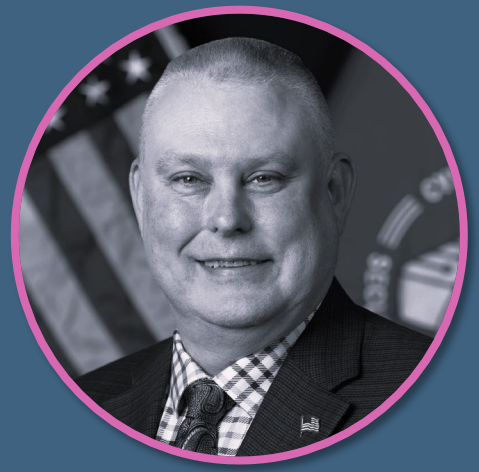
# SESSION THREE

## 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)

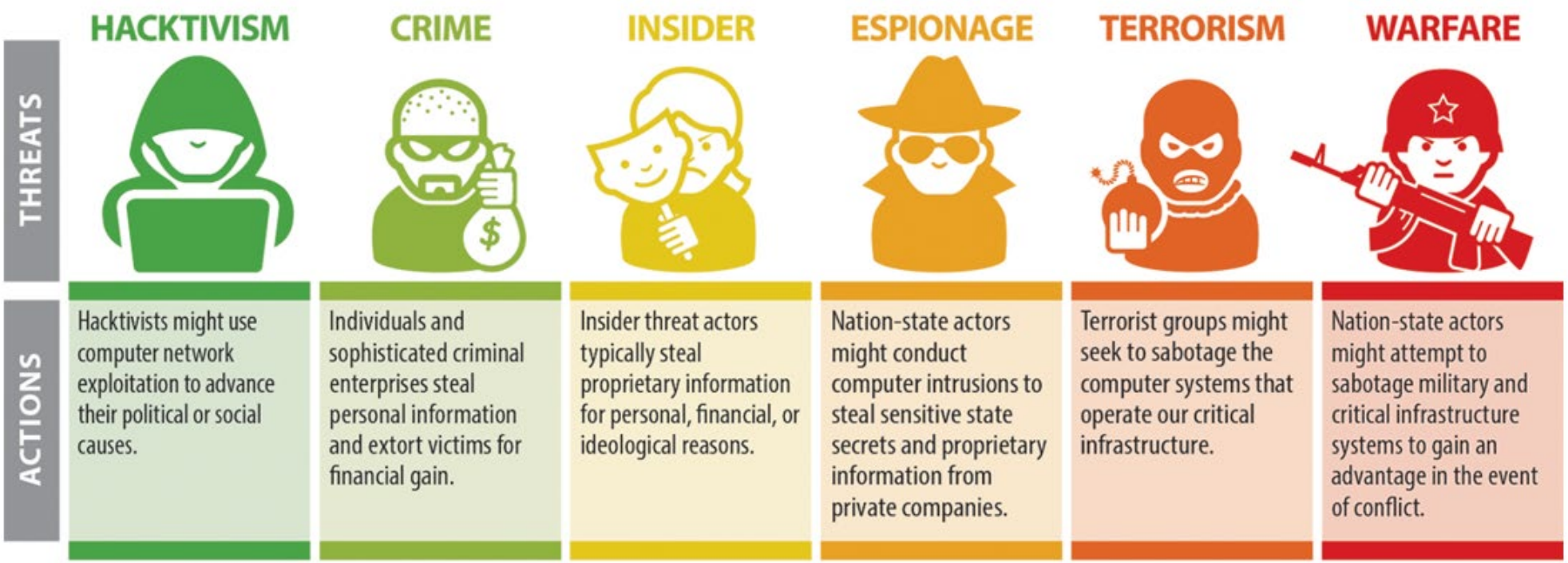
# SEC 2020 Statement on Importance of Disclosure

- 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

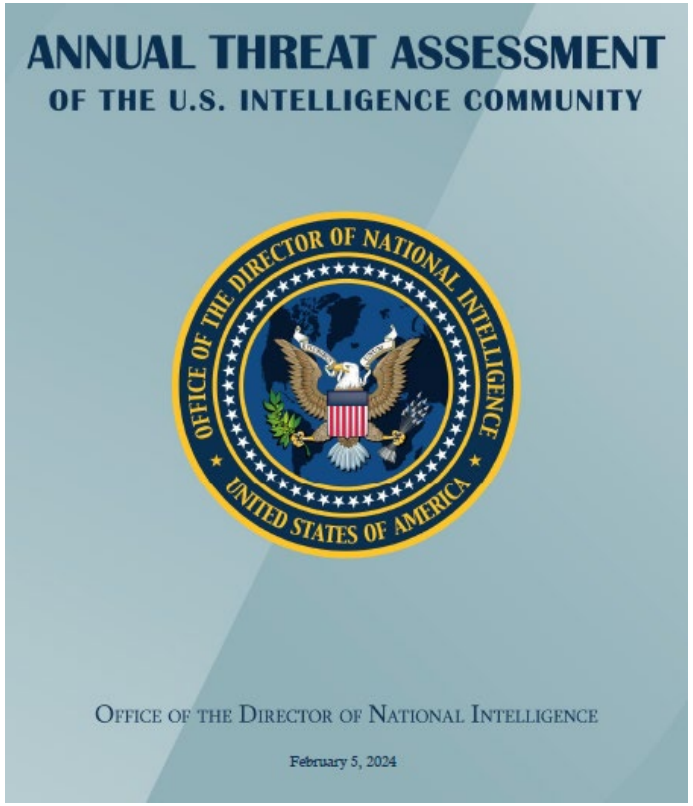


# ODNI Annual Threat Assessment

### 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."




https://www.odni.gov/index.php/newsroom/reports-publications/reports-publications-2024/3787-2024-annual-threat-assessment-of-the-u-s-intelligence-community

