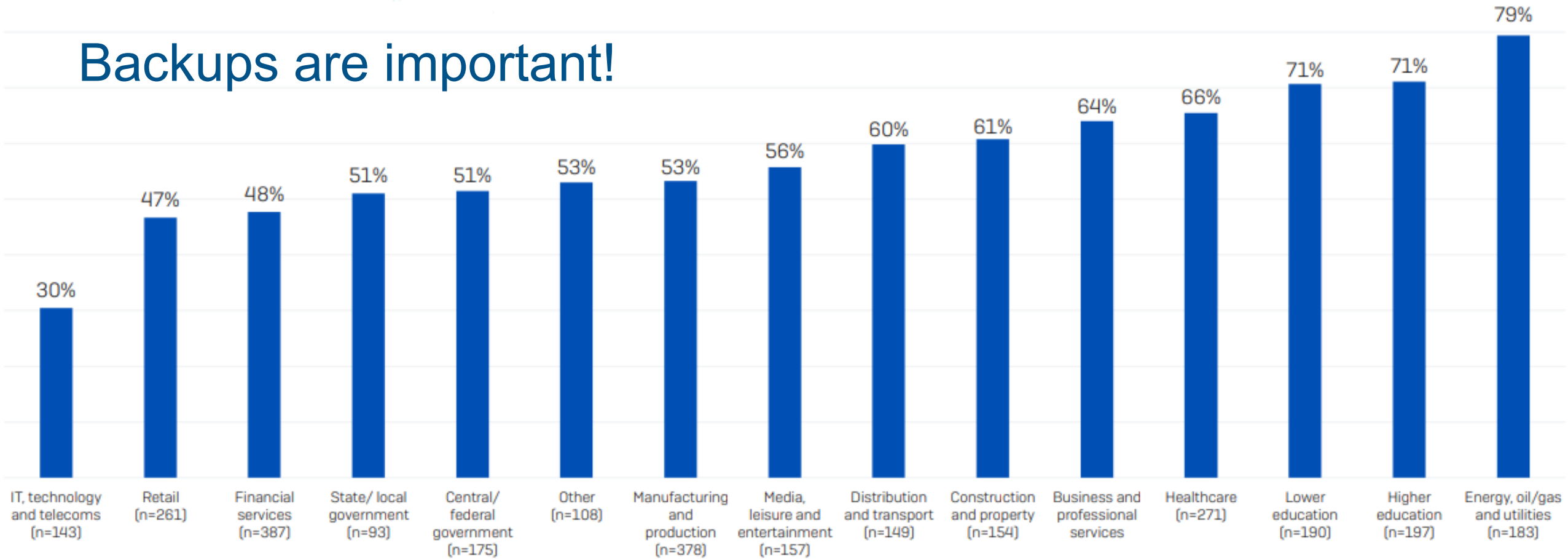
Infrastructure Sectors Affected by Ransomware



Causes of Ransomware Attack



Backups are important!



- Ransom demands were, on average, more than double that of those whose backups weren't impacted (\$2.3M vs. \$1M median initial ransom demand)
- Organizations whose backups were compromised were almost twice as likely to pay the ransom to recover encrypted data (67% vs. 36%)
- Median overall recovery costs came in eight times higher (\$3M vs. \$375K) for those that had backups compromised

Recovery Costs

2021	2022	2023	2024
\$1.85M	\$1.4M	\$1.82M	\$2.73M

What was the approximate cost to your organization to rectify the impacts of the most significant ransomware attack (considering downtime, people time, device cost, network cost, lost opportunity etc.)? n=2,974 (2024)/ 1,974 (2023)/ 3,702 (2022)/ 2,006 (2021). N.B. 2022 and 2021 question wording also included "ransom payment".



IOCTA 2024

- The number of cybercriminals entering the market continues to grow steadily, both due to new technologies, which effectively lower the entry barriers, and to an increasing complexity of the digital infrastructure, which widens the potential attack surface.
- High-level affiliates and developers remain an important asset, with different ransomware-as-a-service (RaaS) providers competing for their services.



Critical Infrastructure

- Domestic and foreign adversaries almost certainly will continue to threaten the integrity of our critical infrastructure with **disruptive and destructive cyber and physical attacks**, in part, because they perceive targeting these sectors will have cascading impacts on US industries and our standard of living.
- We expect adversarial state cyber actors will continue to **seek access** to, or to **pre-position** themselves on, US critical infrastructure networks.



OFFICE of INTELLIGENCE and ANALYSIS
Homeland Threat Assessment



Critical Infrastructure

- In addition to our adversaries targeting US critical infrastructure for **destructive and disruptive attacks**, adversaries also target the entities that make up critical infrastructure sectors for foreign intelligence collection.
- Adversarial **nation-states** continue to use cyber tactics to access and **steal sensitive information** from US networks, including those of entities that are part of critical infrastructure, for **broader espionage** purposes to advance their military, diplomatic, and economic goals.



OFFICE of INTELLIGENCE and ANALYSIS
Homeland Threat Assessment



Disruptive Technology: AI Threats

- Attacks on AI Systems
- AI Enabled Phishing
- AI Enabled Vulnerability Research
- AI Enabled Hacking
- Used to Create Disinformation
- Voice Cloning



Key Takeaways

- Top threat actors are Nation States and cyber criminals
- Outdated software and vulnerabilities are highest risk
- Stolen credentials are the next highest risk
- The average cost of a cyber incidents is up
- Keep a close eye on disruptive technologies
- Good backups will save you money
- Patch Management and MFA greatly reduce risk



CISA Can Help

- Risk Assessment Services
 - Cyber Performance Goals (Assessment)
 - Ransomware Readiness Assessment
 - Cyber Hygiene (Vulnerability Scanning)
 - Tabletop Exercises

- CISA Resources and Services
 - No Cost

IDENTIFY (1)				
1.A Asset Inventory	ID.AM-1, ID.AM-2, ID.AM-4, DE.CM-1, DE.CM-7	CURRENT ASSESSMENT	YEAR 1 ASSESSMENT	NOTES
COST: \$000 IMPACT: HIGH COMPLEXITY: MEDIUM TACTIC, TECHNIQUE, AND PROCEDURE (TTP) OR RISK ADDRESSED: Hardware Additions (T2200) Exploit Public-Facing Application (TO819, ICS TO819) Internet-accessible device (CS TO883) RECOMMENDED ACTION: Maintain a regularly updated inventory of all organizational assets with an IP address (including IPv6), including OT. This inventory is updated on a recurring basis, no less than monthly for both IT and OT. FREE SERVICES AND REFERENCES: Cyber Hygiene Services , Smart OT Search Guide, or email cyberact@cisa.dhs.gov		DATE: <input type="text"/> <input type="checkbox"/> IMPLEMENTED <input type="checkbox"/> IN PROGRESS <input type="checkbox"/> SCOPED <input type="checkbox"/> NOT STARTED	DATE: <input type="text"/> <input type="checkbox"/> IMPLEMENTED <input type="checkbox"/> IN PROGRESS <input type="checkbox"/> SCOPED <input type="checkbox"/> NOT STARTED	
1.B Organizational Cybersecurity Leadership	ID.OV-1, ID.OV-2	CURRENT ASSESSMENT	YEAR 1 ASSESSMENT	NOTES
COST: \$000 IMPACT: HIGH COMPLEXITY: LOW TTP OR RISK ADDRESSED: Lack of sufficient cybersecurity accountability, investment, or effectiveness. RECOMMENDED ACTION: A named role/position/title is identified as responsible and accountable for planning, resourcing, and execution of cybersecurity activities. This role may undertake activities, such as managing cybersecurity operations at the senior level, requesting and securing budget resources, or leading strategy development to inform future positioning.		DATE: <input type="text"/> <input type="checkbox"/> IMPLEMENTED <input type="checkbox"/> IN PROGRESS <input type="checkbox"/> SCOPED <input type="checkbox"/> NOT STARTED	DATE: <input type="text"/> <input type="checkbox"/> IMPLEMENTED <input type="checkbox"/> IN PROGRESS <input type="checkbox"/> SCOPED <input type="checkbox"/> NOT STARTED	
1.C OT Cybersecurity Leadership	ID.OV-1, ID.OV-2	CURRENT ASSESSMENT	YEAR 1 ASSESSMENT	NOTES
COST: \$000 IMPACT: HIGH COMPLEXITY: LOW TTP OR RISK ADDRESSED: Lack of accountability, investment, or effectiveness of OT cybersecurity program. RECOMMENDED ACTION: A named role/position/title is identified as responsible and accountable for planning, resourcing, and execution of OT-specific cybersecurity activities. In some organizations this may be the same position as identified in 1.B.		DATE: <input type="text"/> <input type="checkbox"/> IMPLEMENTED <input type="checkbox"/> IN PROGRESS <input type="checkbox"/> SCOPED <input type="checkbox"/> NOT STARTED	DATE: <input type="text"/> <input type="checkbox"/> IMPLEMENTED <input type="checkbox"/> IN PROGRESS <input type="checkbox"/> SCOPED <input type="checkbox"/> NOT STARTED	
1.D Improving IT and OT Cybersecurity Relationships	ID.OV-2, PRAT-6	CURRENT ASSESSMENT	YEAR 1 ASSESSMENT	NOTES
COST: \$000 IMPACT: MEDIUM COMPLEXITY: LOW TTP OR RISK ADDRESSED: Poor working relationships and a lack of mutual understanding between IT and OT cybersecurity can often result in increased risk for OT cybersecurity. RECOMMENDED ACTION: Organizations sponsor at least one "pizza party" or equivalent social gathering per year that is focused on strengthening working relationships between IT and OT security personnel, and is not a working event (such as providing meals during an incident response).		DATE: <input type="text"/> <input type="checkbox"/> IMPLEMENTED <input type="checkbox"/> IN PROGRESS <input type="checkbox"/> SCOPED <input type="checkbox"/> NOT STARTED	DATE: <input type="text"/> <input type="checkbox"/> IMPLEMENTED <input type="checkbox"/> IN PROGRESS <input type="checkbox"/> SCOPED <input type="checkbox"/> NOT STARTED	



When you get back to the office...

- Contact your local Cybersecurity Advisor (CSA)
- Sign up for Cyber Hygiene scanning service
- Contact CSA for guided self-assessment of the Cyber Performance Goals (CPG) & Ransomware Readiness Assessment (RRA)
- Schedule a Tabletop Exercise
- Find more at <https://www.cisa.gov/>



Cybersecurity Through a Ratings Lens



Krystal L. Tena
Associate Director, Local Governments - West Region
Americas Public Finance, S&P Global Ratings
Email: krystal.tena@spglobal.com
Office: 212-438-1628

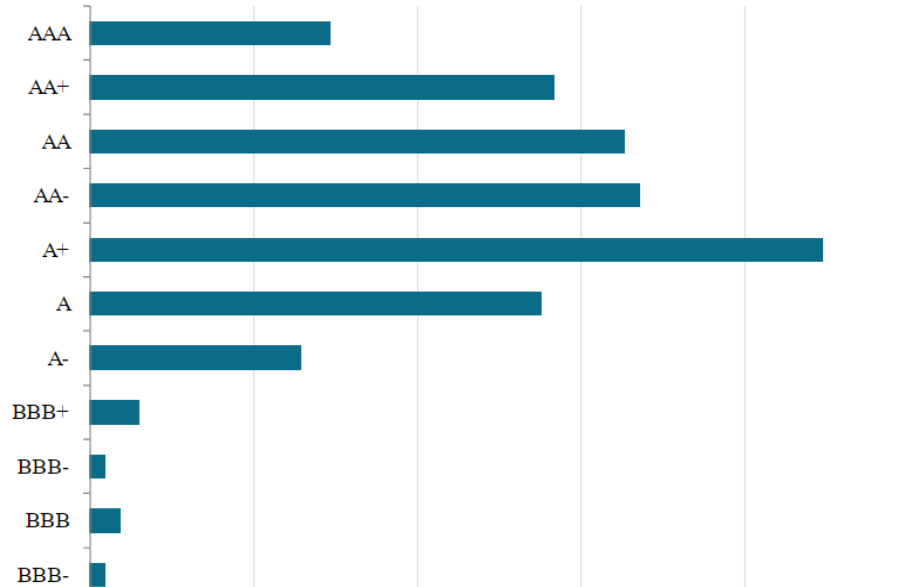
Agenda

- **US Public Finance overview**
- **Why cyber?**
- **Trends in cyber attacks**
- **How incorporated into rating methodology and what factors are important to investors?**
- **Questions you may be asked by an S&P Global Ratings' analyst**
- **Q&A**

US Local Government - Sector Summary

Ratings distribution

Local government ratings distribution
As of Dec. 31, 2024



What We're Watching for 2025

Local Governments | 2025 Outlook -- What We're Watching



Federal policy initiatives
Uncertainty of impact from pending Trump administration policies on immigration and trade could affect both revenues and expenditures.



Federal budget
A closely divided Congress will ensure difficult budget negotiations, including renegotiation of the TCJA.



Stimulus winddown
Deadlines for spending and designating could cause operating imbalances if the loss of one-time federal revenues isn't managed proactively.



Slower economic trends
Commercial real estate occupancy may have steadied, but given projections for slower GDP growth and elevated inflation, economic pressures remain.



Climate hazards
Higher-cost, higher-frequency major storms are likely to pressure government debt and push up insurance costs.



Governance gets trickier
Skilled labor shortages--including among auditors--and management turnover could raise governance risk at a point of fiscal and economic inflection.

TCJA--Tax Cut and Jobs Act, Source: S&P Global Ratings.
Copyright © 2024 by Standard & Poor's Financial Services LLC. All rights reserved.

S&P Global
Ratings

Cyber Headlines & Trends

As of Dec. 2023, the U.S. Securities and Exchange Commission (SEC) has required public companies to report material cyber security incidents on a Form 8-K within four business days of materiality determination.

