

Sarbanes Oxley Compliance Professionals Association (SOXCPA)  
1200 G Street NW Suite 800, Washington DC, 20005-6705 USA  
Tel: 202-449-9750 Web: [www.sarbanes-oxley-association.com](http://www.sarbanes-oxley-association.com)



## *Sarbanes Oxley News, May 2023*

Dear members and friends,

We have the Public Company Accounting Oversight Board's 2022 Annual Report. There are some very interesting goals:



### *Goal One: Modernize Standards*

Effective standards advance audit quality and are foundational to the PCAOB's execution of its mission to protect investors. Not only do our standards provide the requirements auditors must satisfy when conducting their audits, they also serve as the basis for our inspection and enforcement activities.

When the PCAOB was first getting off the ground in 2003, it adopted existing standards that had been set by the auditing profession on what was intended to be an interim basis.

Twenty years later, far too many of those interim standards remain unchanged. The world has changed since 2003. And our standards must adapt to keep up with developments in auditing and the capital markets.

So in 2022, the Board announced one of the most ambitious standard-setting agendas in PCAOB history, and our staff began work on more than 30 standards within 13 standard-setting and research projects.

### *Goal Two: Enhance Inspections*

Inspecting registered public accounting firms is one of the most important tools the PCAOB uses to protect investors.

In fact, the Division of Registration and Inspections is our largest division, with over 460 dedicated professionals inspecting roughly 200 audit firms and 800 audit engagements in more than 30 jurisdictions around the world each year.

PCAOB inspections determine whether firms are complying with PCAOB standards meant to protect investors, and inspectors' work can also provide information that may lead to PCAOB investigations and enforcement actions, as well as standard setting.

The PCAOB's inspection reports provide valuable information to investors, audit committees, and others to help inform their decisions. And the inspection process is the PCAOB's principal means of evaluating the state of audit quality to best keep investors protected.

In 2022, the PCAOB also enhanced its inspections by adapting to emerging risks and issues around the world and providing new insights. Additionally, the PCAOB is now inspecting registered firms in Mainland China and Hong Kong for the first time in PCAOB history. (See page 10 for more on the PCAOB's work to gain complete access to inspect and investigate firms in Mainland China and Hong Kong.)



# 2022 Annual Report

### *Goal Three: Strengthen Enforcement*

The PCAOB's enforcement program protects investors by holding accountable those who put investors at risk by violating PCAOB rules and standards and other related laws and rules. Strong enforcement and meaningful sanctions also deter wrongdoing.

In 2022, the PCAOB approached enforcement with a renewed vigilance, increasing average penalties, pursuing enforcement actions involving certain types of violations for the first time, and taking steps to identify wrongdoing proactively by expanding the use of sweeps of firms to determine whether there may be a violation of PCAOB standards or rules.

### *Goal Four: Improve Organizational Effectiveness*

The PCAOB's most valuable resource is people, including the more than 800 dedicated professionals on our staff who carry out our mission, as well as external stakeholders whose input makes us more effective.

In 2022, the PCAOB took significant steps to invest in our staff and to enhance our stakeholder engagement.

### *Strategic Goals*

The PCAOB's 2022-2026 strategic plan sets out four strategic goals that guide the organization's efforts to achieve its mission of protecting investors.



## Protecting Investors Through One of the Most Ambitious Standard-Setting Agendas in PCAOB History

The PCAOB made progress after updating its standard-setting and research agendas in 2022. More remains to be done. As of December 31, 2022, these were the PCAOB's active research and standard-setting projects. Track and learn more about these projects at [www.pcaobus.org/standards](http://www.pcaobus.org/standards). (See page 14 for more on the PCAOB's advisory groups, which in 2022 provided perspective on our standard-setting and research agendas.)

### Short-Term Standard-Setting Projects



- Quality Control
- Confirmation
- Noncompliance with Laws and Regulations
- Attestation Standards Update
- Going Concern
- Interim Standards – AS 1000
- Amendments Related to Certain Aspects of Designing and Performing Audit Procedures that Involve Technology-Assisted Data Analysis

### Mid-Term Standard-Setting Projects



- Substantive Analytical Procedures
- Fraud
- Interim Ethics and Independence Standards
- Interim Standards

### Research Projects



- Data and Technology
- Firm and Engagement Performance Metrics



Erica Y. Williams  
Chair



Duane M. DesParte  
Board Member



Christina Ho  
Board Member



Kara M. Stein  
Board Member



Anthony C. Thompson  
Board Member

The report: [https://assets.pcaobus.org/pcaob-dev/docs/default-source/about/administration/documents/annual\\_reports/2022-annual-report\\_final.pdf?sfvrsn=d73be283\\_2](https://assets.pcaobus.org/pcaob-dev/docs/default-source/about/administration/documents/annual_reports/2022-annual-report_final.pdf?sfvrsn=d73be283_2)

## Recommendations to Achieve Greater Convergence in Cyber Incident Reporting, Final Report



### *Executive summary*

Cyber incidents are rapidly growing in frequency and sophistication. At the same time, the cyber threat landscape is expanding amid digital transformation, increased dependencies on third party service providers and geopolitical tensions.