# 2024 ODNI Annual Threat Assessment

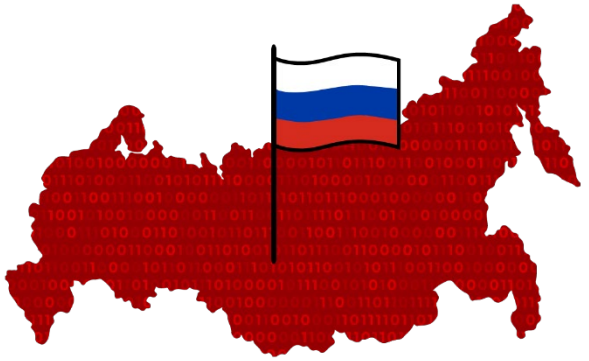
## Foreign Threat Actors

### 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."

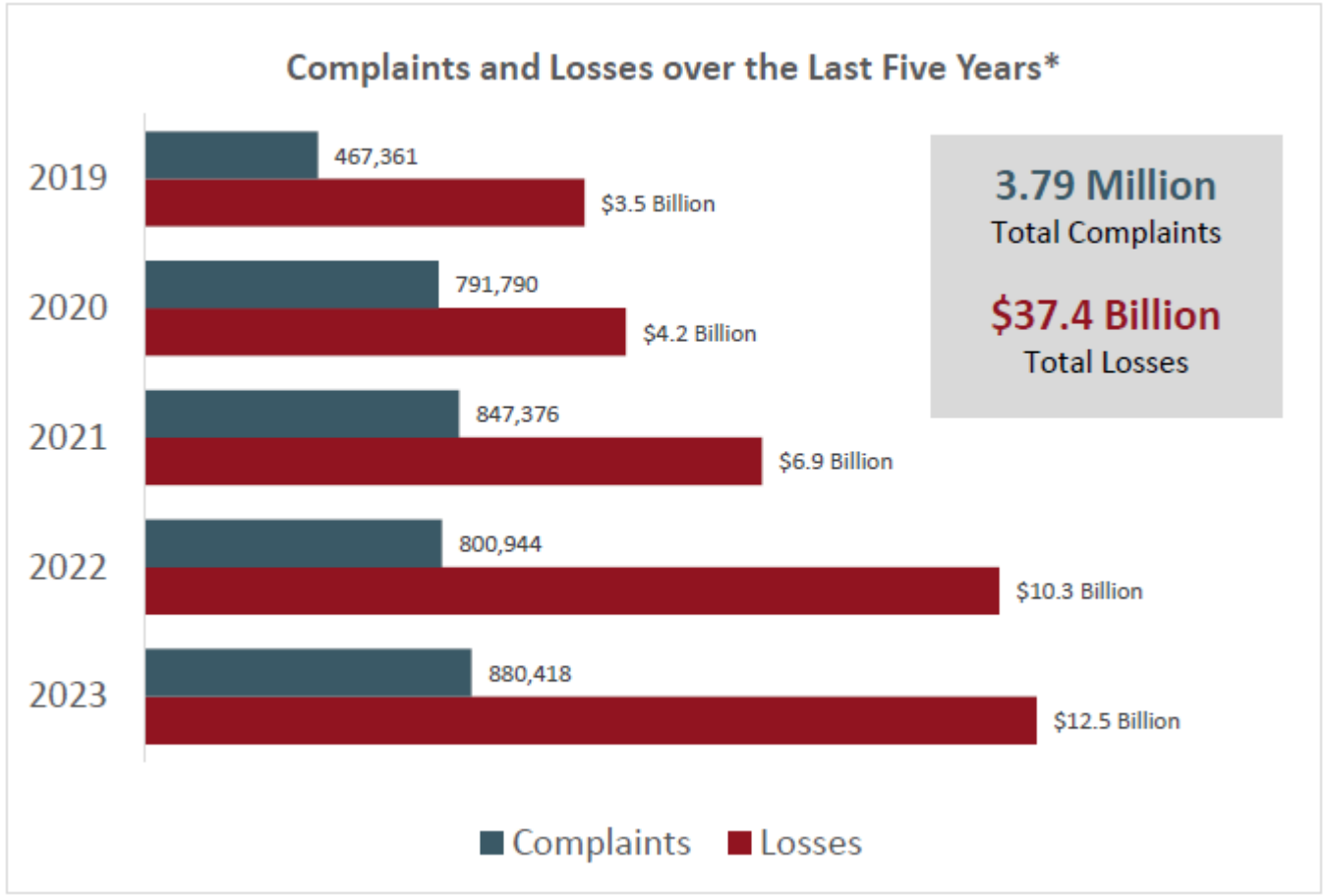


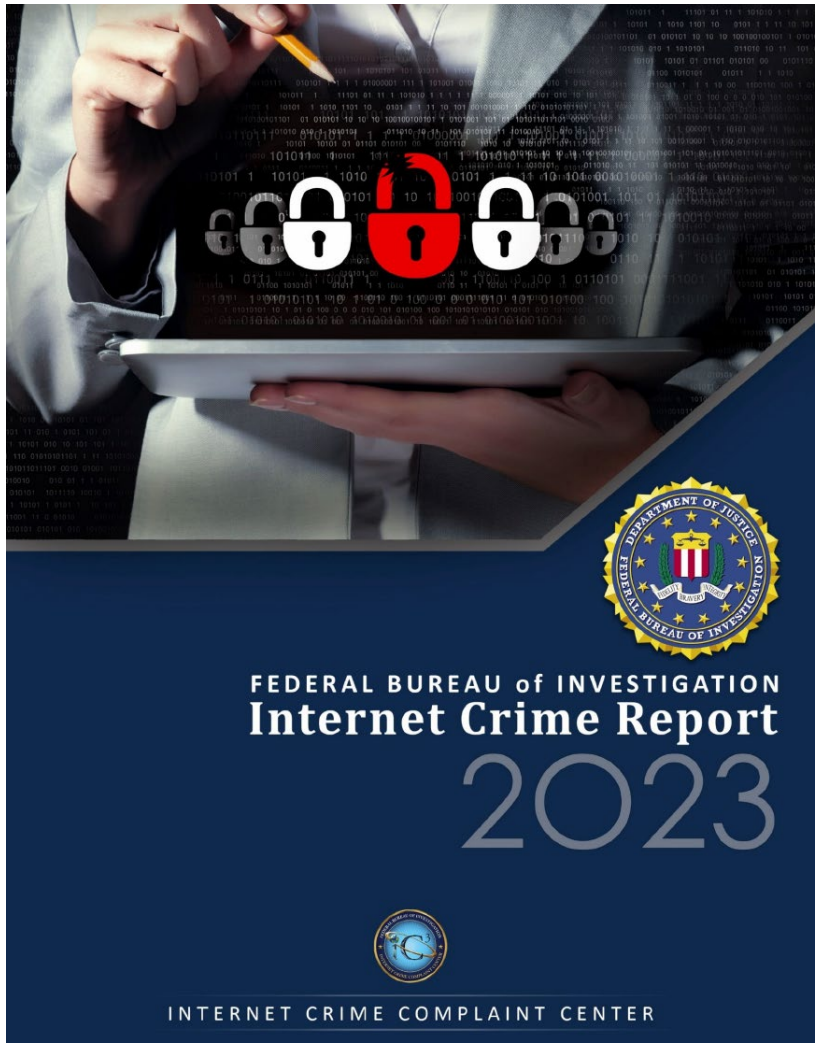
### RUSSIA

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

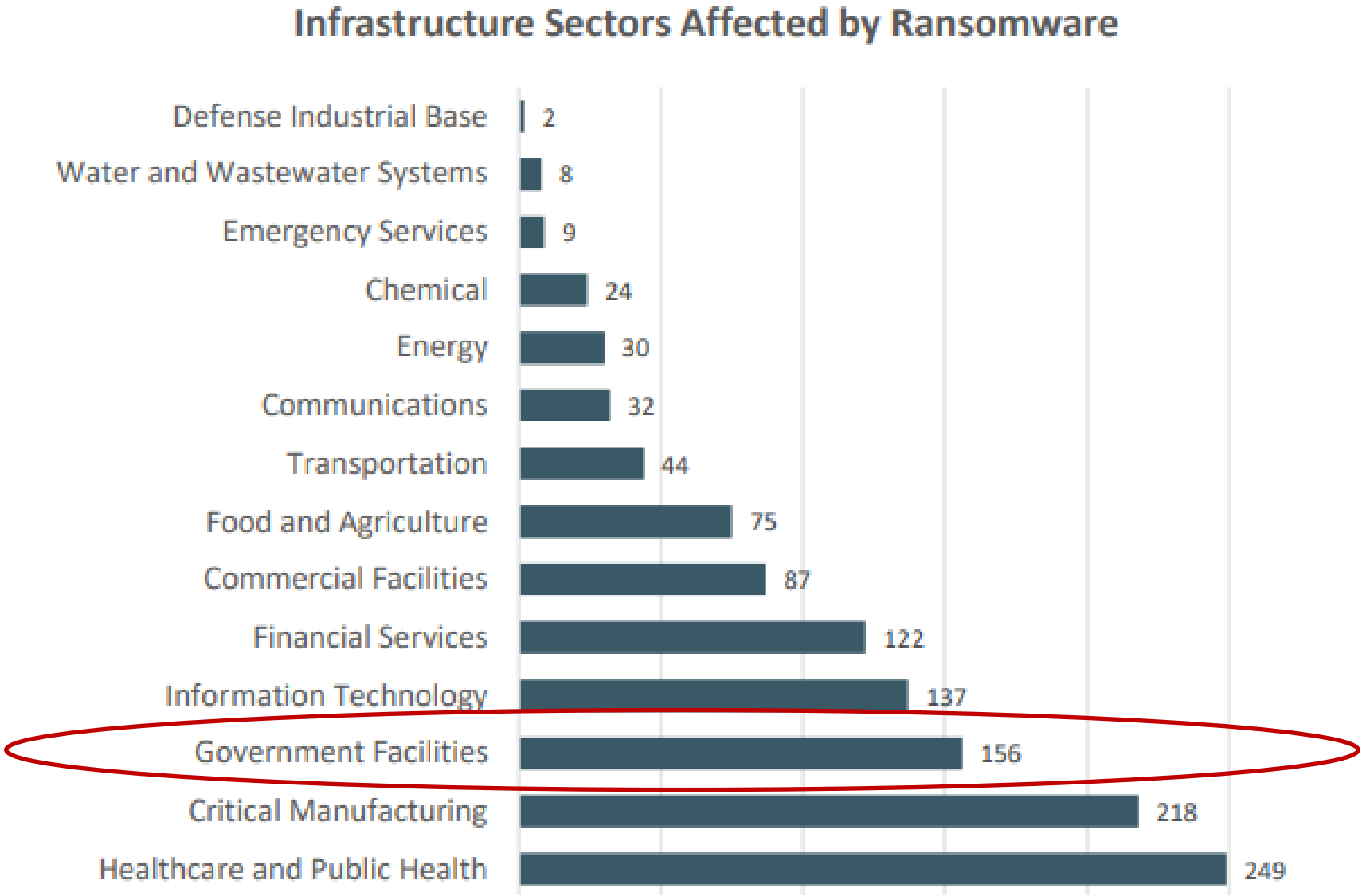
https://www.odni.gov/index.php/newsroom/reports-publications/reports-publications-2024/3787-2024-annual-threat-assessment-of-the-u-s-intelligence-community