“In 2024, the **average cost of a data breach** reached a staggering **\$4.88 million**, marking a **10% increase over last year.**” IBM Security's Cost of a Data Breach Report 2024

“**68% of all breaches include the human element, with people being involved either via Error, Use of stolen credentials or Social Engineering.**” Verizon's 2024 Data Breach Investigations Report

“67% of the 10,626 breaches reviewed in 2024 were done by **organized crime** (less than 10% nation-state or state-affiliated actors).” Verizon's 2024 Data Breach Investigations Report

“Sadly, too few organizations learn how valuable MFA is until they experience a breach.” Jen Easterly, Director U.S. Cybersecurity and Infrastructure Security Agency

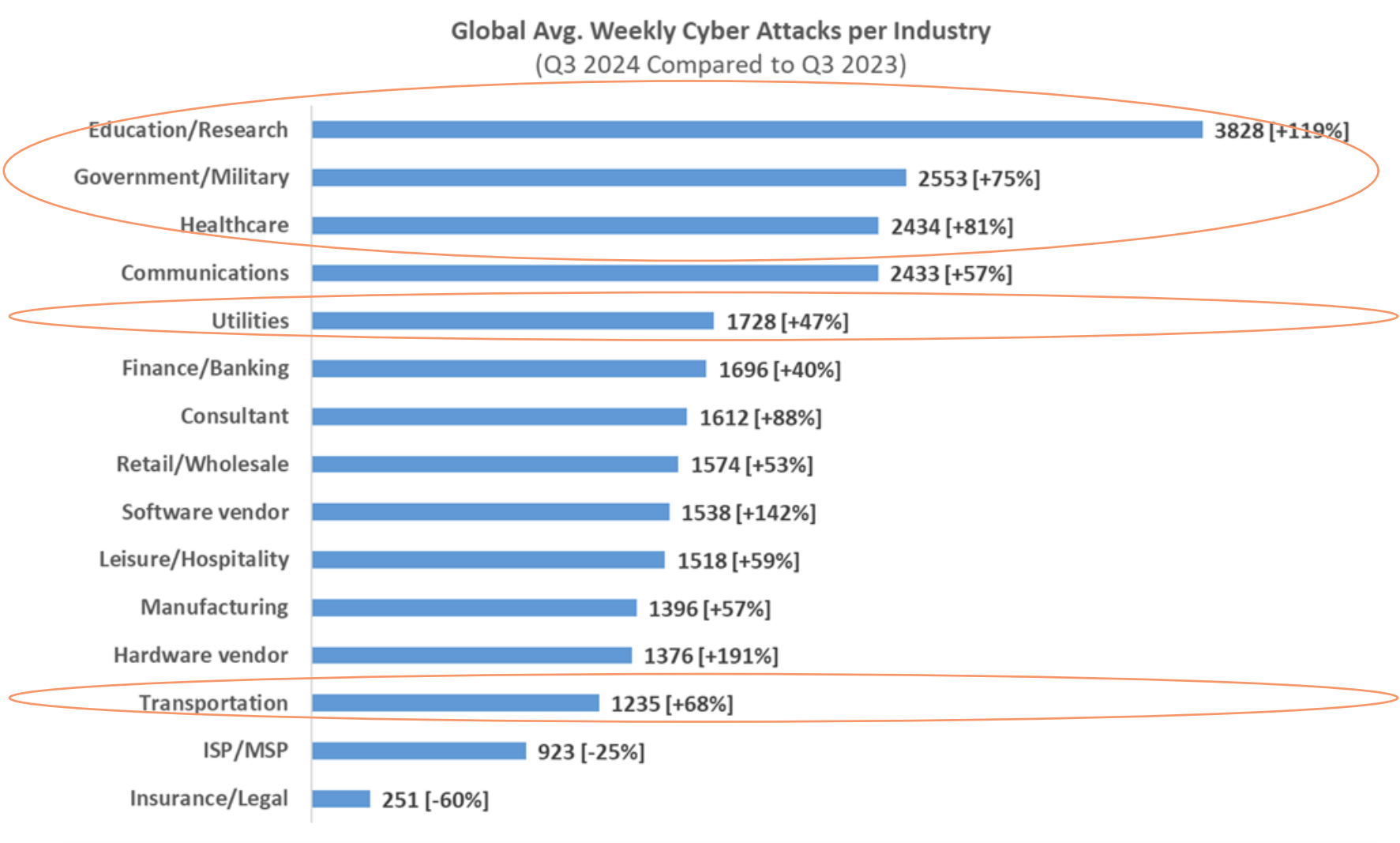
“**This is the new frontier of cybersecurity—an arms race where we're not just battling hackers, but also battling AI-powered machines that can think, adapt, and innovate faster than ever before.**” Forbes, October 2024

“**U.S. utilities faced a near 70% jump in cyberattacks** this year over the same period in 2023, according to data from Check Point Research, underlining the escalating threat to a **critical infrastructure.**” Reuters Sept 2024

“The ransomware attack against Scripps Health that led to more than four weeks of electronic health record (EHR) downtime procedures and the theft of some patient data, resulted in **\$112.7 million** in estimated revenue loss and incremental expenses.” Scripps, Aug. 10, 2021

S&P Global Ratings | Cyber Risk Management

Cyber attacks Increasing Across All Industries



S&P Global Ratings | Cyber Risk Management

Cyberattacks lifecycle



Preparation: Conduct initial due diligence and develop a malware payload that is tailored to the target organization.



Delivery: Introduce the malware payload into the target organization's systems through actions such as phishing or social engineering.



Exploitation: Use the malware payload to exploit a vulnerability in the target organization's systems to gain initial access.



Persistence and control: Establish persistence and control by using the malware payload to install backdoors and command channels.



Actions: Use command channels to conduct desired activities including internal reconnaissance, lateral movement, privilege escalation, data exfiltration, encryption, and business interruption.

Source: S&P Global Ratings.

Copyright © 2023 by Standard & Poor's Financial Services LLC. All rights reserved.

S&P Global Ratings | Cyber Risk Management

Key takeaways from recent cyber incidents



Business impact

- Operations disrupted
- Containment measures
- Manual workarounds or partial service levels
- Reputational risk and brand damage



Communication

- Extensive investigations
- Comply with external reporting rules
- Inform and update diverse stakeholders
- Employee business process updates



M&G

- Reduce management bandwidth
- Multiple external and internal parties involved
- Enhance cyber security framework
- Expand employee training and awareness to cover new risk areas



Financial impact

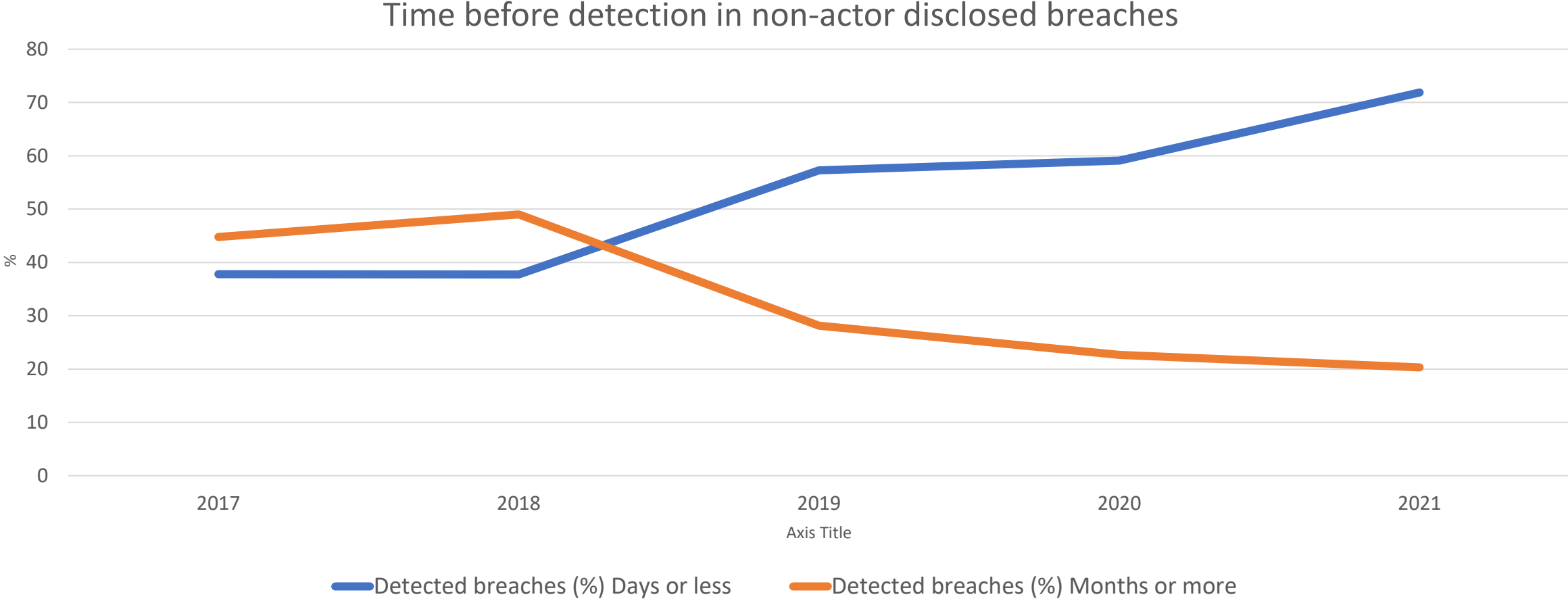
- Increase in opex and capex spend to implement remediation program
- Cyber insurance—loss recovery and exclusions
- Financial position and liquidity
- Regulatory fines or litigation risk

M&G--Management and governance. Opex--Operational expenditure. Capex--Capital expenditure.

Source: S&P Global Ratings.

Copyright © 2023 by Standard & Poor's Financial Services LLC. All rights reserved.

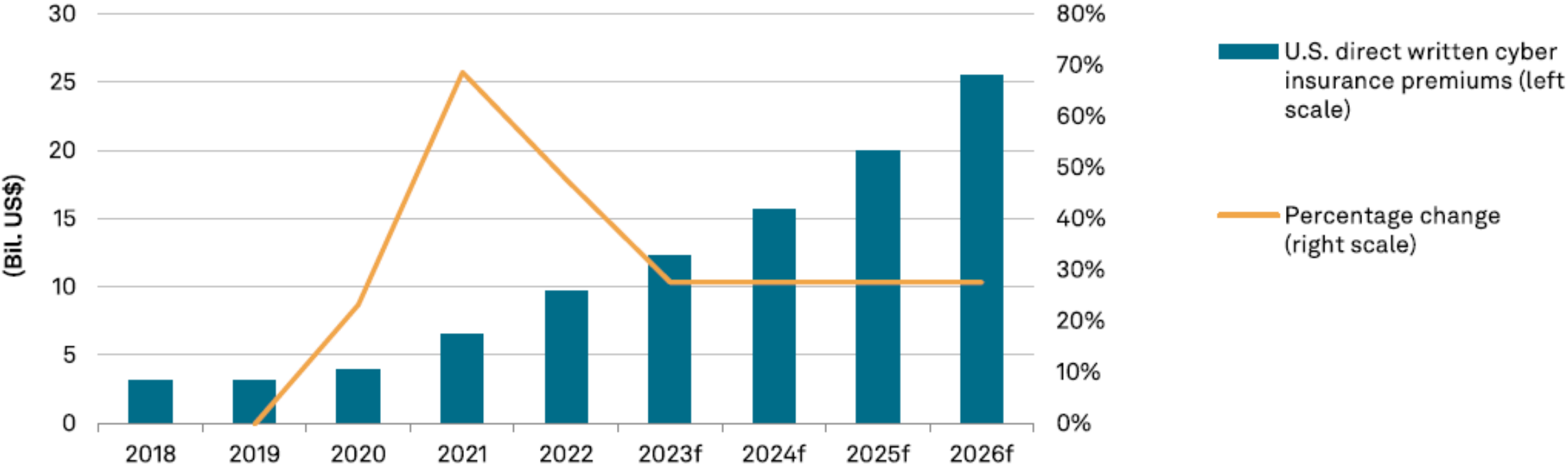
S&P Global Ratings | Cyber Attack Detection is Accelerating



Sources: S&P Global Ratings. 2022 Data Breach Investigations Report, Verizon.

S&P Global Ratings | Cyber Insurance

U.S. cyber insurance premiums will continue to climb



f--Forecast. Source: National Association of Insurance Commissioners, S&P Global Ratings

Copyright © 2024 by Standard & Poor's Financial Services LLC. All rights reserved.

U.S. Public Finance | Cyber Risk Management

What we're watching



Prepare

- ✓ Identify areas of risk
- ✓ Protect assets and data
- ✓ Engage in cyber hygiene practices



Respond

- ✓ Detect and respond to an attack



Recover

- ✓ Recover data
- ✓ Maintain sufficient liquidity
- ✓ Disclose attacks

Source: S&P Global Ratings.

Copyright © 2023 by Standard & Poor's Financial Services LLC. All rights reserved.

U.S. Public Finance | Sample Questions – All Issuers

1. What steps have you (the Issuer) taken to *identify* and *protect* your assets and data from cyberattacks?

- Device registration and access controls
- Firewalls, staff training, virus, and malware scans
- Two-signature requirements on wire transfers and payments

2. What policies and practices have you implemented to enable you to *detect*, *respond* to, and *recover* from a cyberattack?

- Data recovery plans including offsite backups
- Cyber insurance
- System scans to detect malware/attacks
- Ability to isolate attack from affecting entire network

Appendix:

U.S. Public Finance | Other Sample Questions

Local Governments

Management and Governance: What is management's approach to mitigating cyber security threats? (*Prepare*)

States

Management and Governance / System Support: How is the state aiding school districts and local governments in their efforts to mitigate cyber security threats? (*Prepare*)

Healthcare

Management and Governance: How does the organization overall think about risk – whether it be cyber, environmental, epidemics? How has that evolved over time? (*Prepare, Recover*)

Utilities

Management and Governance: How has the utility system incorporated cybersecurity into its risk management practices? How has that evolved over time? (*Prepare, Recover*)

U.S. Public Finance | Cyber Risk Management

Analytical Considerations – Issuer Preparedness



All USPF sectors

Issuers unable to properly identify cyber event risks could encounter significant delays in stopping or recovering from an attack, leading to service disruption, additional liabilities such as ransomware payouts or legal issues from data breaches, or other negative effects that could cause rating pressure. Certain sectors face additional heightened risk if they fail to thoroughly assess their risks and create an action plan to follow should an attack occur.



Electric cooperatives and municipal-owned public power utilities

Given the interconnected nature of the electric grid in the U.S. and its status as both critical infrastructure and highly vulnerable to a sovereign-backed cyberattack, we expect a robust understanding of digitized systems that could be attacked and the downstream impacts an attack could have on operations. This includes understanding if networks are vulnerable to shared risks with state or local governments, or if assets operate on separate networks.



Water and sewer utilities

Water and sewer utilities are at risk on two fronts: infiltration of operations and potential hijacking of customer account information or municipal financial records. With the precedent set for a cyberattack that can threaten the safety of water supply, we expect water utility operators to understand the risks presented by digitalization of services and operations, with sufficient protective measures in place to prevent life and safety risks following an attack. Failure to do so could lead to significant operational and legal costs, pressuring ratings. Furthermore, industry best practices generally specify that utility operations not be connected to the outside world to limit the risk of an intrusion.