The interconnectedness of the global financial system makes it possible that a cyber incident at one financial institution (FI) (or an incident at one of its third-party service providers) could have spill-over effects across borders and sectors.

Recognising that timely and accurate information on cyber incidents is crucial for effective incident response and recovery and promoting financial stability, the G20 asked the FSB to deliver a report on achieving greater convergence in cyber incident reporting (CIR).

To meet this call, the FSB conducted work to promote greater convergence in CIR in three ways:

- (i) setting out recommendations to address the issues identified as impediments to achieving greater harmonisation in incident reporting;
- (ii) enhancing the Cyber Lexicon<sup>1</sup> to include additional terms related to CIR as a 'common language' is necessary for increased convergence; and
- (iii) identifying common types of information that are submitted by FIs to authorities for CIR purposes, which culminated in a concept for a common format for incident reporting exchange (FIRE) to collect incident information from FIs and use between themselves.

FIRE would be flexible to allow a range of adoption choices and include the most relevant data elements for financial authorities.

Drawing from the FSB's body of work on cyber, including engagement with external stakeholders, this report sets out recommendations that aim to promote convergence among CIR frameworks, while recognising that a one-size-fits-all approach is not feasible or preferable.

Financial authorities and FIs can choose to adopt these recommendations as appropriate and relevant, consistent with their legal and regulatory framework.

## Table of Contents

Executive summary .....	1
1. Introduction .....	3
2. Practical issues and challenges to achieving greater convergence in CIR .....	3
2.1. Operational challenges .....	4
2.2. Setting reporting criteria .....	8
2.3. Culture of timely reporting .....	8
2.4. Early assessment challenges .....	10
2.5. Secure communications .....	10
2.6. Cross-border and cross-sectoral issues .....	11
3. Recommendations .....	11
3.1. Design of approach to CIR .....	11
3.2. Supervisory activities and collaboration between authorities .....	18
3.3. Industry engagement .....	20
3.4. Capability development (individual and shared) .....	21
Annex A: 2022 Survey findings .....	24
Annex B: Recommendations mapped to identified issues and challenges .....	32
Annex C: Initial reporting trigger reference material .....	33

### *Recommendations:*

**1. Establish and maintain objectives for CIR.** Financial authorities should have clearly defined objectives for incident reporting, and periodically assess and demonstrate how these objectives can be achieved in an efficient manner, both for FIs and authorities.

**2. Explore greater convergence of CIR frameworks.** Financial authorities should continue to explore ways to align their CIR regimes with other relevant authorities, on a cross-border and cross-sectoral basis, to minimise potential fragmentation and improve interoperability.

**3. Adopt common data requirements and reporting formats.** Financial authorities should individually or collectively identify common data requirements, and, where appropriate, develop or adopt standardised formats for the exchange of incident reporting information.

**4. Implement phased and incremental reporting requirements.** Financial authorities should implement incremental reporting requirements in a phased manner, balancing the authority's need for timely reporting with the affected institution's primary objective of

bringing the incident under control.

- 5. Select appropriate incident reporting triggers.** Financial authorities should explore the benefits and implications of a range of reporting trigger options as part of the design of their CIR regime.
- 6. Calibrate initial reporting windows.** Financial authorities should consider potential outcomes associated with window design or calibration used for initial reporting.
- 7. Provide sufficient details to minimise interpretation risk.** Financial authorities should promote consistent understanding and minimise interpretation risk by providing an appropriate level of detail in setting reporting thresholds, using common terminologies and supplementing CIR guidance with examples.
- 8. Promote timely reporting under materiality-based triggers.** Financial authorities that use materiality thresholds should consider finetuning threshold language, or explore other suitable approaches, to encourage prompt reporting by FIs for material incidents.
- 9. Review the effectiveness of CIR and cyber incident response and recovery (CIRR) processes.** Financial authorities should explore ways to review the effectiveness of FIs' CIR and CIRR processes and procedures as part of their existing supervisory or regulatory engagement.
- 10. Conduct ad-hoc data collection.** Financial authorities should explore ways to complement CIR frameworks with supervisory measures as needed and engage FIs on cyber incidents, both during and outside of live incidents.
- 11. Address impediments to cross-border information sharing.** Financial authorities should explore methods for collaboratively addressing legal or confidentiality challenges relating to the exchange of CIR information on a cross-border basis.
- 12. Foster mutual understanding of benefits of reporting.** Financial authorities should engage regularly with FIs to raise awareness of the value and importance of incident reporting, understand possible challenges faced by FIs and identify approaches to overcome them when warranted.
- 13. Provide guidance on effective CIR communication.** Financial authorities should explore ways to develop, or foster development of, toolkits and guidelines to promote effective communication practices in cyber incident reports.