# IC3 Internet Crime Report 2023

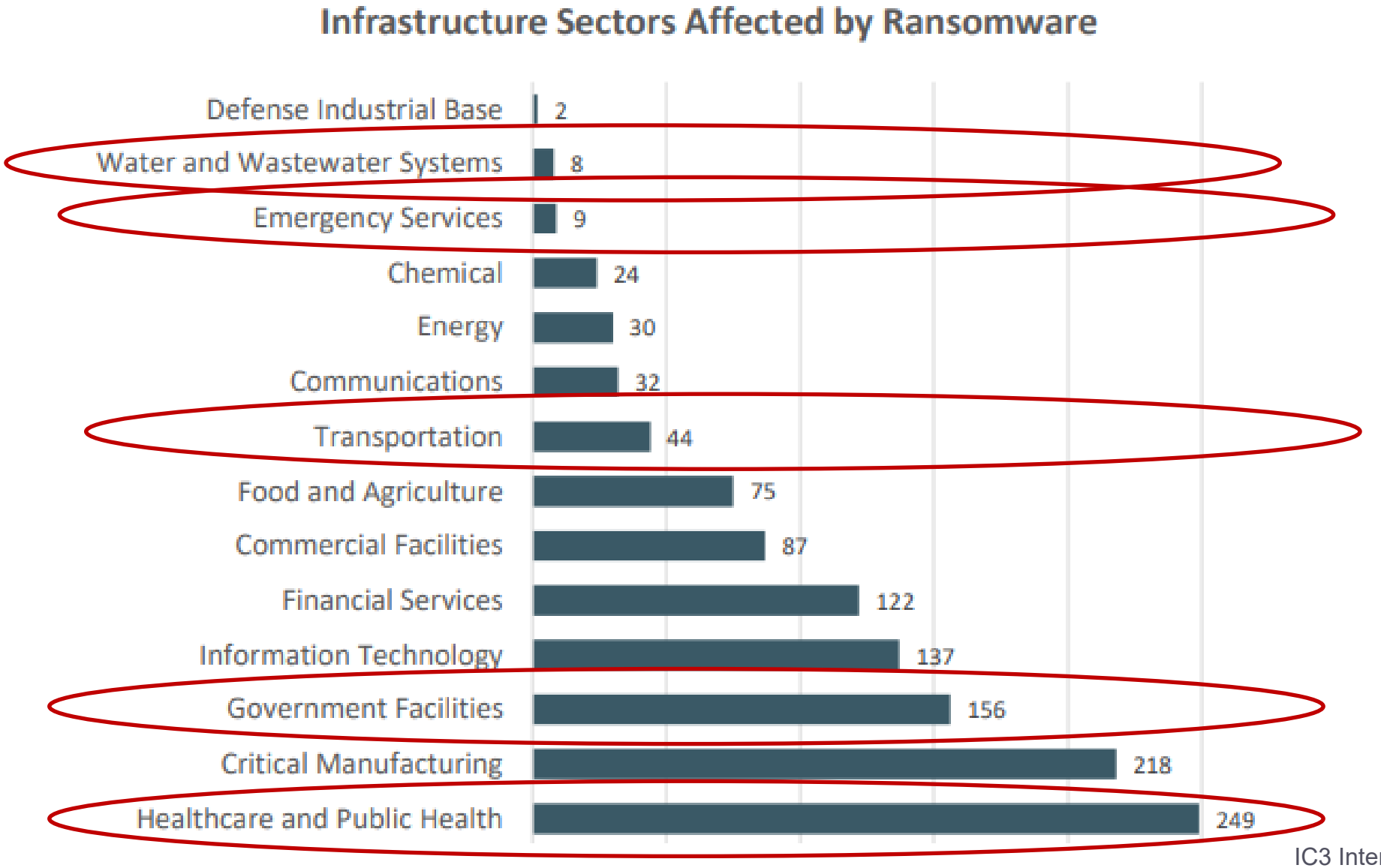


# Sectors Affected by Ransomware



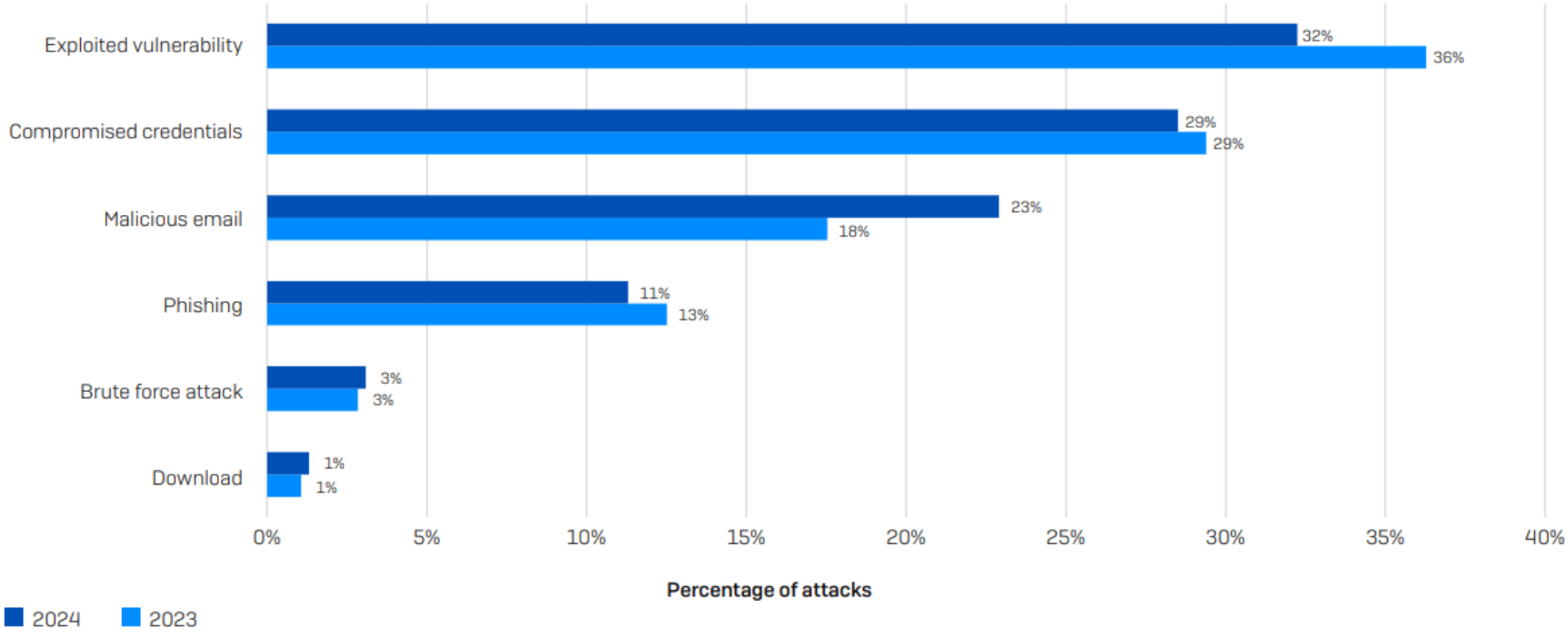
# Sectors Affected by Ransomware



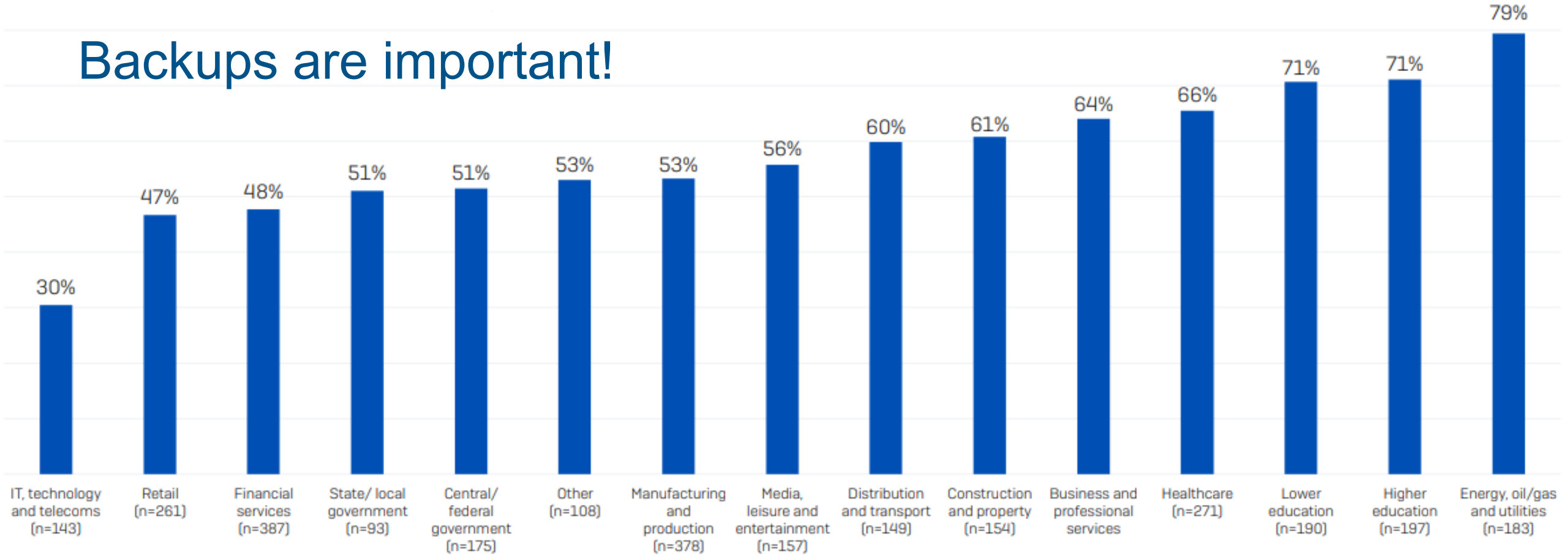



IC3 Internet Crime Report 2023

# 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

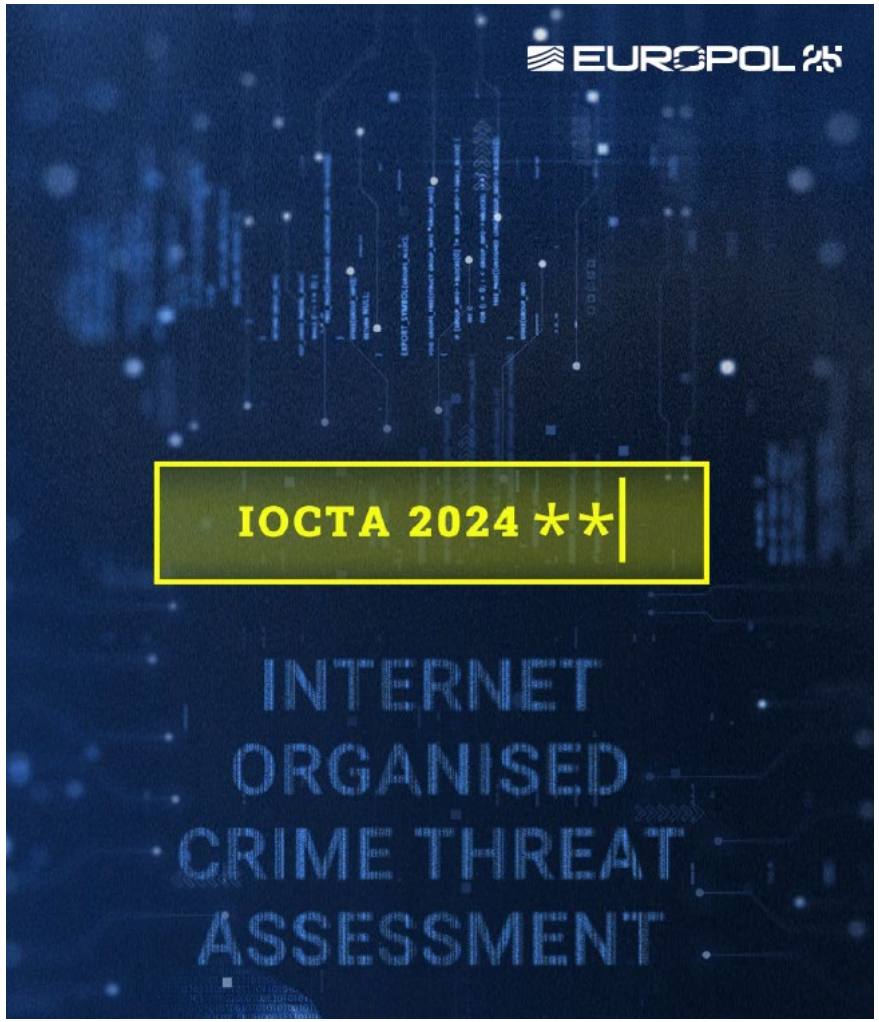
# Recovery Costs

| 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.




https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024

# 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.

# 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.

# 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: $$$$ IMPACT: HIGH COMPLEXITY: MEDIUM<br>TACTIC, TECHNIQUE, AND PROCEDURE (TTP) OR RISK ADDRESSED:<br>Hardware Additions (T1200)<br>Exploit Public-Facing Application (T0819, ICS T0819)<br>Internet-accessible device (ICS T0883)<br>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.<br>FREE SERVICES AND REFERENCES: Cyber Hygiene Services, "Stuff Off Search" Guide or email vulnerability@cisa.DHS.gov | DATE:<br>IMPLEMENTED<br>IN PROGRESS<br>SCOPED<br>NOT STARTED | DATE:<br>IMPLEMENTED<br>IN PROGRESS<br>SCOPED<br>NOT STARTED | |

| 1.B Organizational Cybersecurity Leadership — ID.GV-1, ID.GV-2 | CURRENT ASSESSMENT | YEAR 1 ASSESSMENT | NOTES |
|---|---|---|---|