U.S. Public Finance | Cyber Risk Management



Not-for-profit health care

With significant amounts of personally identifiable information and medical information subject to HIPAA privacy laws, we expect issuers to have a thorough understanding of retained data and a formidable cyber defense strategy. Failure to have a proper cyber defense strategy and data-management procedures in place is of particular concern for hospitals and health systems as this not only increases the risk of contingent liabilities stemming from data breaches but also jeopardizes the health and safety of patients.



Higher education

Due to the amount of personally identifiable information collected and retained through the admissions process, fundraising, and the conduct of sensitive research, cyber criminals often view higher education institutions as rich targets. In addition, the huge number of devices on college and university information technology networks creates an expectation that these issuers have processes in place to manage these assets in a secure manner as students and faculty join and leave the system frequently. We believe a well-defined threat matrix is crucial to the identification of information that could be at risk from a targeted attack.

Copyright © 2025 by Standard & Poor's Financial Services LLC. All rights reserved.

No content (including ratings, credit-related analyses and data, valuations, model, software or other application or output therefrom) or any part thereof (Content) may be modified, reverse engineered, reproduced or distributed in any form by any means, or stored in a database or retrieval system, without the prior written permission of Standard & Poor's Financial Services LLC or its affiliates (collectively, S&P). The Content shall not be used for any unlawful or unauthorized purposes. S&P and any third-party providers, as well as their directors, officers, shareholders, employees or agents (collectively S&P Parties) do not guarantee the accuracy, completeness, timeliness or availability of the Content. S&P Parties are not responsible for any errors or omissions (negligent or otherwise), regardless of the cause, for the results obtained from the use of the Content, or for the security or maintenance of any data input by the user. The Content is provided on an "as is" basis. S&P PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, FREEDOM FROM BUGS, SOFTWARE ERRORS OR DEFECTS, THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED, OR THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION. In no event shall S&P Parties be liable to any party for any direct, indirect, incidental, exemplary, compensatory, punitive, special or consequential damages, costs, expenses, legal fees, or losses (including, without limitation, lost income or lost profits and opportunity costs or losses caused by negligence) in connection with any use of the Content even if advised of the possibility of such damages.

Credit-related and other analyses, including ratings, and statements in the Content are statements of opinion as of the date they are expressed and not statements of fact. S&P's opinions, analyses, and rating acknowledgment decisions (described below) are not recommendations to purchase, hold, or sell any securities or to make any investment decisions, and do not address the suitability of any security. S&P assumes no obligation to update the Content following publication in any form or format. The Content should not be relied on and is not a substitute for the skill, judgment and experience of the user, its management, employees, advisors and/or clients when making investment and other business decisions. S&P does not act as a fiduciary or an investment advisor except where registered as such. While S&P has obtained information from sources it believes to be reliable, S&P does not perform an audit and undertakes no duty of due diligence or independent verification of any information it receives. Rating-related publications may be published for a variety of reasons that are not necessarily dependent on action by rating committees, including, but not limited to, the publication of a periodic update on a credit rating and related analyses.

To the extent that regulatory authorities allow a rating agency to acknowledge in one jurisdiction a rating issued in another jurisdiction for certain regulatory purposes, S&P reserves the right to assign, withdraw, or suspend such acknowledgement at any time and in its sole discretion. S&P Parties disclaim any duty whatsoever arising out of the assignment, withdrawal, or suspension of an acknowledgment as well as any liability for any damage alleged to have been suffered on account thereof.

S&P keeps certain activities of its business units separate from each other in order to preserve the independence and objectivity of their respective activities. As a result, certain business units of S&P may have information that is not available to other S&P business units. S&P has established policies and procedures to maintain the confidentiality of certain nonpublic information received in connection with each analytical process.

S&P may receive compensation for its ratings and certain analyses, normally from issuers or underwriters of securities or from obligors. S&P reserves the right to disseminate its opinions and analyses. S&P's public ratings and analyses are made available on its Web sites, www.spglobal.com/ratings (free of charge) and www.ratingsdirect.com (subscription) and may be distributed through other means, including via S&P publications and third-party redistributors. Additional information about our ratings fees is available at www.spglobal.com/ratings/usratingsfees.

Australia: S&P Global Ratings Australia Pty Ltd holds Australian financial services license number 337565 under the Corporations Act 2001. S&P Global Ratings' credit ratings and related research are not intended for and must not be distributed to any person in Australia other than a wholesale client (as defined in Chapter 7 of the Corporations Act).

STANDARD & POOR'S, S&P and RATINGSDIRECT are registered trademarks of Standard & Poor's Financial Services LLC.

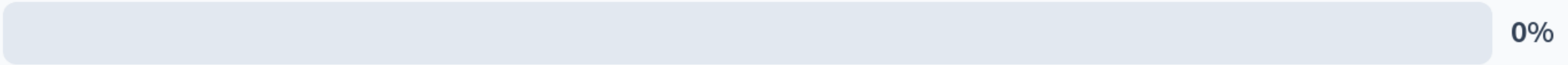
spglobal.com/ratings

Has your organization experienced a material cybersecurity breach in the last five years?

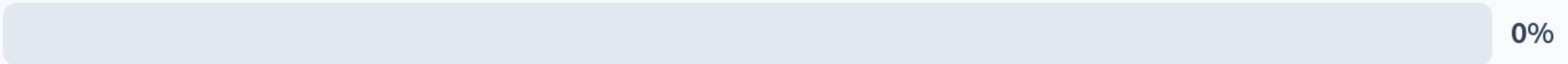
Yes, and we disclosed the event in an offering statement or voluntary filing



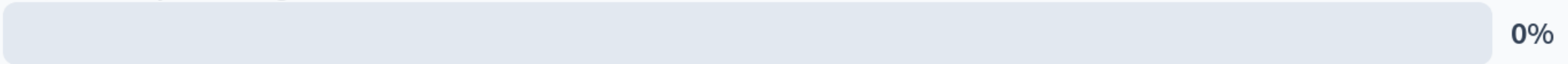
Yes, and we did not refer to it in an offering document or voluntary filing



We experienced one or more cyber breaches, but they were not material



No, not to my knowledge

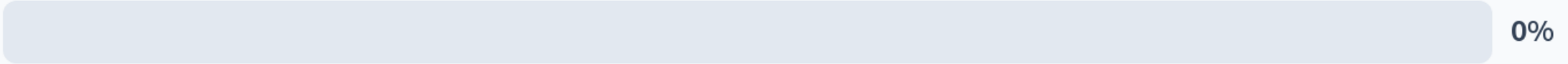


Discussion on Question 1

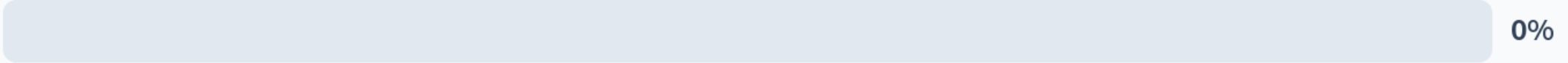
- Market Perspective
- Issuer Perspective
 - No obligation to speak absent contractual agreement or other arrangement; disclosure contexts
 - Public offering – disclosure; option to delay offering
 - Voluntary disclosure; cybersecurity incident disclosure guidance; cautionary statements

Does your organization have established cybersecurity procedures and processes?

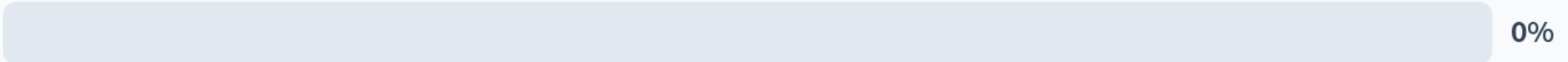
Yes, we have management-approved established procedures and processes



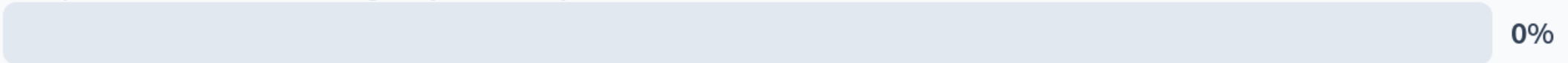
No; we have established practices



No; we have an ad hoc approach to cybersecurity



No specific instructions relating to cybersecurity have been communicated to me



Discussion on Question 2

❖ Market Perspective

- Potential impact on rating
- How to positively impact rating

❖ Issuer Perspective

- Additional protection from threat actors
- 2023 SEC cybersecurity guidance
- Third parties
- Insurance

California Debt and Investment Advisory Commission 2025



GASB DIGITAL REPORTING UPDATE

Electronic Financial Reporting Update

April 2025

The views expressed in this presentation are those of Paulina Haro.
Official positions of the GASB are reached only after extensive due process and deliberations.

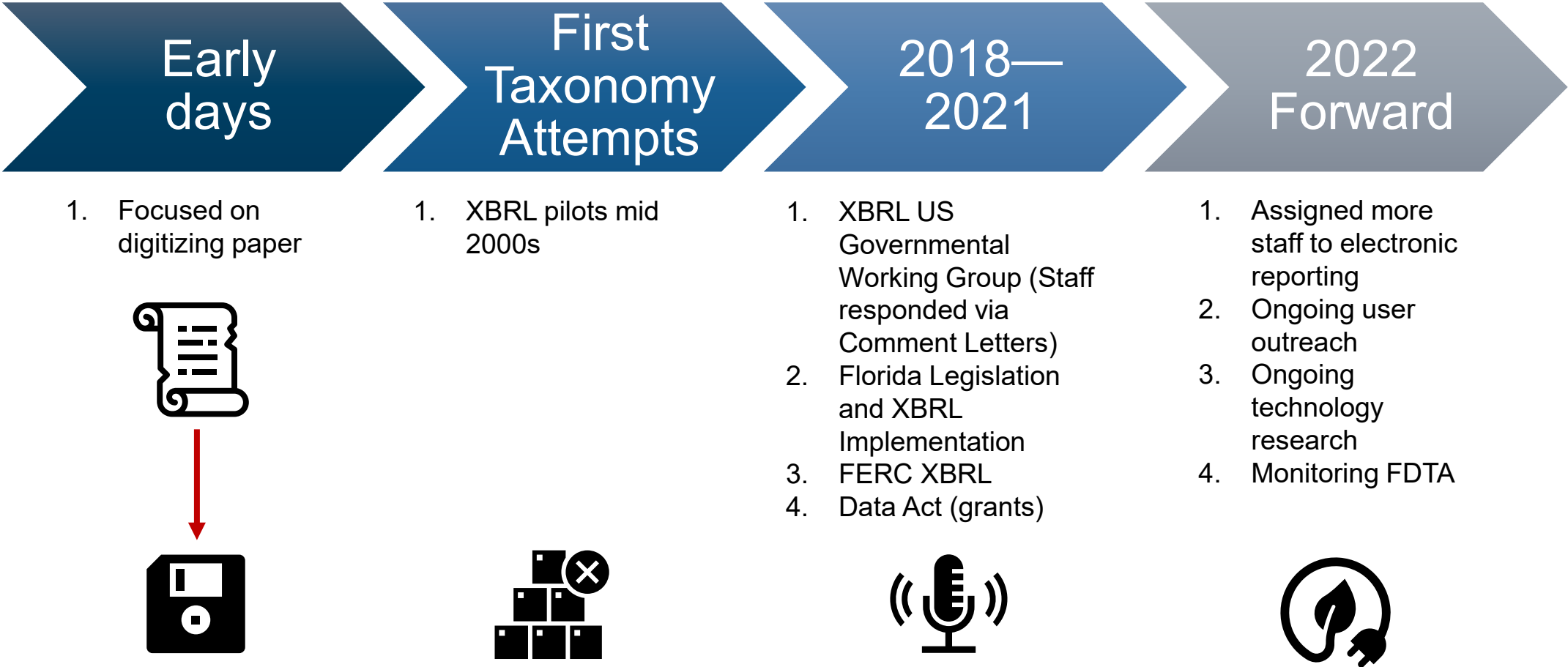
Presentation Outline

- Background and Financial Data Transparency Act (FDTA)
- GASB-GAAP Taxonomy
 - Line Item Approach
 - Basis of Accounting Design Options
 - Notes to Financial Statements
- Project Plan



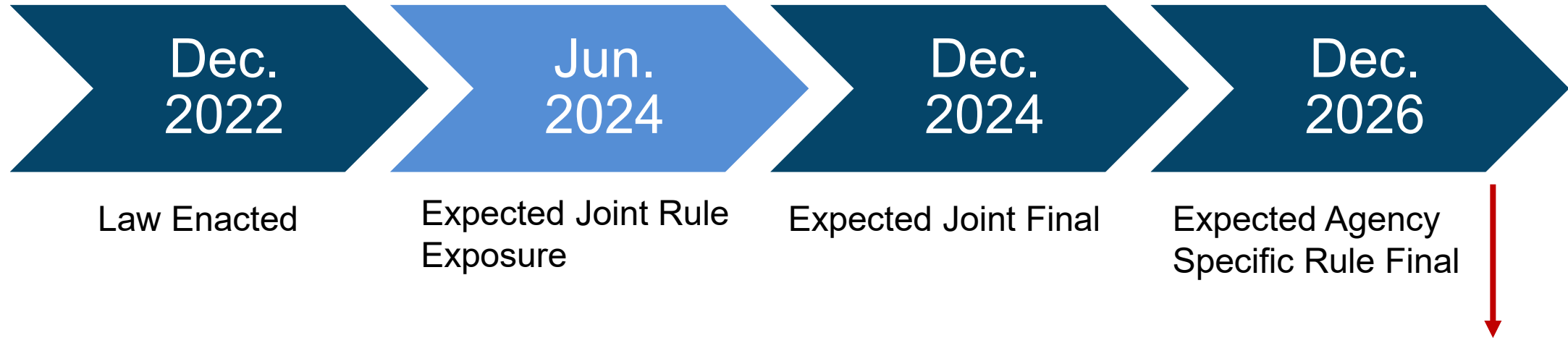
Background and Project Information

GASB and Electronic Financial Reporting



Staff has been engaged in Electronic Financial Reporting for over a decade.

Financial Data Transparency Act—FDTA



■ **Joint Rule Making:**

- Proposal: July 30, 2024
- Comment period ends: October 21, 2024
- Final rule expected: December 2024
- Three topics proposed (see next slide)

- FDTA is effective 2027; except for the reporting that may be required by the SEC and/or MSRB which does not have a defined effective date.