**14. Maintain response capabilities which support CIR.** FIs should continuously identify and address any gaps in their cyber incident response capabilities which directly support CIR, including incident detection, assessment and training on a continuous basis.

**15. Pool knowledge to identify related cyber events and cyber incidents.** Financial authorities and FIs should collaborate to identify and implement mechanisms to proactively share event, vulnerability and incident information amongst financial sector participants to combat situational uncertainty, and pool knowledge in collective defence of the financial sector.

**16. Protect sensitive information.** Financial authorities should implement secure forms of incident information handling to ensure protection of sensitive information at all times.

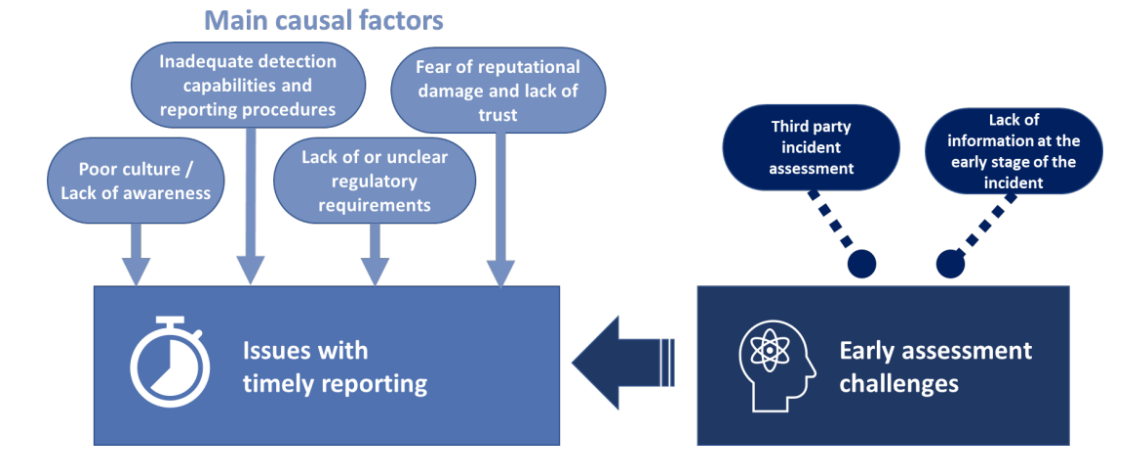


## Recommendations to Achieve Greater Convergence in Cyber Incident Reporting

Final Report





**Possible causal factors to issues with timely reporting****Figure 3**

The report: <https://www.fsb.org/wp-content/uploads/P130423-1.pdf>

## Chair Williams Keynotes Baruch Conference on Financial Reporting



Public Company Accounting Oversight Board (PCAOB) Chair Erica Y. Williams discussed a range of topics from the PCAOB's work to inspect and investigate completely in China, to their 2023 inspection priorities, to the state of audit quality and more during a virtual keynote session, which aired today at Baruch College's 21st Annual Financial Reporting Conference.

The Q&A session was moderated by Sr. Assoc. Dean Paquita Davis-Friday, and can be viewed below.



You may visit: <https://www.youtube.com/watch?v=F5DK37eaHoM>

## SEC Issues Largest-Ever Whistleblower Award



The Securities and Exchange Commission announced the largest-ever award, **nearly \$279 million**, to a whistleblower whose information and assistance led to the successful enforcement of SEC and related actions.

This is the highest award in the SEC's whistleblower program's history, more than doubling the \$114 million whistleblower award the SEC issued in October 2020.

"The size of today's award – the highest in our program's history – not only incentivizes whistleblowers to come forward with accurate information about potential securities law violations, but also reflects the tremendous success of our whistleblower program," said Gurbir S. Grewal, Director of the SEC's Division of Enforcement.

"This success directly benefits investors, as whistleblower tips have contributed to enforcement actions resulting in orders requiring bad actors to disgorge more than \$4 billion in ill-gotten gains and interest. As this award shows, there is a significant incentive for whistleblowers to come forward with accurate information about potential securities law violations."