| COST: $$$$ IMPACT: HIGH COMPLEXITY: LOW<br>TTP OR RISK ADDRESSED:<br>Lack of sufficient cybersecurity accountability, investment, or effectiveness.<br>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:<br>IMPLEMENTED<br>IN PROGRESS<br>SCOPED<br>NOT STARTED | DATE:<br>IMPLEMENTED<br>IN PROGRESS<br>SCOPED<br>NOT STARTED | |

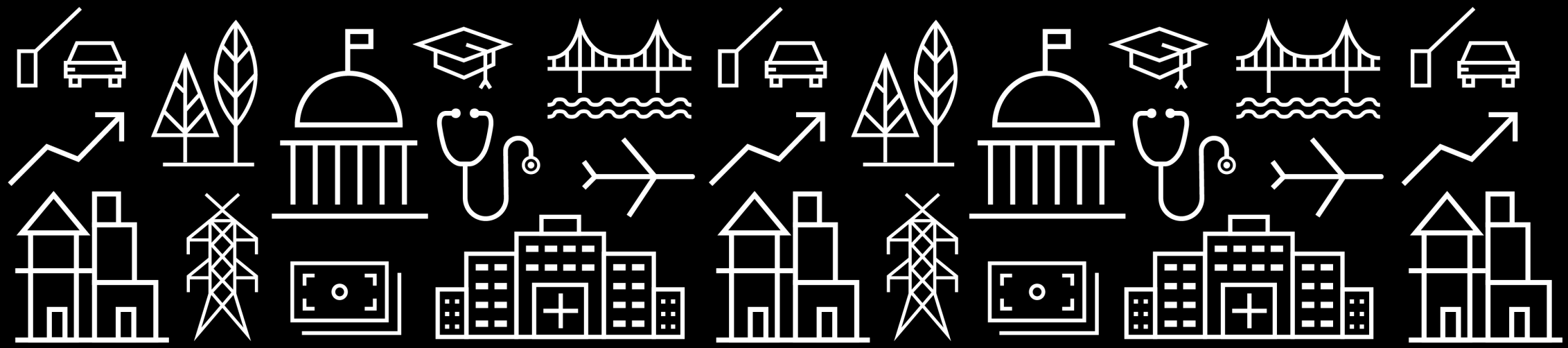
| 1.C OT Cybersecurity Leadership — ID.GV-1, ID.GV-2 | CURRENT ASSESSMENT | YEAR 1 ASSESSMENT | NOTES |
|---|---|---|---|
| COST: $$$$ IMPACT: HIGH COMPLEXITY: LOW<br>TTP OR RISK ADDRESSED:<br>Lack of accountability, investment, or effectiveness of OT cybersecurity program.<br>RECOMMENDED ACTION: A named 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:<br>IMPLEMENTED<br>IN PROGRESS<br>SCOPED<br>NOT STARTED | DATE:<br>IMPLEMENTED<br>IN PROGRESS<br>SCOPED<br>NOT STARTED | |

| 1.D Improving IT and OT Cybersecurity Relationships — ID.GV-2, PR.AT-5 | CURRENT ASSESSMENT | YEAR 1 ASSESSMENT | NOTES |
|---|---|---|---|
| COST: $$$$ IMPACT: MEDIUM COMPLEXITY: LOW<br>TTP OR RISK ADDRESSED:<br>Poor working relationships and a lack of mutual understanding between IT and OT cybersecurity can often result in increased risk for OT cybersecurity.<br>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:<br>IMPLEMENTED<br>IN PROGRESS<br>SCOPED<br>NOT STARTED | DATE:<br>IMPLEMENTED<br>IN PROGRESS<br>SCOPED<br>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

S&P Global
Ratings

Copyright © 2020 by S&P Global.
All rights reserved.