Joint Rule Proposal

Identifiers

- Legal Entity Identifier
- Securities Identifier (FIGI)
- Other Identifiers

Technology

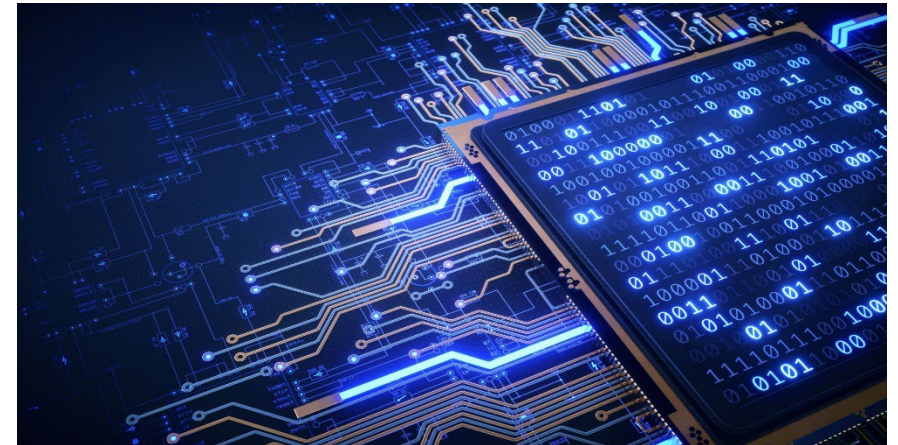
- Characteristics (4)
- List of examples

Accounting Taxonomies

- Joint Standard for taxonomies
- Agency Specific Taxonomies

Examples Identified

1. CSV
2. XML
3. JSON
4. PDF/A
5. HTML-XBRL (Inline XBRL)



GASB-GAAP Taxonomy

GAAP Reporting Requirements

ONE set of GAAP financial reporting requirements for ALL types of Governments

Three Communication Methods

Basic Financial Statements

Required Supplementary Information

Supplementary Information

Minimum Requirements for Each Communication Method

Basic financial statements include:

- Government Wide Financial Statements
- Fund Financial Statements
- Notes to Financial Statements

Optionality in GAAP

- For example: Statement of Net Position
1. Classified presentation
 2. Unclassified presentation
 3. Combined Resource Focus


Common Practice

For example, line items:

- Assets, Deferred outflows of resources, Liabilities, Deferred inflows of resources, Net Position




Industry Concerns—Overview



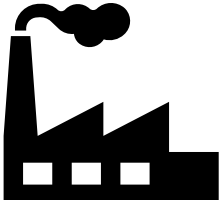
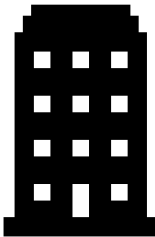
Structure of Financial Statements

- Different statements for different types of governments



Line items are different in each industry

- Level of detail is different



Taxonomy Development Example—City of ABC

Assets:

Cash, cash equivalents and investments

Receivables, net:

Property taxes

Accounts

Lease receivable

Other

Total receivables

	General	Debt Service	Capital Projects	General COVID Relief	Other Governmental Funds	Total Governmental Funds
\$	206,527	\$ 197,985	\$ 188,610	\$ -	\$ 239,659	\$ 832,781
Property taxes	6,607	1,643	189	-	90	8,529
Accounts	5,478	-	32	-	3	5,513
Lease receivable	12,735	-	21	-	19	12,775
Other	54	-	-	-	179	233
Total receivables	24,874	1,643	242	-	291	27,050

Governmental Funds [Axis]

Governmental Funds [Domain]

General Fund [Member]

Other Major Governmental Funds Excluding General Funds [Member]

Major Special Revenue Funds [Member]

Major Capital Project Funds [Member]

Major Debt Service Funds [Member]

Major Permanent Funds [Member]

Nonmajor Governmental Funds [Member]

Nonmajor Special Revenue Funds [Member]

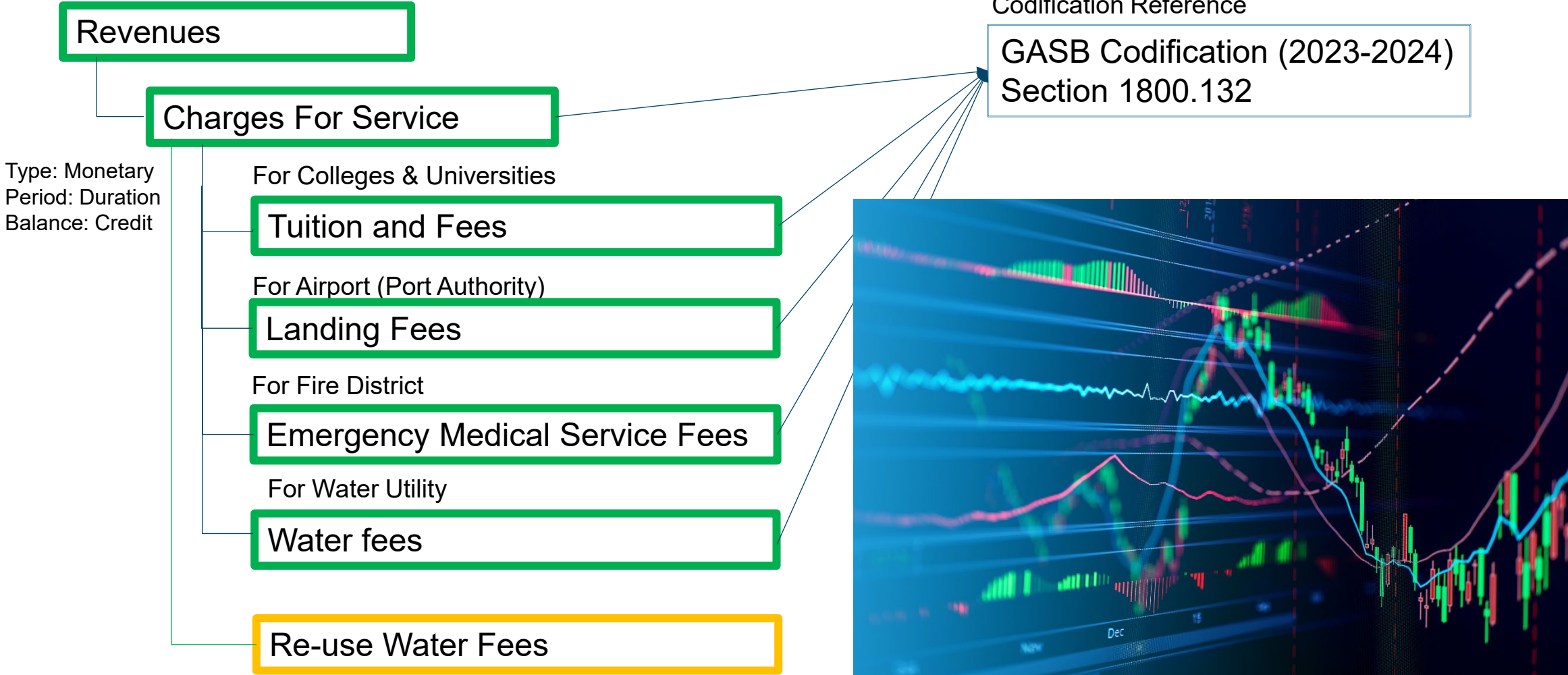
Nonmajor Capital Project Funds [Member]

Nonmajor Debt Service Funds [Member]

Nonmajor Permanent Funds [Member]

Other Nonmajor Governmental Funds [Member]

GASB's Tentative Approach



Notes to Financial Statements (Unstructured Data)

3. Securities Lending

State Statutes permit the State Treasurer to lend its securities, through the use of agents, to broker-dealers and other entities with simultaneous agreement to return the collateral for the same securities in the future. The State's agents lend securities, of the type on loan at year-end, for collateral in the form of cash or other securities at 100% of value for US Treasury Strips and US Treasury Bills, and 102% of value for other securities. The State, through its agents, measures the fair value of the securities loaned against the fair value of the collateral on a daily basis. Additional collateral is obtained as necessary to ensure such transactions are adequately collateralized. Securities lent for securities collateral are classified according to the category of the collateral. At year-end, the State has no credit risk exposure to borrowers because the amounts the State owes the borrowers exceed the amounts the borrowers owe the State. The contract with the State's agent requires the agent to indemnify the State if the borrowers fail to return the securities (and if the collateral is inadequate to replace the securities lent) or fail to pay the State for income distributions by the securities' issuers while the securities are on loan.

The following represents the balances relating to the securities lending transactions at the financial statement date:

Without WYO-STAR:

Securities Lent	Fair Value of Underlying Securities without Accrued Interest	Cash Collateral Received/Securities Collateral Value
Lent for Cash Collateral		
U.S. Governments	\$ 3,236,874,620	\$ 3,315,933,782
U.S. Corporate Securities	345,185,368	356,741,200
U.S. Equities	551,739,838	563,743,345
Non U.S. Governments (USD)	3,554,172	3,655,633
Non U.S. Equities	58,738,273	60,710,138
Total Lent for Cash Collateral	4,196,092,271	4,300,784,098
Lent for Securities Collateral		
U.S. Governments	1,389,586,164	1,424,574,498
U.S. Corporate Securities	5,201,617	5,416,144
U.S. Equities	110,828,489	114,055,005
Non U.S. Equities	25,111,629	26,396,303
Total Lent for Bulk (Securities) Lending	1,530,727,900	1,570,441,951
Total Securities Lending	\$ 5,726,820,170	\$ 5,871,226,049

Details for Unstructured Data

- Implementation Y1: Large block text

- Implementation Y2: Discrete block text

- Implementation Y3: Detailed items

ALL Unstructured Data in GASB-GAAP (notes to financials, MD&A, and notes to RSI) are modeled in this tiered approach

Project Update

Due Process document

GASB-GAAP Taxonomy

Voluntary Digital Financial Reporting Project



Phase I

- Basic Financial Statements
- Required Supplementary Information

Basic Financial Statements:

- Government-Wide Financial Statements
- Fund Financial Statements
- Notes to Financial Statements



Phase II

- Supplementary Information

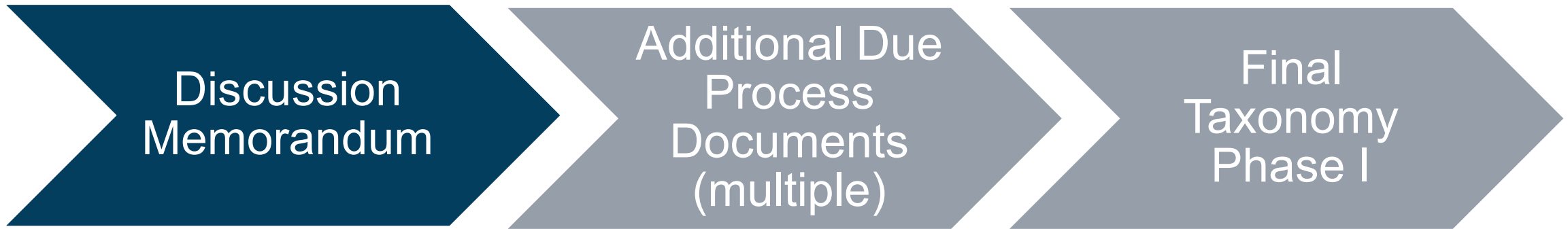
Required Supplementary Information:

- Pensions and OPEB Schedules
- Infrastructure Schedule
- Budgetary Schedules

GASB-GAAP Taxonomy

Voluntary Digital Financial Reporting Project

Phase I



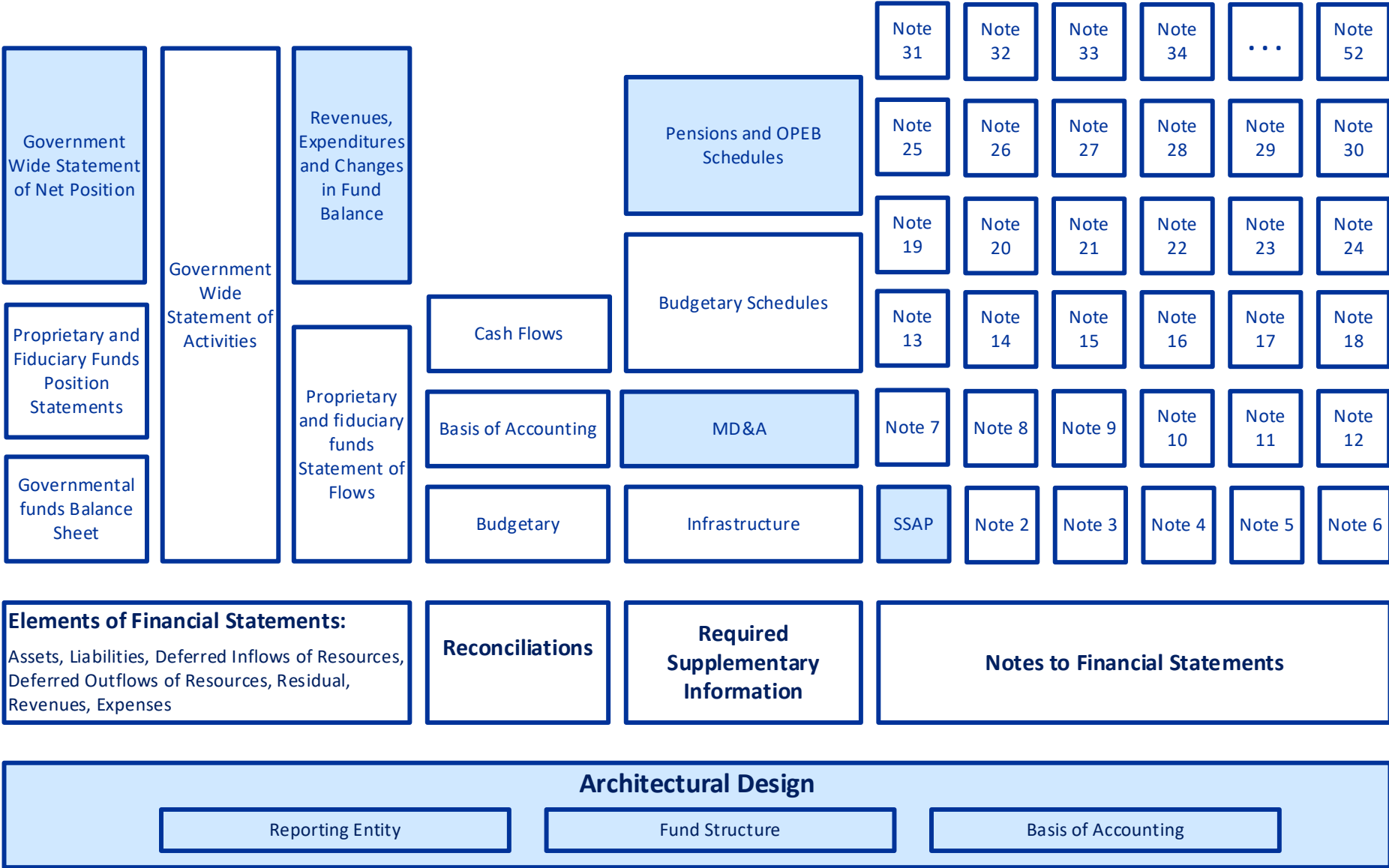
Content

- Government-Wide Statement of Net Position (Unclassified)
- Revenues, Expenditures, and Changes in Fund Balance
- Pension and OPEB RSI Schedules
- Management’s Discussion and Analysis