"The whistleblower's sustained assistance including multiple interviews and written submissions was critical to the success of these actions," said Creola Kelly, Chief of the SEC's Office of the Whistleblower. "While the whistleblower's information did not prompt the opening of the Commission's investigation, their information expanded the scope of misconduct charged."

Payments to whistleblowers are made out of an investor protection fund, established by Congress, which is financed entirely through monetary sanctions paid to the SEC by securities law violators.

No money has been taken or withheld from harmed investors to pay whistleblower awards. Whistleblowers may be eligible for an award when they voluntarily provide the SEC with original, timely, and credible information that leads to a successful enforcement action, and adhere to filing requirements in the whistleblower rules. Whistleblower awards can range from 10 to 30 percent of the money collected when the monetary sanctions exceed \$1 million.

As set forth in the Dodd-Frank Act, the SEC protects the confidentiality of whistleblowers and does not disclose any information that could reveal a whistleblower's identity.

For more information about the whistleblower program and how to report a tip, visit <https://www.sec.gov/whistleblower>

You may visit: <https://www.sec.gov/news/press-release/2023-89>

## Supercharging security with generative AI

Sunil Potti, VP/GM, Google Cloud Security



At Google Cloud, we continue to invest in key technologies to progress towards our true north star on invisible security: making strong security pervasive and simple for everyone.

Our investments are based on insights from our world-class threat intelligence teams and experience helping customers respond to the most sophisticated cyberattacks.

Customers can tap into these capabilities to gain perspective and visibility on the most dangerous threat actors that no one else has.

Recent advances in artificial intelligence (AI), particularly large language models (LLMs), accelerate our ability to help the people who are responsible for keeping their organizations safe.

These new models not only give people a more natural and creative way to understand and manage security, they give people access to AI-powered expertise to go beyond what they could do alone.

At the RSA Conference 2023, we are excited to announce Google Cloud Security AI Workbench, an industry-first extensible platform powered by a specialized, security LLM, Sec-PaLM.

This new security model is fine-tuned for security use cases, incorporating our unsurpassed security intelligence such as Google's visibility into the threat landscape and Mandiant's frontline intelligence on vulnerabilities, malware, threat indicators, and behavioral threat actor profiles.

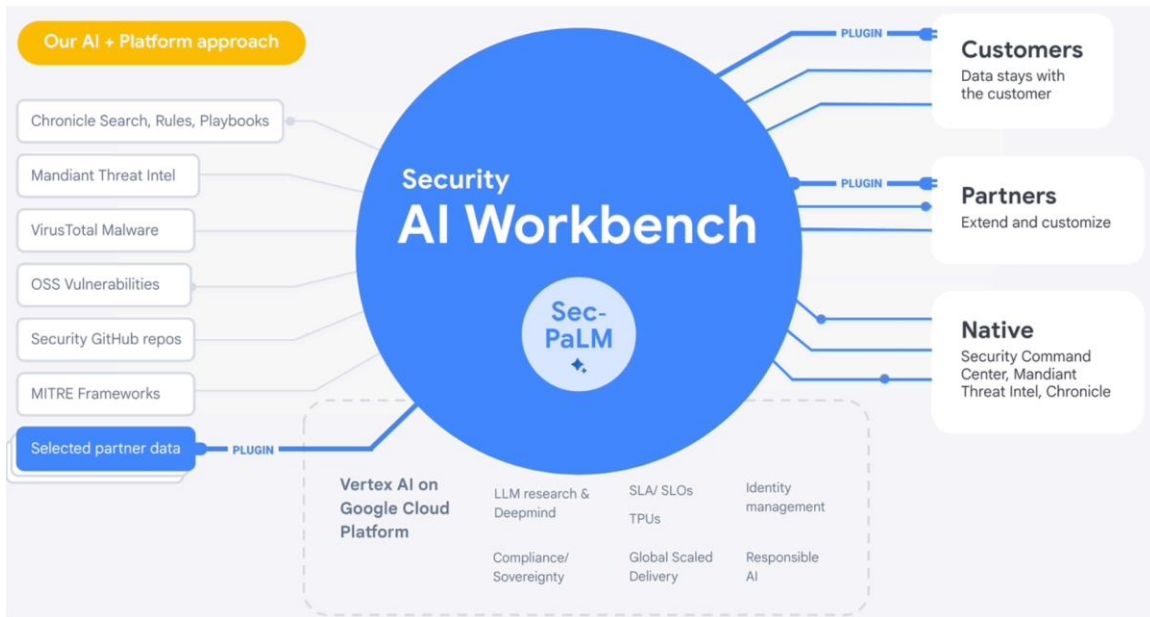
Google Cloud Security AI Workbench powers new offerings that can now uniquely address three top security challenges: threat overload, toilsome tools, and the talent gap.