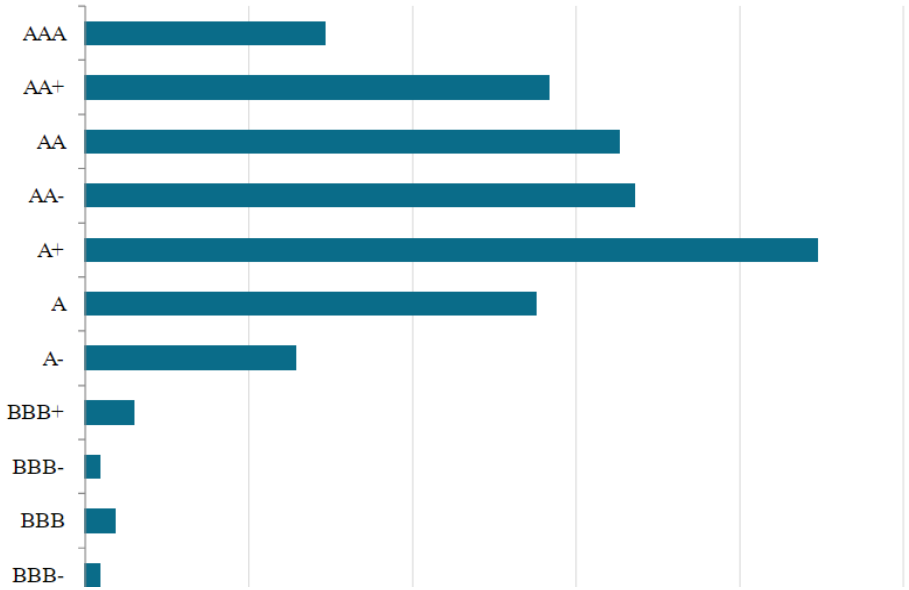
# Agenda

- 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

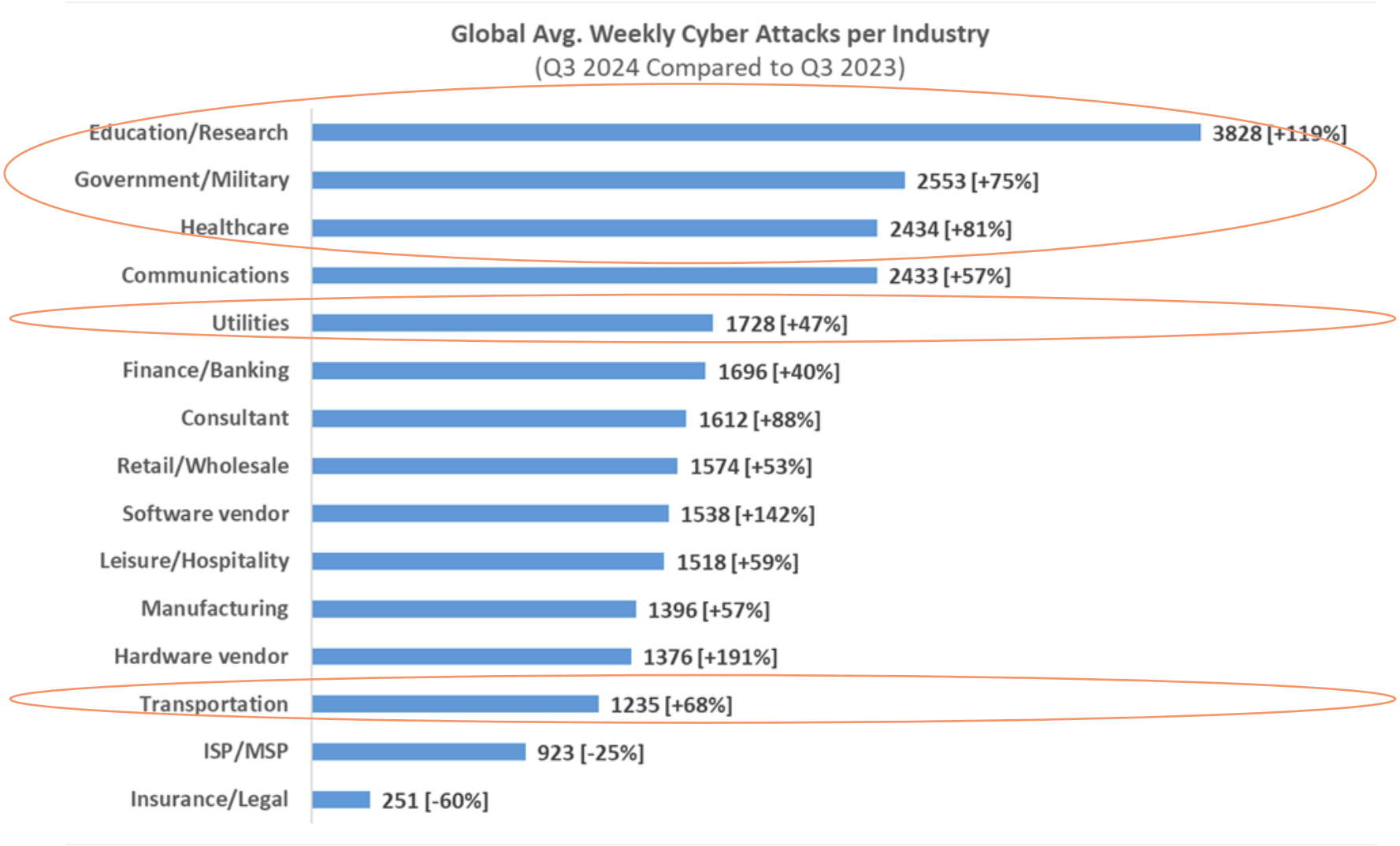
**"This is the new frontier of cybersecurity—an arms race where we're not just battling hackers, but also battling AI-powered machines that can think, adapt, and innovate faster than ever before." Forbes, October 2024**

**"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




*Source: Check Point Research*
*A Closer Look at Q3 2024: 75% Surge in Cyber Attacks Worldwide, published Oct. 18, 2024*

# 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

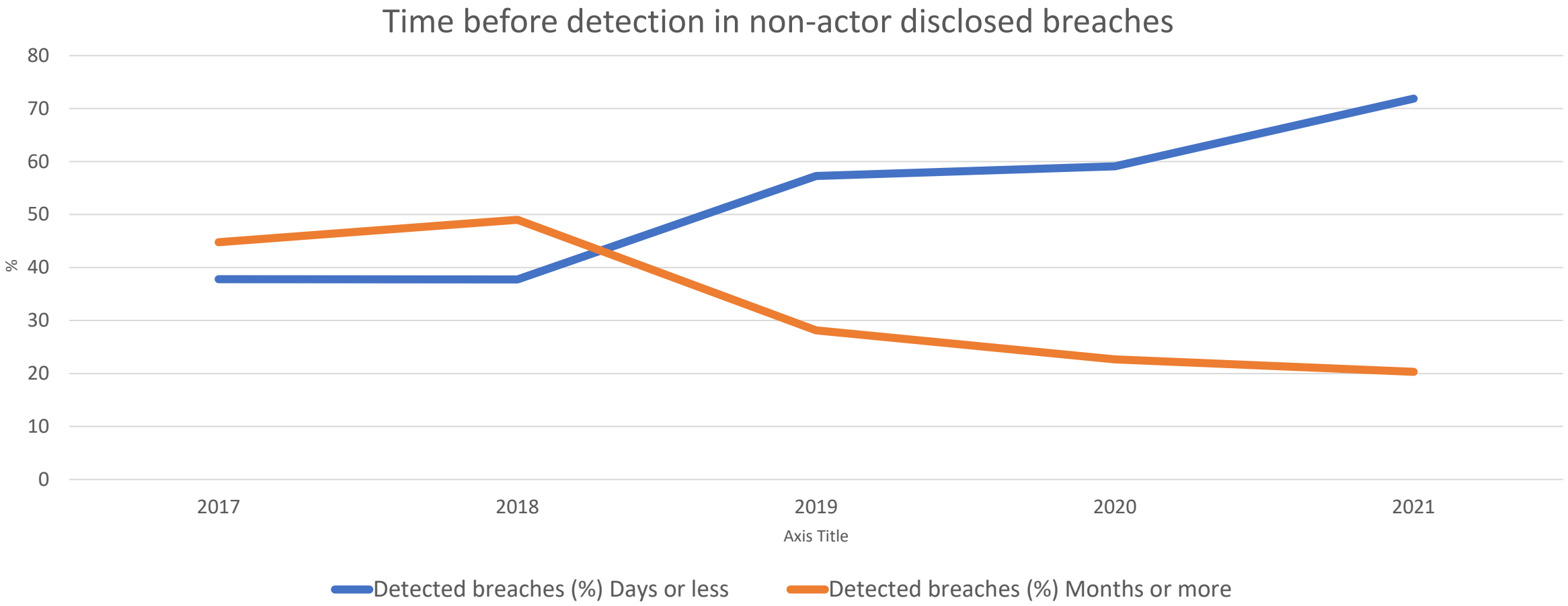
- Reduce management bandwidth
- Multiple external and internal parties involved
- Enhance cyber security framework
- Expand employee training and awareness to cover new risk areas