Purpose—Solicit Feedback

- The architectural design choices made in the design of the GASB-GAAP Taxonomy
- Does NOT include all components of the taxonomy
- Is NOT a final product, its an early discussion document

GASB GAAP Taxonomy—Phase I Components

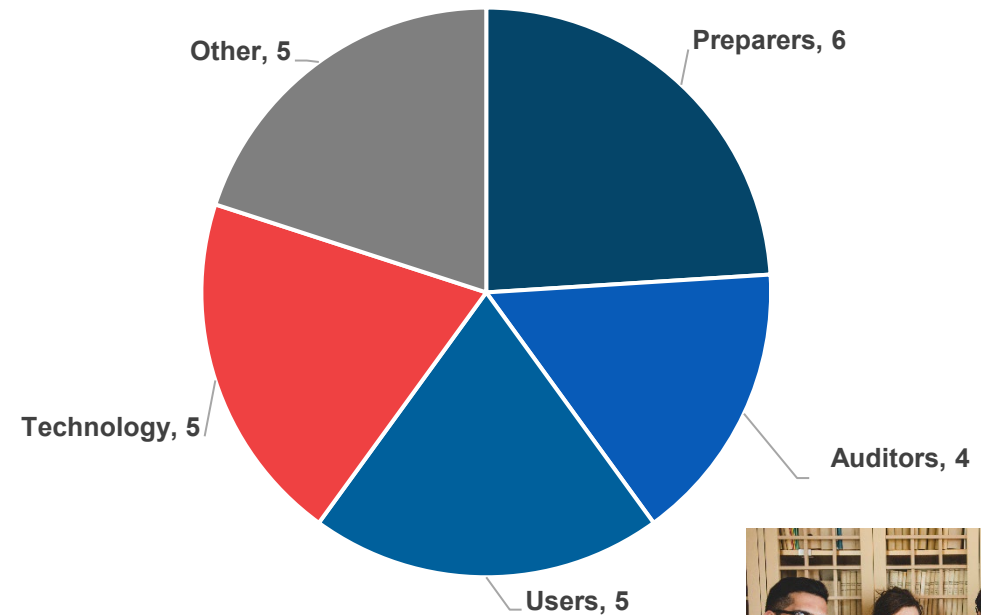


Components scheduled for exposure in December

Taxonomy Consultative Group (TCG)

1. Charter and participants are ready
 - We expect 25 members
2. Meetings will begin after March Board meeting
 - Virtual meetings
 - Subgroup strategy
3. Periodic feedback will be solicited
 - Technology
 - Common practice
4. Board meeting with TCG: Q4 2025

TCG Composition



QUESTIONS?



PAULINA HARO
Senior Project Advisor
Governmental
Accounting Standards
Board



DONALD HESTER
Cybersecurity Advisor
Cybersecurity and
Infrastructure
Security Agency



DIANE QUAN
Partner
Hawkins Delafield
& Wood LLP



KRYSTAL TENA
Associate Director
S&P Global Ratings



15-MINUTE --- BREAK

SESSION FOUR

Climate Change and Natural Hazard Risk Assessment and Disclosures



DANIEL DEATON
Partner
Nixon Peabody LLP



RENEE DOUGHERTY, CFA
*Director, Municipal
Research*
Charles Schwab Asset
Management



BRIAN MCCARTAN
Senior Fellow
Ceres, Inc.



JAN WHITTINGTON, PhD
Professor
University of
Washington, Seattle

SESSION FOUR

Climate Change and Natural
Hazard Risk Assessment and
Disclosures

DANIEL DEATON

Partner

Nixon Peabody LLP



SESSION FOUR

Climate Change and Natural
Hazard Risk Assessment and
Disclosures

JAN WHITTINGTON

*Professor, U of Washington
CEO, Climate Solutions Intl.*



Issuer Capacity to Assess Climate Risk



CA Govts have a mandate, talent, and capital budgets / financial plans



There are tools and data with forecasts from global climate models



Climate risk info can be localized (downscaled) to visualize risk over time



Historical studies have made forecasts of material loss and damage possible



Issuers can adapt capital budgets / financial plans to disclose climate risk

California law (SB 379) Mandated Assessments of Vulnerability

- Required all cities and counties to
 - Address climate adaptation and resiliency strategies
 - Applicable to the city or county
 - In the ‘safety elements’ of their general plans or FEMA-mandated local hazard mitigation plans

Learn more at ResilientCA.org
- Key question
 - Is this used in capital budgets / financial plans?

Local Gov't. Approaches to Assessing Climate Risk Vary

- CA publicly available tool: CalAdapt
 - Helpful access to data from global climate models
 - Needs more work to localize risk to assets
- Some Cities and Counties have localized risk
 - Still challenged to integrate with budget & finance

CalAdapt is a Starting Point for Climate Risk Assessments

cal-adapt

Tools

Data

Help

Blog

Events

About



Explore and analyze climate data from California's Climate Change Assessments

Cal-Adapt provides the public, researchers, government agencies and industry stakeholders with essential data & tools for climate adaptation planning, building resiliency, and fostering community engagement.



Cal-Adapt is evolving!

Learn about the Cal-Adapt enterprise and our mission to support California's climate change initiatives and preview our future plans.

[READ MORE](#)

i Looking for climate data for California's Fifth Climate Change Assessment? Visit the [blog post on accessing next generation climate data](#)















Latest on Cal-Adapt Blog

144

[Empowering Climate Resilience at the](#)

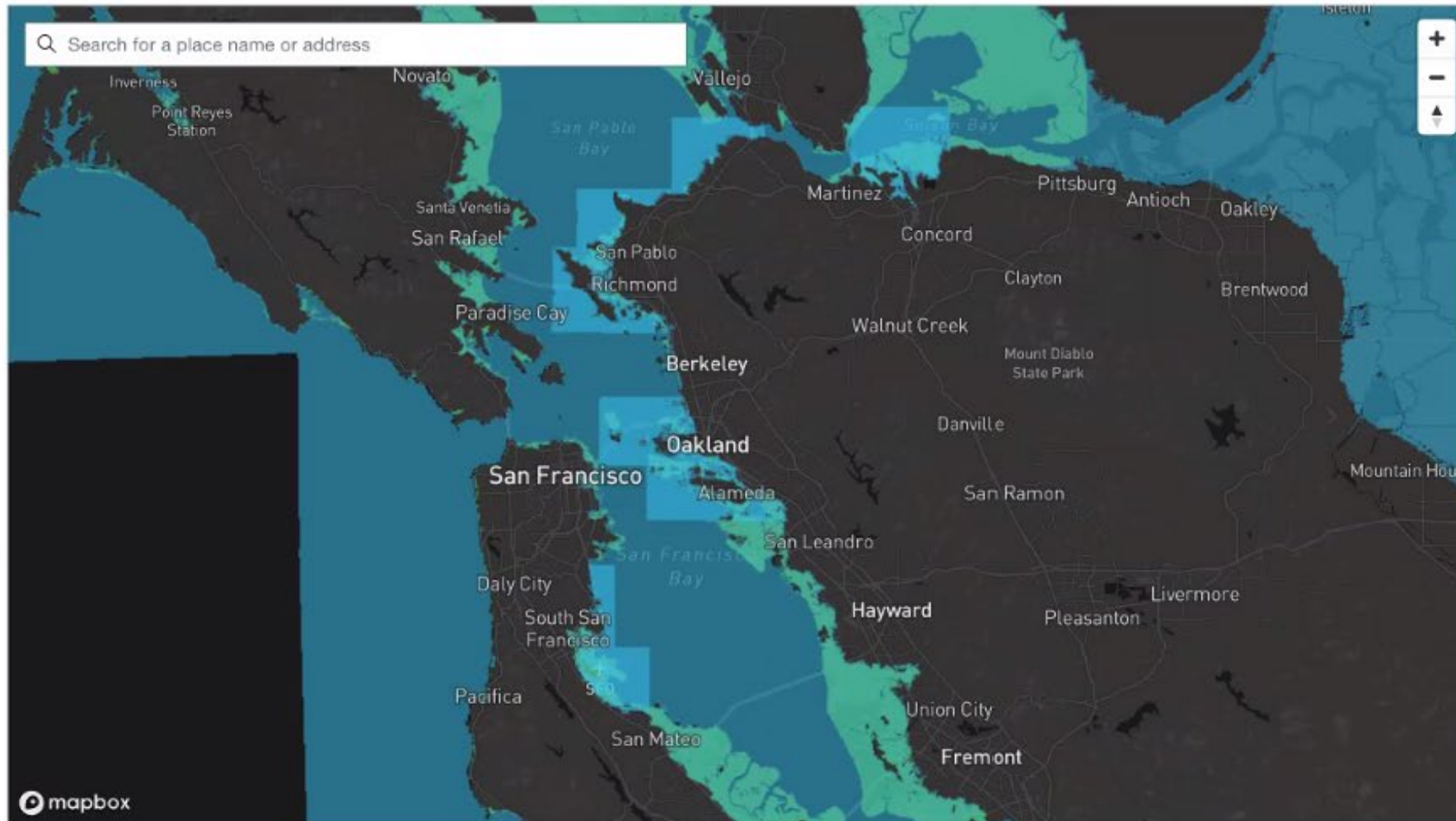
[California Adaptation Framework 2022](#)

CalAdapt is a Toolkit for Accessing Global Climate Models

 <p>Local Climate Change Snapshot</p> <p>A starting point to get climate impacts for your location.</p> <p>EXPLORE</p>	 <p>Annual Averages</p> <p>Projected annual averages of maximum & minimum temperatures and precipitation.</p> <p>EXPLORE</p>	 <p>Sea Level Rise – Coastal Inundation Scenarios</p> <p>Explore the extent of coastal inundation associated with Sea Level Rise and a 100-year storm from two different SLR models.</p> <p>EXPLORE</p>	 <p>Extreme Weather</p> <p>Extreme weather events for baseline and future climates.</p> <p>EXPLORE</p>
 <p>Maps of Projected Change</p> <p>Maps depicting long-term (30 years) changes in annual average temperature and precipitation.</p> <p>EXPLORE</p>	 <p>Extreme Precipitation Events</p> <p>Changes in intensity and frequency of extreme precipitation events.</p> <p>EXPLORE</p>	 <p>Extreme Heat Days & Warm Nights</p> <p>Projected frequency and duration of extreme heat days and warm nights.</p> <p>EXPLORE</p>	 <p>Sea Level Rise – CalFloD-3D</p> <p>Maps of inundation during 100 year storm events with projected Sea Level Rise scenarios.</p> <p>EXPLORE</p>
 <p>Snowpack</p> <p>Timelapse animation and monthly averages of projected Snow Water Equivalent.</p> <p>EXPLORE</p>	 <p>Wildfire</p> <p>Annual and monthly averages of area burned and decadal fire probability for 4 GCMs, and 2 RCPs.</p> <p>EXPLORE</p>	 <p>Cooling Degree Days and Heating Degree Days</p> <p>A common proxy for energy needed to heat and cool buildings.</p> <p>EXPLORE</p>	 <p>Streamflow</p> <p>Charts of VIC routed and bias corrected streamflows driven by LOCA downscaled temperature and precipitation.</p> <p>EXPLORE</p>
			

CalAdapt: Sea Level Rise

Showing available data for **CoSMoS** and **CalFloD3D-TFS (5m)** and **CalFloD3D-TFS (50m)** under a **median** flood scenario for the **2080–2100** period.



SELECT MAP DATA LAYERS

- CoSMoS
- CalFloD3D-TFS (5m)
- CalFloD3D-TFS (50m)

[Learn More](#) ⓘ

SELECT TIME PERIOD

- 2020–2040
- 2080–2100

[Learn More](#) ⓘ

SELECT FLOOD SCENARIO

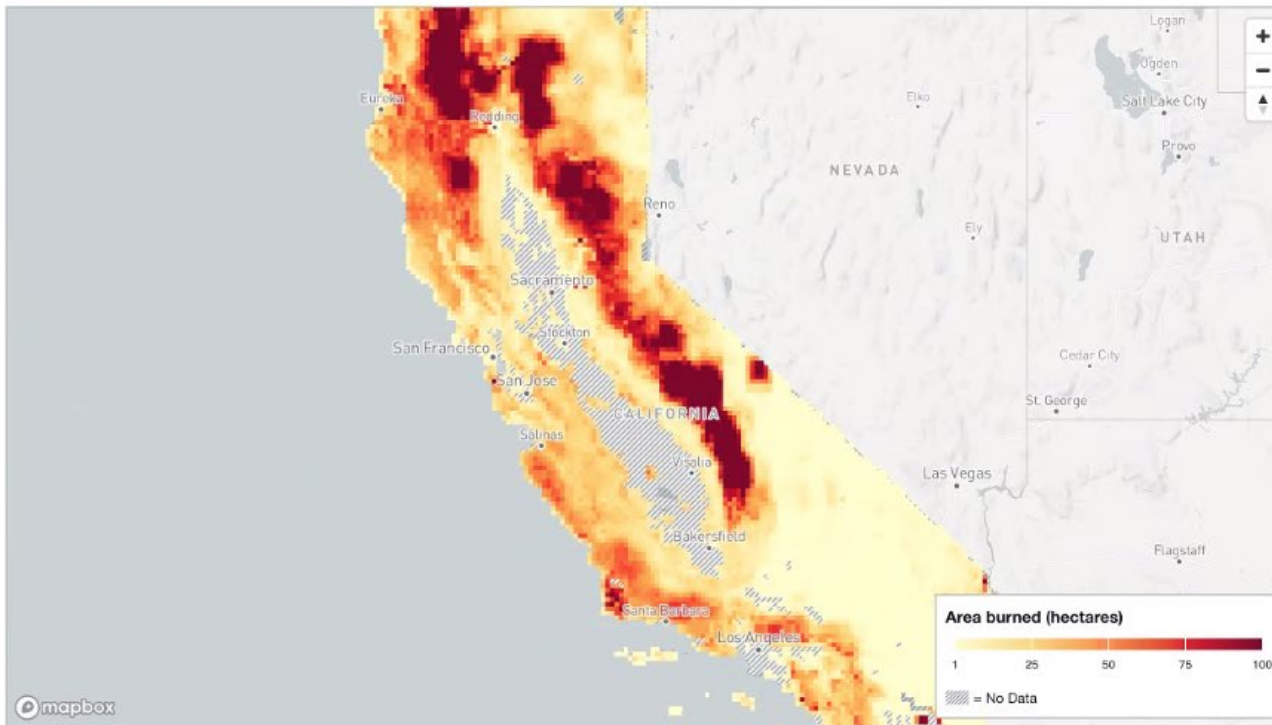
- minimum
- median
- maximum

[Learn More](#) ⓘ

CalAdapt: Wildfire

Decadal Averages Map showing **Modeled Annual Area Burned** over 2090–2099 under a **High Emissions (RCP 8.5) Scenario** and Central Population Growth scenario for **HadGEM2-ES**

! Locations outside the combined state and federal fire protection responsibility areas were excluded from these wildfire simulations and have no wildfire projections.. These areas are shaded in gray.