### 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.

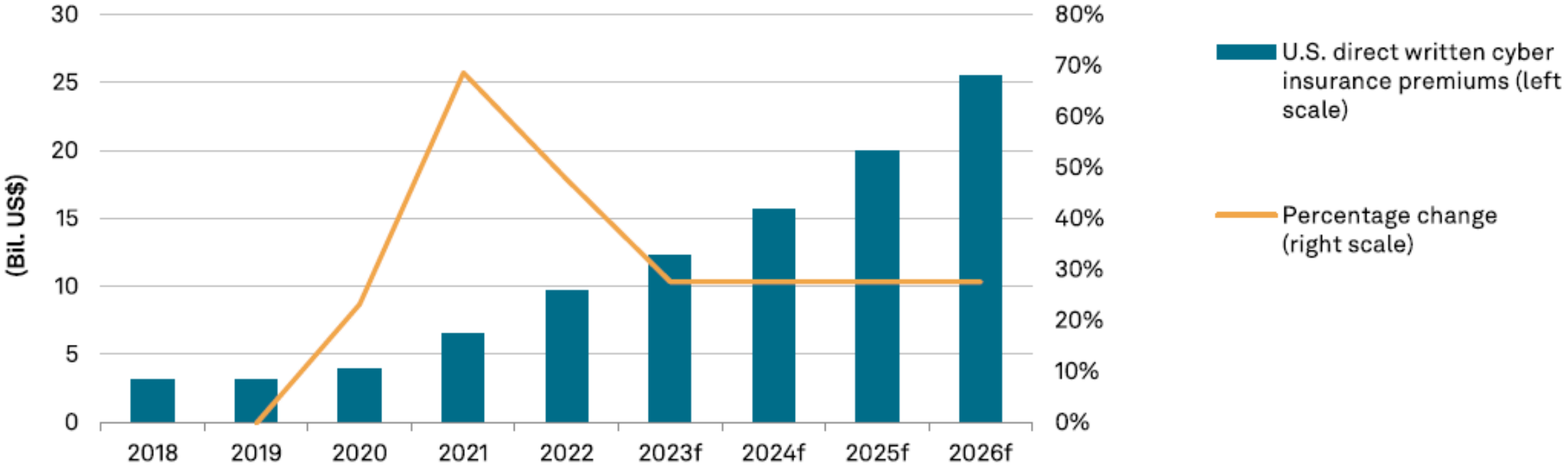
# S&P Global Ratings | Cyber Attack Detection is Accelerating




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:

S&P Global
Ratings

# 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

0%

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

0%

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

0%

No, not to my knowledge

0%

Start the presentation to see live content. For screen share software, share the entire screen. Get help at **pollev.com/app**

# 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

0%

No; we have established practices

0%

No; we have an ad hoc approach to cybersecurity

0%

No specific instructions relating to cybersecurity have been communicated to me

0%

Start the presentation to see live content. For screen share software, share the entire screen. Get help at **pollev.com/app**

# 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

# 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.



Copyright 2025 by Financial Accounting Foundation, Norwalk CT. For non-commercial, educational/academic purposes only.

# 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

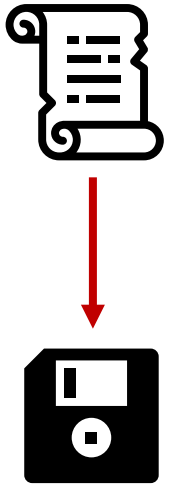
Copyright 2025 by Financial Accounting Foundation, Norwalk CT. For non-commercial, educational/academic purposes only.

# Background and Project Information

# GASB and Electronic Financial Reporting

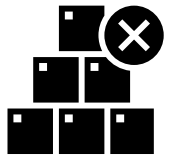
## Early days

1. Focused on digitizing paper



## First Taxonomy Attempts

1. XBRL pilots mid 2000s



## 2018—2021

1. XBRL US Governmental Working Group (Staff responded via Comment Letters)
2. Florida Legislation and XBRL Implementation
3. FERC XBRL
4. Data Act (grants)

## 2022 Forward

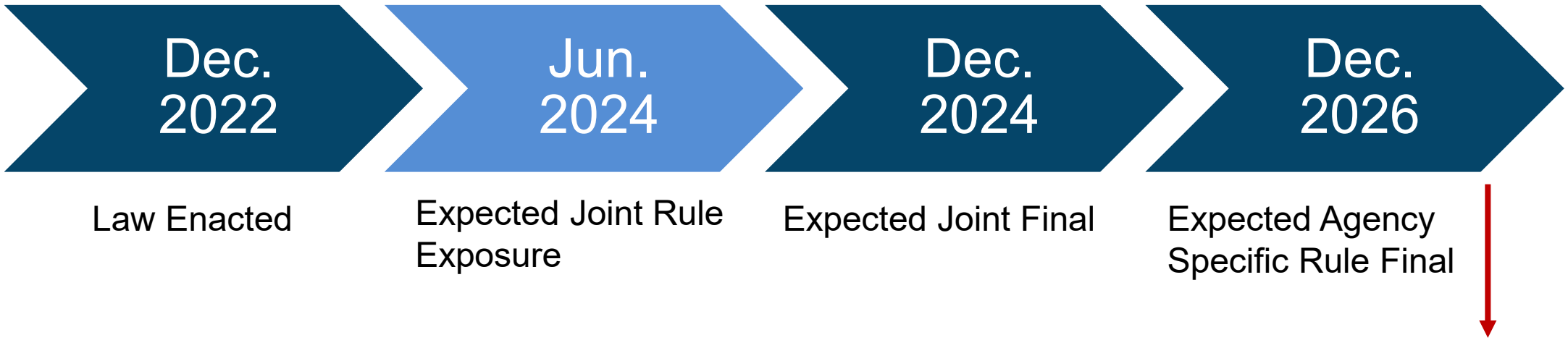
1. Assigned more staff to electronic reporting
2. Ongoing user outreach
3. Ongoing technology research
4. Monitoring FDTA

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



Copyright 2025 by Financial Accounting Foundation, Norwalk CT. For non-commercial, educational/academic purposes only.

# 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.


Copyright 2025 by Financial Accounting Foundation, Norwalk CT. For non-commercial, educational/academic purposes only.

# Joint Rule Proposal

**Identifiers**

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

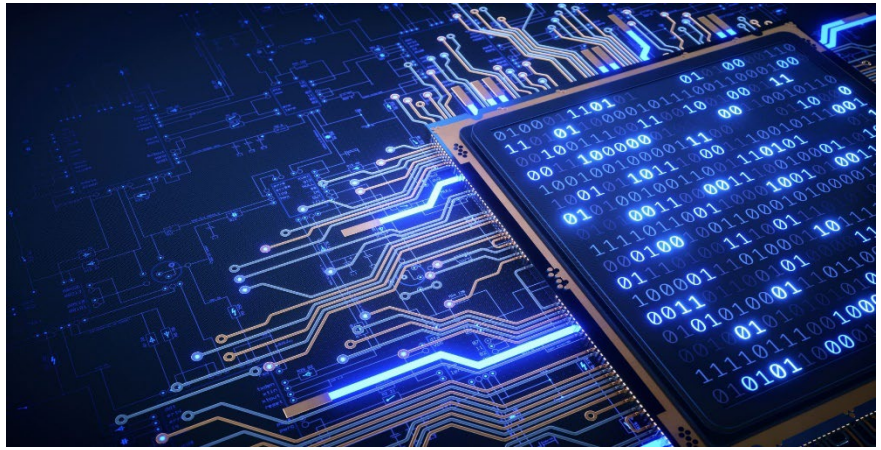
**Technology**

- 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 GOVERNMENTAL ACCOUNTING STANDARDS BOARD



Copyright 2025 by Financial Accounting Foundation, Norwalk CT. For non-commercial, educational/academic purposes only.