Decadal wildfire probability

[Learn More](#) ⓘ

SELECT SCENARIO

Medium (RCP 4.5)

High (RCP 8.5)

[Learn More](#) ⓘ

SELECT SIMULATION

Annually

Monthly

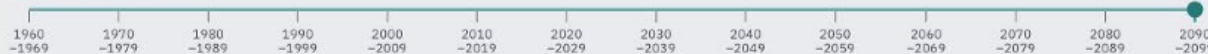
[Learn More](#) ⓘ

SELECT MODEL

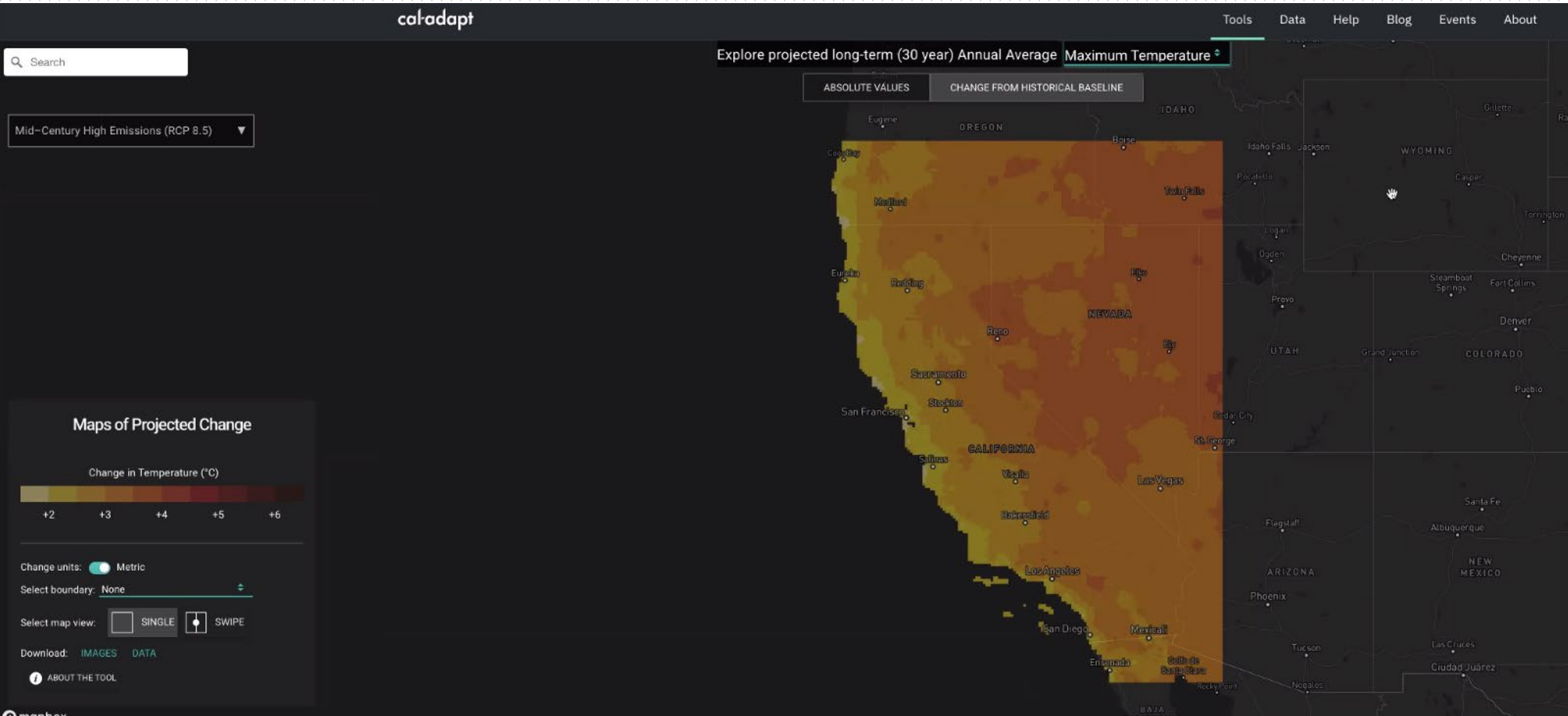
HadGEM2-ES (Warm/Dry) ▾

[Learn More](#) ⓘ

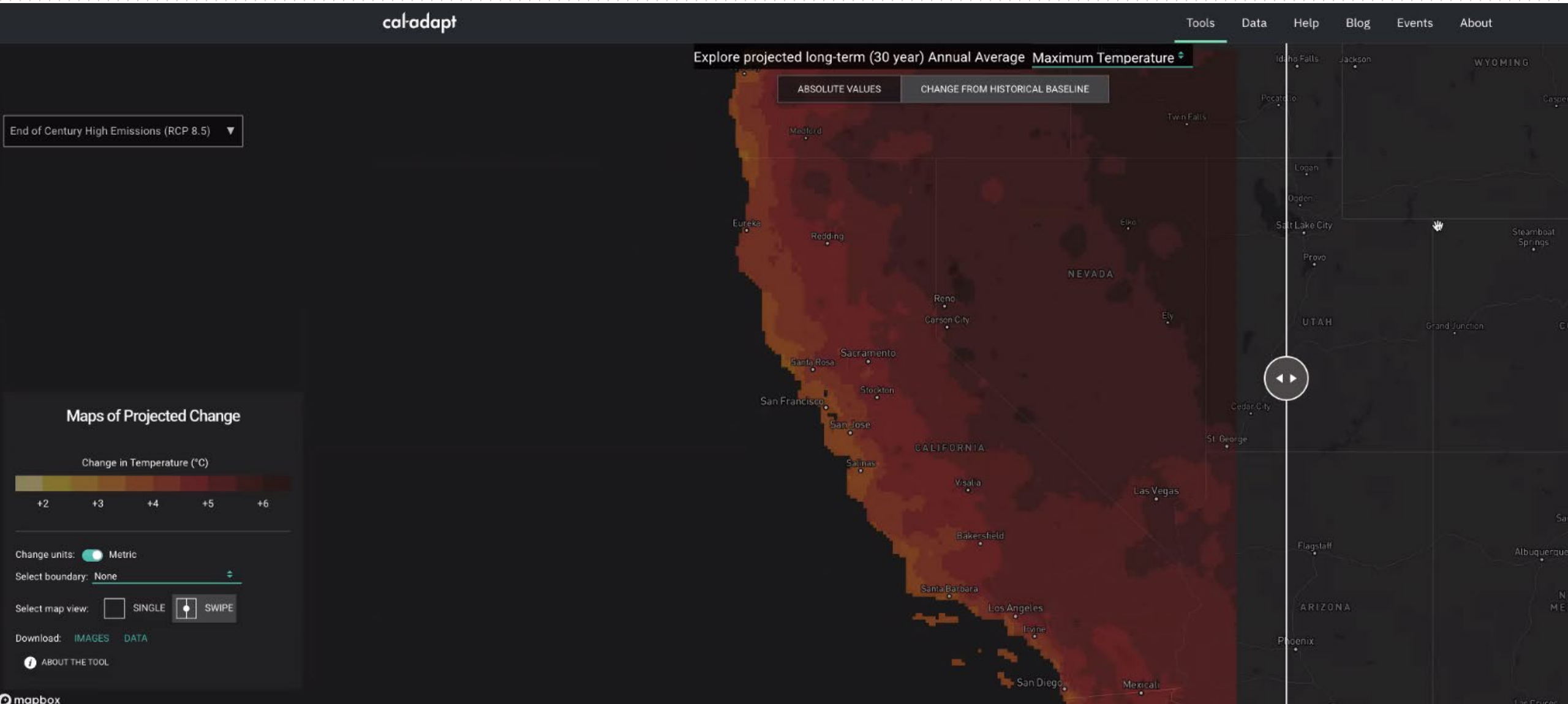
SELECT TIME RANGE



CalAdapt: Max Temperature Rise (Mid-Century)



CalAdapt: Max Temperature Rise (End of Century)



CalAdapt: Extreme Precipitation as Stream Flow

American River at Fair Oaks, California

[Change Location](#)

Projected changes in **Annual Total Unimpaired Flows** by water year for **March, April and May** under a **High Emissions (RCP 8.5) Scenario**.

MODELED HISTORICAL

Baseline (1961-1990)

[Change Period](#)

30 YEAR AVG

22,985 cfs

30 YEAR RANGE

3,440–45,886 cfs

[Learn More](#)

FUTURE PROJECTIONS

Mid-Century (2035-2064)

[Change Period](#)

30 YEAR AVG

22,591 cfs

30 YEAR RANGE

4,134–72,956 cfs

[Learn More](#)

FUTURE PROJECTIONS

End-Century (2070-2099)

[Change Period](#)

30 YEAR AVG

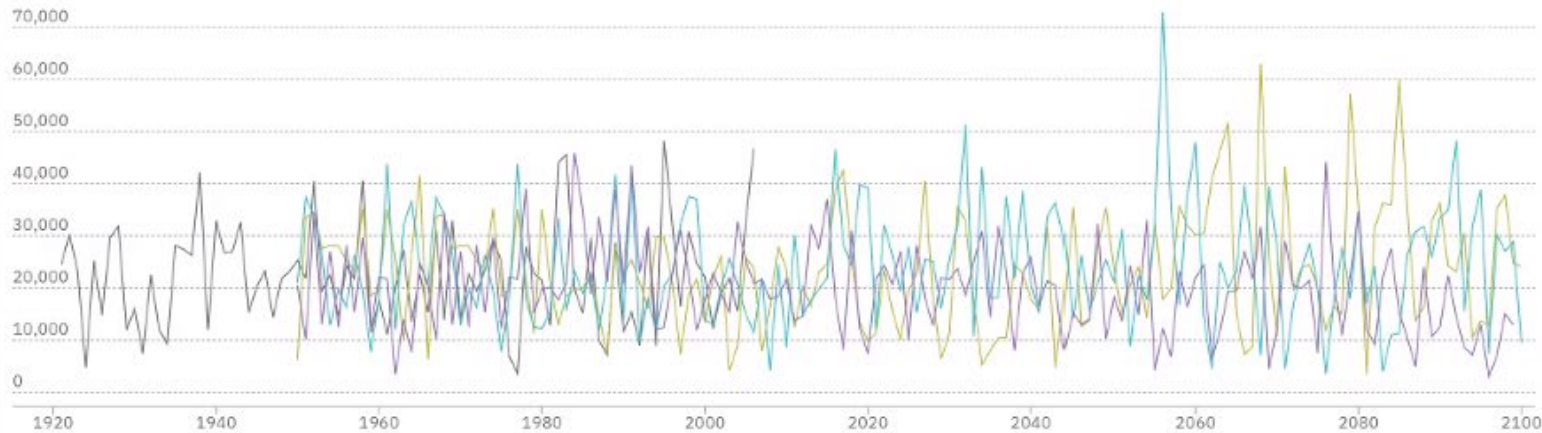
22,109 cfs

30 YEAR RANGE

2,948–60,043 cfs

[Learn More](#)

80,000 Annual Total Unimpaired Flows (cfs)



■ Observed ■ CanESM2 (Average) ■ CNRM-CM5 (Cool/Wet) ■ MIROC5 (Complement)

Source: Cal-Adapt. Data: Routed Streamflow Projections (Scripps Institution of Oceanography), Unimpaired Historical Streamflows (California Department of Water Resources).

SELECT STATION



[Learn More](#)

SELECT INDICATOR

- Annual
- Monthly

[Learn More](#)

SELECT MONTH

3 x Select months ^

- March
- April
- May
- January
- February
- June

3 x Select... v

CanESM2, MIROC5, CNRM-CM5

[Learn More](#)

Climate Risks Need to be Localized and Monetized

- Localize
 - CalAdapt
 - Wildfire
 - Sea Level Rise (but will need tides + precipitation)
 - Get to parcel level projections, 2100
 - Urban Heat Island Effect (Temperature)
 - Flooding (Precipitation)
- Monetize
 - Is this used in capital budgets / financial plans?

Example of Localized Climate Risk: City of San Luis Obispo

- COMMUNITY DEVELOPMENT

+ Key Information & Reporting

+ Cannabis

- Planning & Zoning

+ Zoning

Zoning Map

Specific & Area Plans

Planning Permits

Tiny Home on Wheels

- General Plan

Housing Element

Noise Element






Safety Element

Conservation and Open Space Element



Government » Department Directory » Community Development » Planning & Zoning » General Plan »

CLIMATE ADAPTATION AND SAFETY ELEMENT

Font Size:    Share & Bookmark  Feedback  Print

The Safety Element of the General Plan was last updated on January 17, 2023, in accordance with state law (Senate Bill 379 Government Code Section 65302) that requires integration of comprehensive climate adaptation and resilience strategies, the City applied and received a Sustainable Communities Grant from the California Department of Transportation.

Under state law, a safety element promotes protection for the community from unreasonable risks related to slope instability, seismic activity, subsidence, liquefaction, known geologic hazards, flooding, wildland and urban fires, tsunamis, seiche,

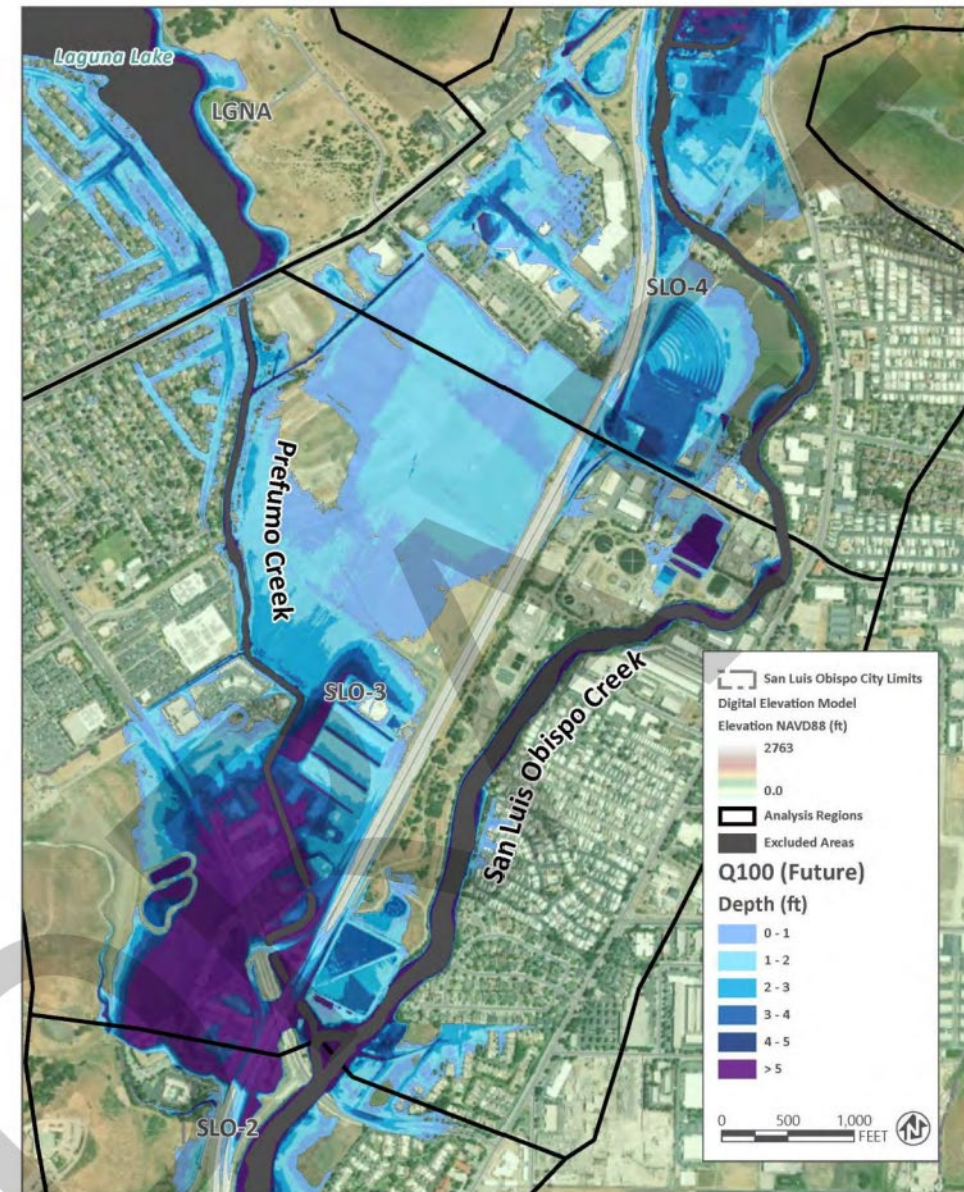
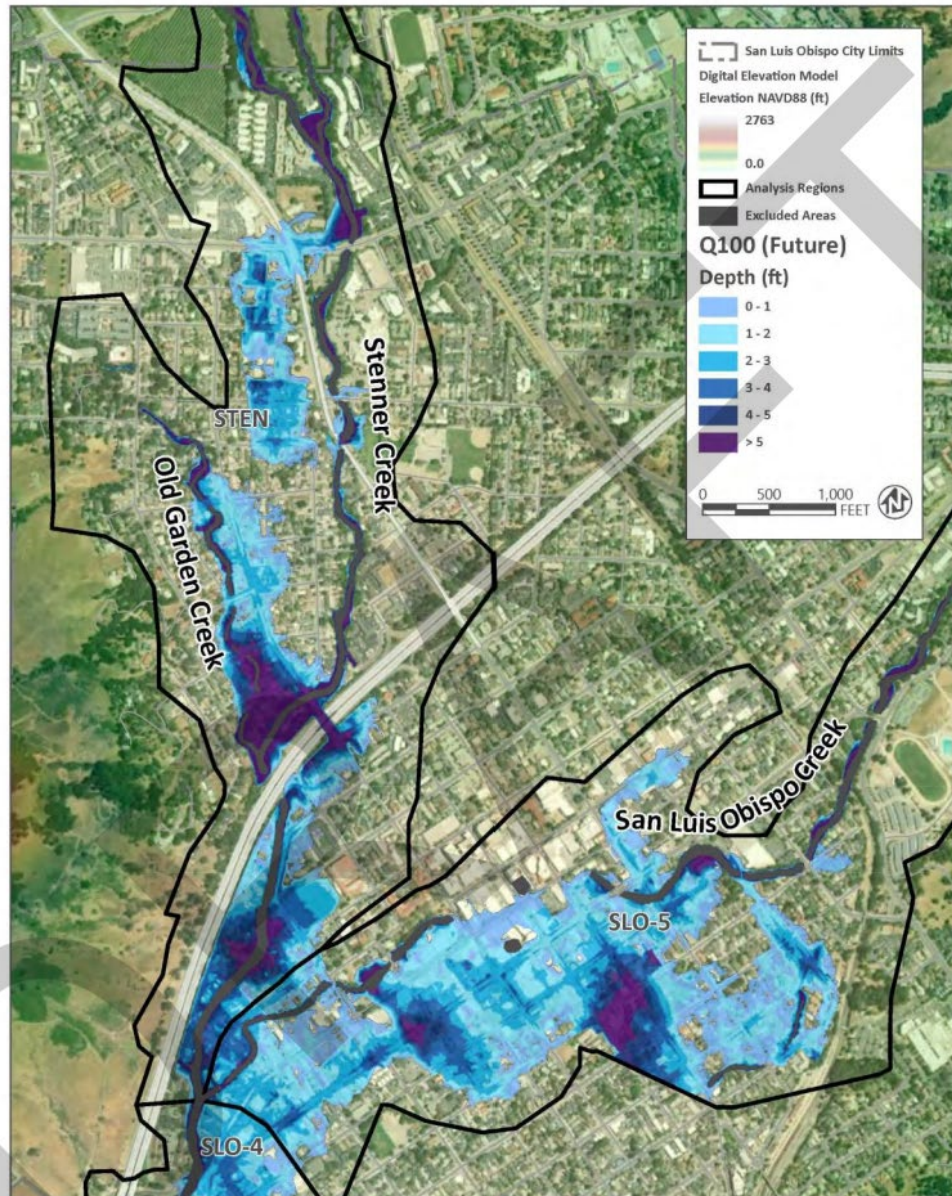
FAQ Box

Will a traffic impact study be required and if so what is the process?

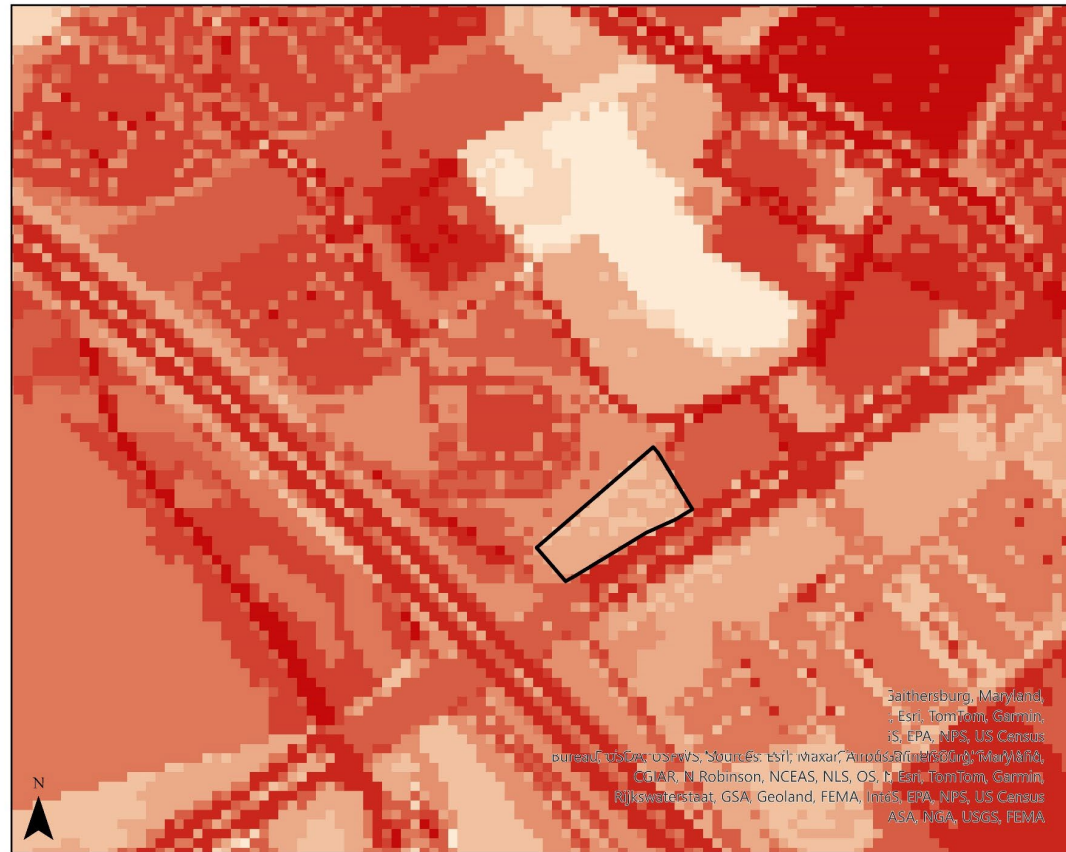
How do I apply for a permit?

What type of approval

Example of Localized Flood Risk: City of San Luis Obispo

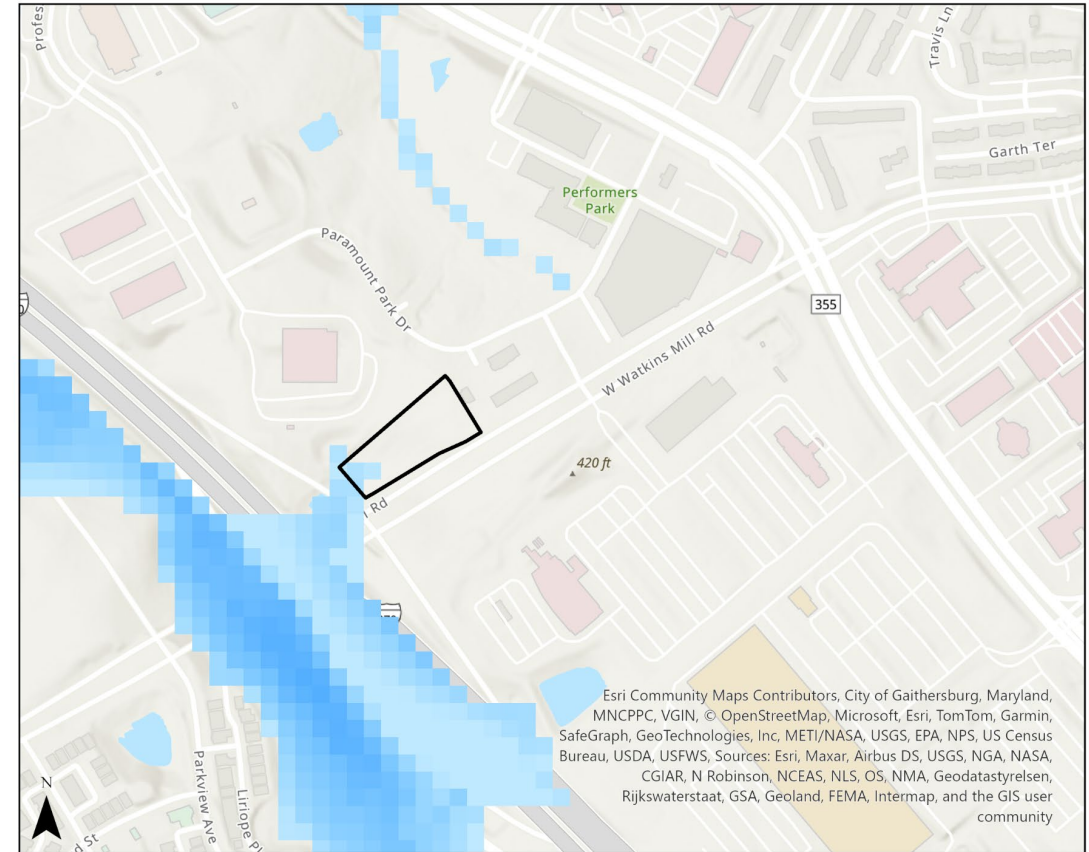


Example of Localization (Climate Solutions Intl.)



PoliceStation_example
 PoliceStation_examp
 Urban Heat Island +
 Climate Change 2100 (C)
 13.3327
 7.33272

0 0.04 0.09 0.18 Miles



PoliceStation_example
 PoliceStation_examp
 Moco GFA 2100 500yr
 24hr depth
 125.5
 0

0 0.05 0.1 0.2 Miles

Why Disclose?