# 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

Copyright 2025 by Financial Accounting Foundation, Norwalk CT. For non-commercial, educational/academic purposes only.

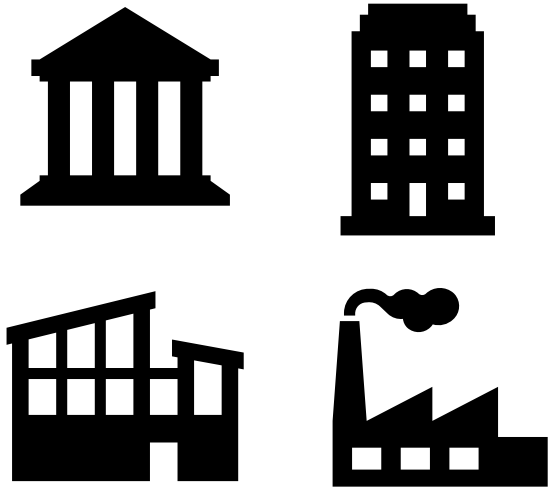
# Industry Concerns—Overview

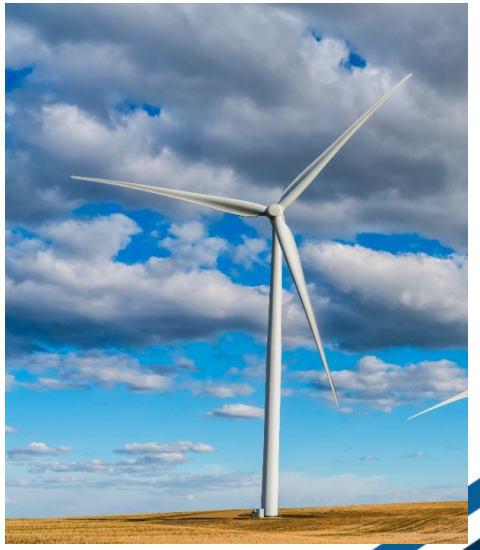
## Structure of Financial Statements

- Different statements for different types of governments

## Line items are different in each industry

- Level of detail is different





GASB GOVERNMENTAL ACCOUNTING STANDARDS BOARD



Copyright 2025 by Financial Accounting Foundation, Norwalk CT. For non-commercial, educational/academic purposes only.

# Taxonomy Development Example—City of ABC

| | General | Debt Service | Capital Projects | General COVID Relief | Other Governmental Funds | Total Governmental Funds |
|---|---|---|---|---|---|---|
| **Assets:** | | | | | | |
| Cash, cash equivalents and investments | $ 206,527 | $ 197,985 | $ 188,610 | $ - | $ 239,659 | $ 832,781 |
| Receivables, net: | | | | | | |
| 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]



Copyright 2025 by Financial Accounting Foundation, Norwalk CT. For non-commercial, educational/academic purposes only.

# GASB's Tentative Approach

Revenues

Charges For Service

Type: Monetary
Period: Duration
Balance: Credit

For Colleges & Universities

Tuition and Fees

For Airport (Port Authority)

Landing Fees

For Fire District

Emergency Medical Service Fees

For Water Utility

Water fees

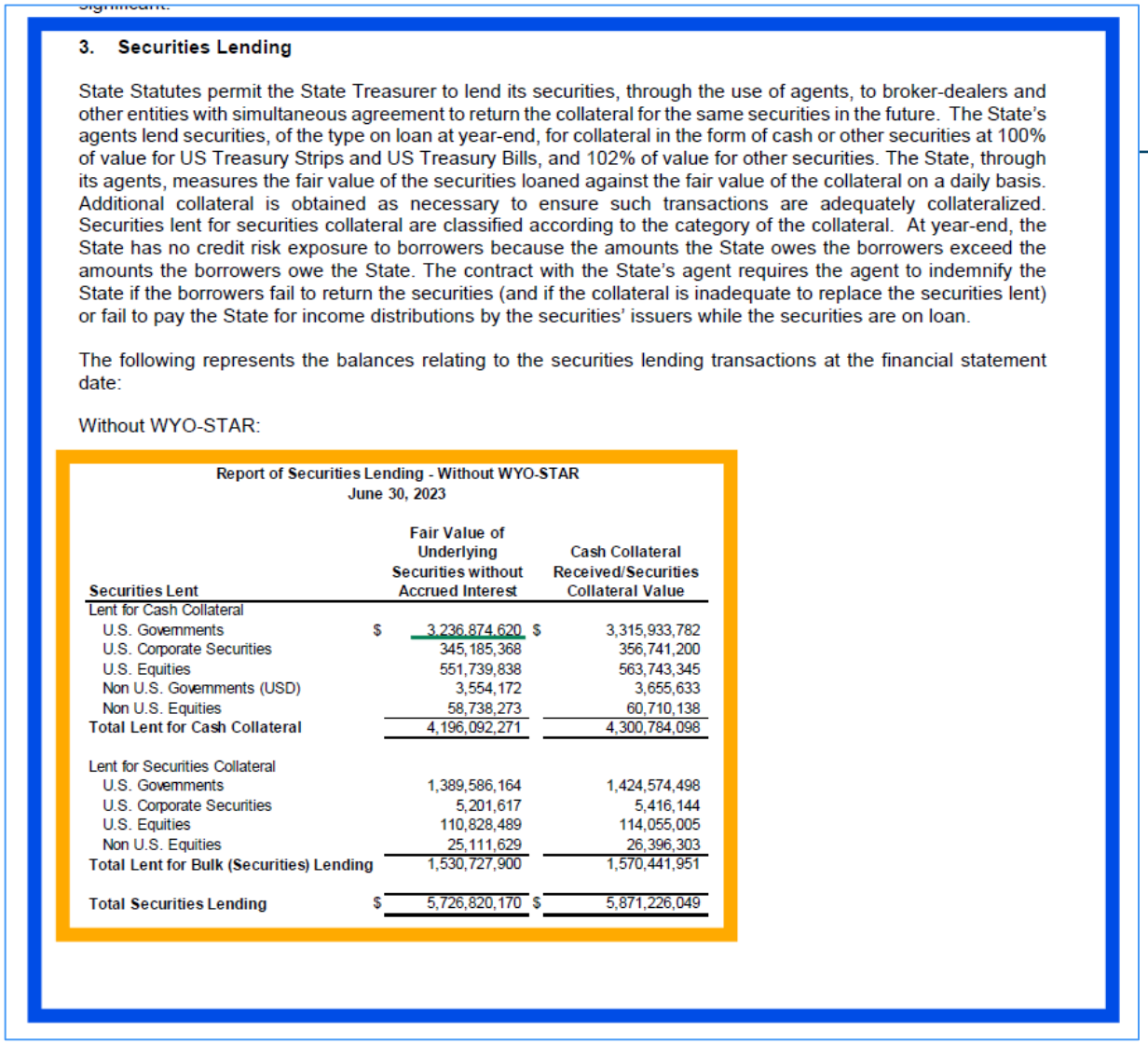
Re-use Water Fees

Codification Reference

GASB Codification (2023-2024)
Section 1800.132

Copyright 2025 by Financial Accounting Foundation, Norwalk CT. For non-commercial, educational/academic purposes only.

# 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:

Report of Securities Lending - Without WYO-STAR
June 30, 2023

| 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



Copyright 2025 by Financial Accounting Foundation, Norwalk CT. For non-commercial, educational/academic purposes only.

# Project Update

## Due Process document

# GASB-GAAP Taxonomy
# Voluntary Digital Financial Reporting Project

Phase I

- Basic Financial Statements
- Required Supplementary Information

Phase II

- Supplementary Information

***Basic Financial Statements:***

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

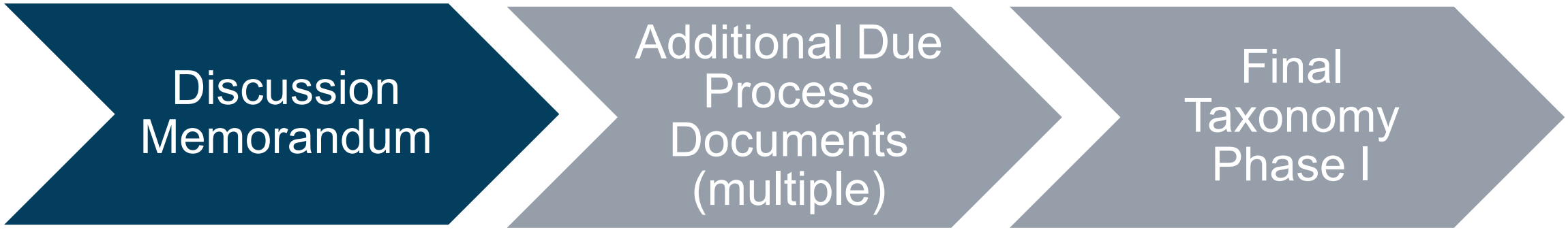
***Required Supplementary Information:***

- Pensions and OPEB Schedules
- Infrastructure Schedule
- Budgetary Schedules



Copyright 2025 by Financial Accounting Foundation, Norwalk CT. For non-commercial, educational/academic purposes only.