- Don't let fear of public reaction prevent disclosure
 - Data is already out there! (Riskfactor.com)
 - It's designed for residential (30-year forecast)
 - It's not the right data for Cities/Counties
- Cities and Counties need to show they know
 - With better data for their purposes
 - Incorporated into their planning and budgeting process

Example from Riskfactor.com for Residential Risk

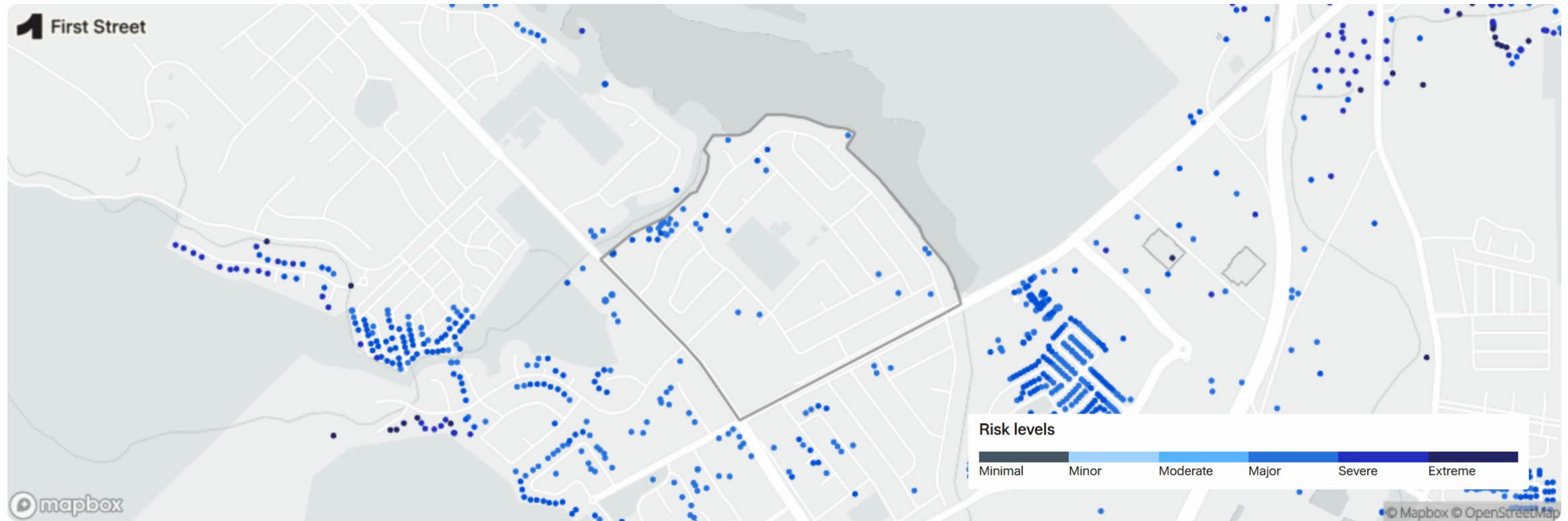
[Flood Factor](#)

[Fire Factor](#)

[Air Factor](#)

[Heat Factor](#)

Madonna Flood Map



Community Impact from Flooding in Madonna

Find the Flood Risk for Any Property

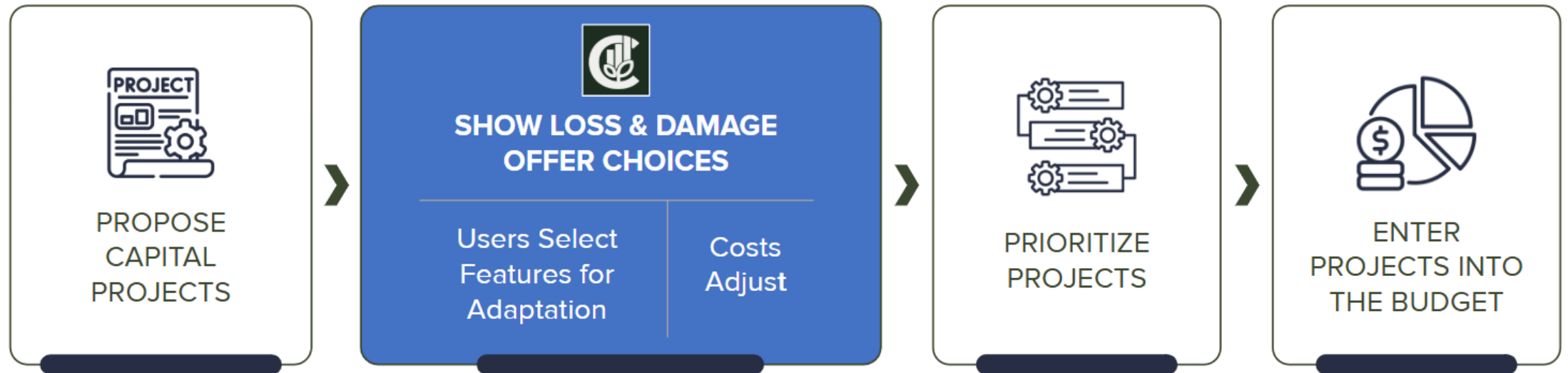
In addition to property damage, flooding can cut off access to utilities, emergency services, transportation,

About Monetizing Climate Risk

- The Cost of Doing Nothing (it's a Forecast)
 - A business-as-usual baseline
 - It is a forecast of loss and damage
 - Adaptation brings forecasts of avoided loss and damage
- The Key is to Integrate these Measures
 - in Capital Plans and Budgets
 - In Financial plans

Example: Capital Budgets

- Climate Solutions International's Approach
 - Integrate with existing capital budgeting process



climatesolutionsintl.com

Example of Monetization: Climate Solutions Intl. Software

REVIEW SITE CLIMATE HAZARDS

WE'VE IDENTIFIED THE FOLLOWING POSSIBLE CLIMATE RISKS TO YOUR CURRENT SELECTED SITE. CHOOSE WHETHER TO CONTINUE WITH THIS SITE AND EXPLORE MITIGATION OPTIONS, OR CHANGE THE LOCATION FOR THIS SUBPROJECT.

FLOOD URBAN HEAT WIND

CURRENT SITE **SITE NAME**

Site Details

Expected Lifespan	20 Years
Site Acquisition Costs	\$1.5M
Construction Cost	\$22.2M
Lifetime Operation Cost	\$10M

ACTIVE RISKS

Flooding	Moderate Risk
Risk During Lifetime	15%
Flood Depth	2 ft
Estimated Potential Loses ⓘ	\$5.8M 21%
Urban Heat	Extreme Risk
Expected Temperature Rise	4 °C
Likelihood of 3+ Day Heatwaves	22%
Estimated Potential Loses ⓘ	\$10.2M 35%
Wind	Minor Risk

Flood Depth: 0 ft, 1 ft, 2 ft, 3 ft, 4 ft, 5 ft+

CURRENT DAY +25 YEARS +50 YEARS +75 YEARS +100 YEARS

Example of Monetization: Climate Solutions Intl. Software

FLOOD RISK MITIGATION



A selection interface for flood risk mitigation components. It features a search icon, filter icons, and a list of components, each with an 'ADD' button and a cost indicator:

- BASE ELEVATION INCREASE**: \$ icon, 2 checkmarks, ADD button.
- FLOODWALL**: \$ icon, 2 checkmarks, ADD button.
- RETENTION BASIN**: \$\$ icon, 2 checkmarks, ADD button.
- RESISTANT MATERIALS**: \$ icon, 1 checkmark, ADD button.
- UPSTREAM MANAGEMENT**: \$\$\$ icon, 3 checkmarks, ADD button.

CAPITAL COST	---	ANNUAL COST	---
MODIFIED POTENTIAL LOSS	\$5.8M 21%	RESILIENCE DIVIDEND	0

Conventional builds are what you would traditionally use without consideration of climate resiliency.

Start adding components to create your build.

Example of Monetization: Climate Solutions Intl. Software

FLOOD RISK MITIGATION



THANK YOU!

JAN WHITTINGTON

*Professor, U of Washington
CEO, Climate Solutions Intl.*



SESSION FOUR

Climate Change and Natural
Hazard Risk Assessment and
Disclosures

BRIAN MCCARTAN

Senior Fellow
Ceres, Inc.



Important Disclosures

- The comments, views, and opinions expressed in the presentation are those of the speaker. The content presented is intended for informational purposes only. Neither Schwab Asset Management™ nor Charles Schwab & Co., Inc. (Schwab) endorse nor can make a representation as to the accuracy, timeliness or completeness of the information presented.
- Schwab Asset Management™ is the dba name for Charles Schwab Investment Management, Inc. Schwab Asset Management and Schwab are separate but affiliated companies and subsidiaries of The Charles Schwab Corporation.

Benefits of Strong Natural Hazard Risk Disclosure



Reveals good governance if you have a climate risk strategy



Provides investor confidence and trust in management



Allows the Issuer to shape the “story”, not the headlines



May reduce market price volatility after an adverse event



May improve investor demand if debt is issued to finance recovery efforts

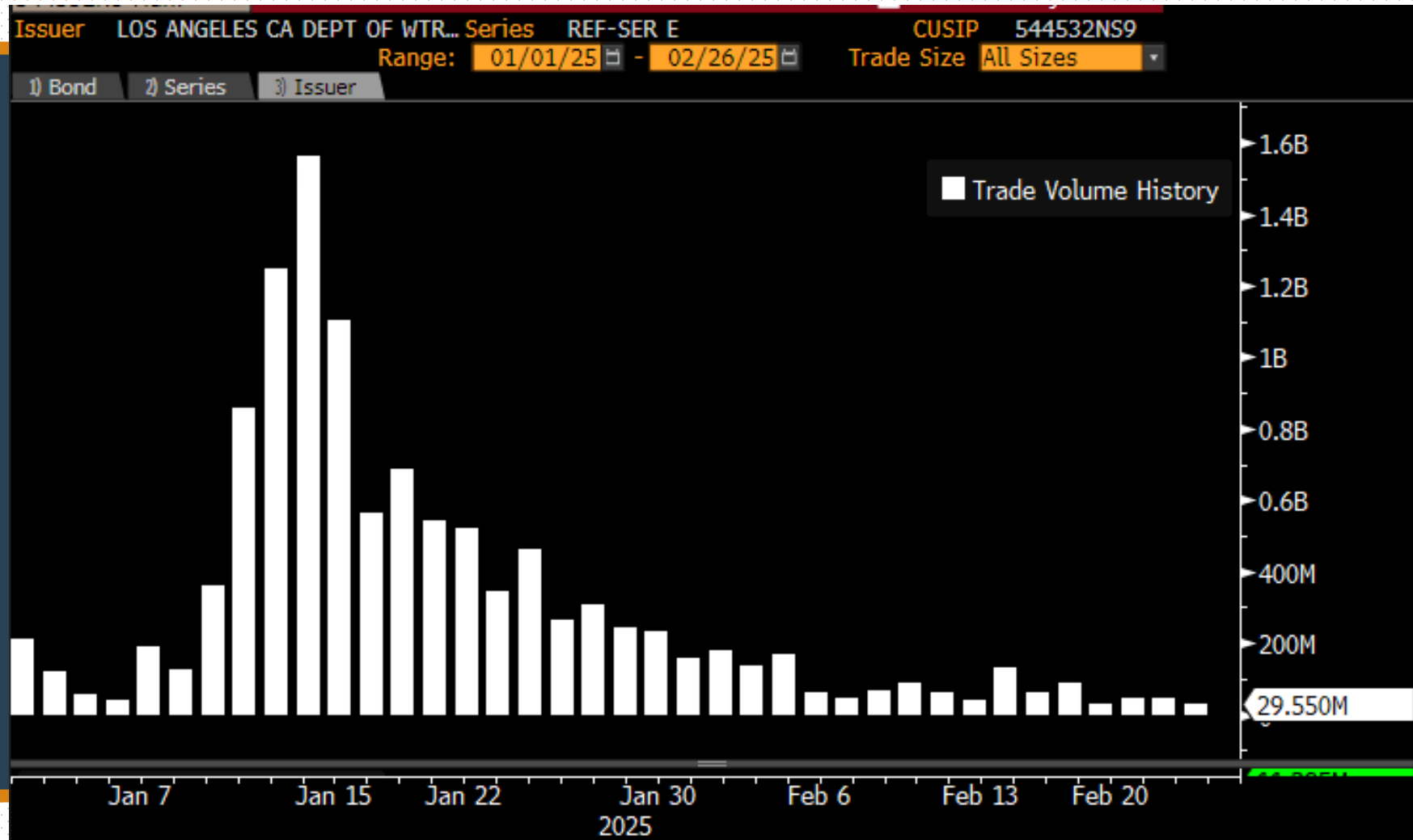
Good Disclosure Includes Discussion of:

- Hazardous risk exposure level of severity
- Risk mitigation strategy and actions taken
- State mandates
- Insurance coverage
- Capital mitigation plans, projected cost, and financing plan

What Does An Investor Look at When a Disaster Hits?

- Size of area impacted relative to service area or tax base
- Disaster response efforts
- Eligibility for state and federal aid
- Impact to revenues and expenses
- Issuer's financial flexibility
 - Liquidity and financial reserves
 - Ability to raise taxes or rates
- Estimate of financial liability
- Market and rating agencies' response

Los Angeles Department of Water & Power, Power System: Impact on Trade Volume from the January 2025 Palisades Fire



Source: Bloomberg

Los Angeles Department of Water & Power, Power Bonds: Impact on Yields from the January 2025 Palisades Fire



Source: Bloomberg

CUSIP 544532NS9: Issued at a 2.84% yield in November 2024, 7/1/2034 maturity, \$59.7 million outstanding

CLASSIFICATION: Public | DISTRIBUTION: Institutional Use

What Drove Market Volatility?

- Fast-moving, uncontrollable nature of the wildfires
- Headlines – mass evacuations, images of Los Angeles on fire, loss estimates
- Inverse condemnation concerns combined with lack of information on LADWP liability for the Palisades Fire
- Selling by investors with low risk tolerance
- Rating agency negative rating actions
- Lack of investor outreach

What Calmed the Markets?

- Moody's January 17 report stating LADWP's power equipment did not appear to be the ignition source for the Palisades Fire
- Moody's commentary that LADWP's Water System operated as designed
- Buying by investors with higher risk tolerance
- Containment of the fires, reduced headline news
- LADWP reports of water and power restored to the burned areas, rapid Phase I (hazardous waste) clean up

QUESTIONS?



DANIEL DEATON
Partner
Nixon Peabody LLP



RENEE DOUGHERTY, CFA
*Director, Municipal
Research*
Charles Schwab Asset
Management



BRIAN MCCARTAN
Senior Fellow
Ceres, Inc.



JAN WHITTINGTON, PhD
Professor
University of
Washington, Seattle



THANK YOU

Please complete the seminar evaluation and leave it on your table.

UPCOMING EVENTS

**Land-secured Financing:
Fundamentals and Evolving Practices**

September 10–11, 2025
Pleasanton, CA

For more information, visit:
treasurer.ca.gov/CDIAC/seminars