# 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***

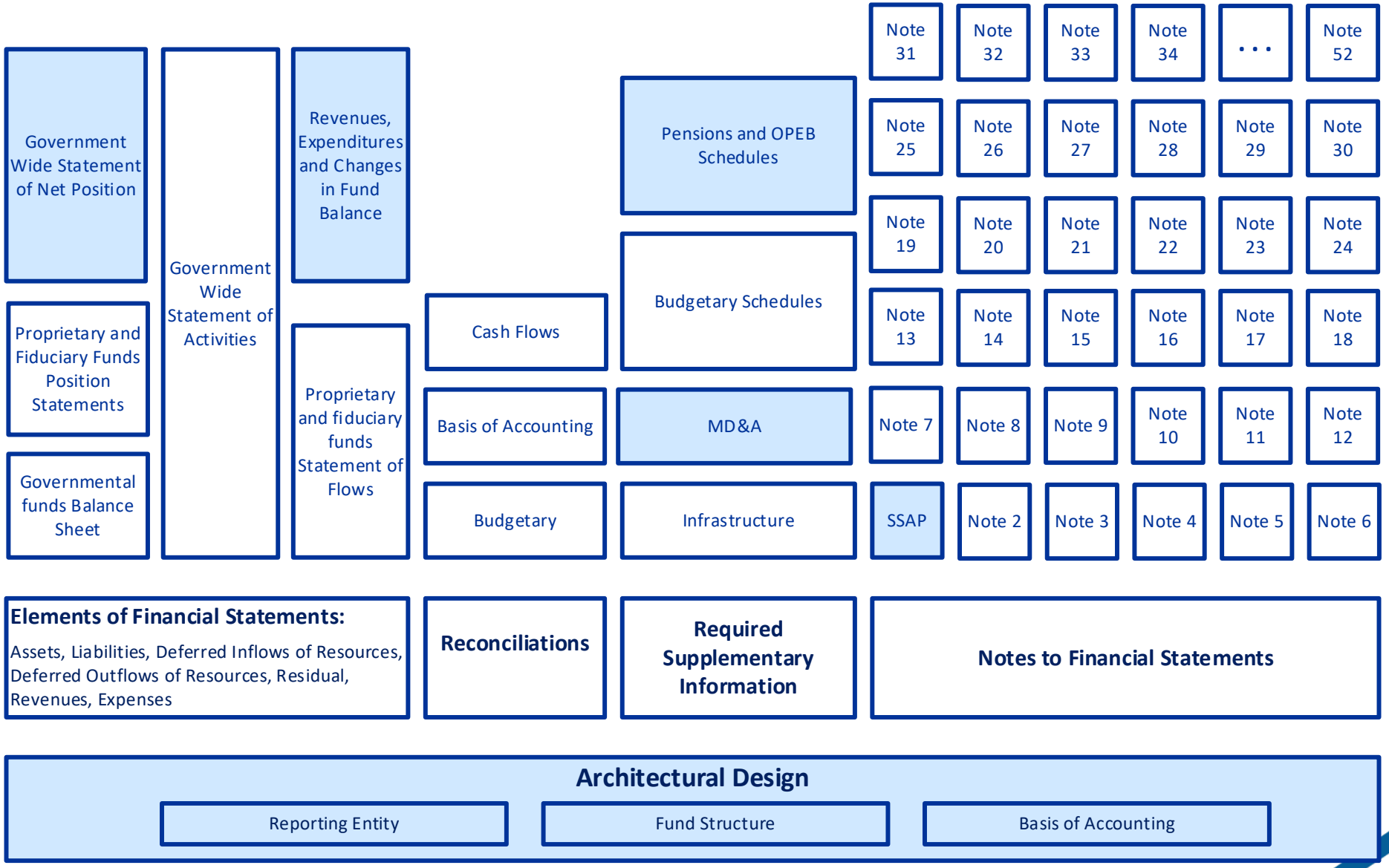
- The architectural design choices made in the design of the GASB-GAAP Taxonomy
- Does NOT include all components of the taxonomy
- Is NOT a final product, its an early discussion document

GASB GOVERNMENTAL ACCOUNTING STANDARDS BOARD



Copyright 2025 by Financial Accounting Foundation, Norwalk CT. For non-commercial, educational/academic purposes only.

# GASB GAAP Taxonomy—Phase I Components



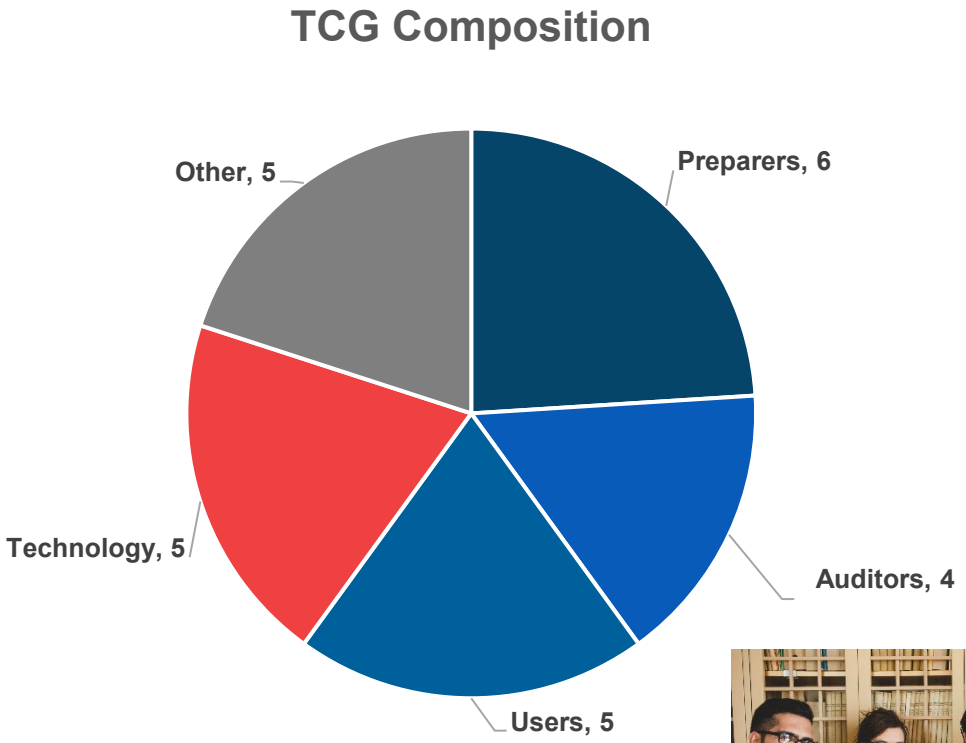

Components scheduled for exposure in December



Copyright 2025 by Financial Accounting Foundation, Norwalk CT. For non-commercial, educational/academic purposes only.

# Taxonomy Consultative Group (TCG)

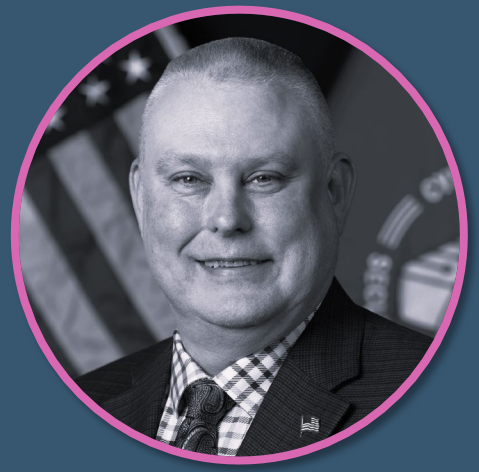
1. Charter and participants are ready
   - We expect 25 members
2. Meetings will begin after March Board meeting
   - Virtual meetings
   - Subgroup strategy
3. Periodic feedback will be solicited
   - Technology
   - Common practice
4. Board meeting with TCG: Q4 2025



Copyright 2025 by Financial Accounting Foundation, Norwalk CT. For non-commercial, educational/academic purposes only.

# 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