It will also feature partner plug-in integrations to bring threat intelligence, workflow, and other critical security functionality to customers, with Accenture being the first partner to utilize Security AI Workbench.

The platform will also let customers make their private data available to the platform at inference time; ensuring we honor all our data privacy commitments to customers.

Because Security AI Workbench is built on Google Cloud's Vertex AI infrastructure, customers control their data with enterprise-grade

capabilities such as data isolation, data protection, sovereignty, and compliance support.



To read more: <https://cloud.google.com/blog/products/identity-security/rsa-google-cloud-security-ai-workbench-generative-ai>

## Introducing Microsoft Security Copilot: Empowering defenders at the speed of AI



Today the odds remain stacked against cybersecurity professionals. Too often, they fight an asymmetric battle against prolific, relentless and sophisticated attackers.

To protect their organizations, defenders must respond to threats that are often hidden among noise.

Compounding this challenge is a global shortage of skilled security professionals, leading to an estimated 3.4 million openings in the field.

The volume and velocity of attacks requires us to continually create new technologies that can tip the scales in favor of defenders.

Security professionals are scarce, and we must empower them to disrupt attackers' traditional advantages and drive innovation for their organizations.

In the last few months, the world has witnessed a wave of innovation as organizations apply advanced AI to new technologies and use cases.

We are ready for a paradigm shift and taking a massive leap forward by combining Microsoft's leading security technologies with the latest advancements in AI.

### *Security Copilot — end-to-end defense at machine speed and scale*

Microsoft Security Copilot is the first security product to enable defenders to move at the speed and scale of AI. Security Copilot combines this advanced large language model (LLM) with a security-specific model from Microsoft.

This security-specific model in turn incorporates a growing set of security-specific skills and is informed by Microsoft's unique global threat intelligence and more than 65 trillion daily signals.

Security Copilot also delivers an enterprise-grade security and privacy-compliant experience as it runs on Azure's hyperscale infrastructure. When Security Copilot receives a prompt from a security professional, it uses the full power of the security-specific model to deploy skills and queries that maximize the value of the latest large language model capabilities. And this is unique to a security use-case.

Our cyber-trained model adds a learning system to create and tune new skills. Security Copilot then can help catch what other approaches might miss and augment an analyst's work. In a typical incident, this boost translates into gains in the quality of detection, speed of response and ability to strengthen security posture. Security Copilot doesn't always get everything right. AI-generated content can contain mistakes.

But Security Copilot is a closed-loop learning system, which means it's continually learning from users and giving them the opportunity to give explicit feedback with the feedback feature that is built directly into the tool.

As we continue to learn from these interactions, we are adjusting its responses to create more coherent, relevant and useful answers.

Security Copilot also integrates with the end-to-end Microsoft Security products, and over time it will expand to a growing ecosystem of third-party products. So, in short, Security Copilot is not only a large language model, but rather a system that learns, to enable organizations to truly defend at machine speed.

We absolutely believe that security is a team sport, and security should be built with privacy at the core. We've built Security Copilot with security teams in mind— your data is always your data and stays within your control.

It is not used to train the foundation AI models, and in fact, it is protected by the most comprehensive enterprise compliance and security controls. While remaining private, each user interaction can be easily shared with other team members to accelerate incident response, collaborate more effectively on complex problems and develop collective skills.

To read more: <https://news.microsoft.com/ai-security-2023/>



## PCAOB Releases 2022 Inspection Reports for Mainland China, Hong Kong Audit Firms

Chair Williams says reports are “a powerful first step toward accountability,” as demand for complete access continues



Public Company Accounting Oversight Board (PCAOB) Chair Erica Y. Williams made the following statement today after the PCAOB released inspection reports for two firms inspected in 2022: KPMG Huazhen LLP in mainland China and PricewaterhouseCoopers in Hong Kong.

INSPECTION REPORT

### KPMG Huazhen LLP

COUNTRY      INSPECTION REPORT DATE  
China      Mar. 28, 2023

 [Download PDF](#)

INSPECTION REPORT

### PricewaterhouseCoopers

COUNTRY      INSPECTION REPORT DATE  
Hong Kong      Mar. 28, 2023

 [Download PDF](#)

*From Chair Williams:*

Thanks to the leadership of the U.S. Congress in passing the Holding Foreign Companies Accountable Act (HFCAA), last year, the PCAOB secured complete access to inspect registered public accounting firms headquartered in mainland China and Hong Kong for the first time in history.

Today, the PCAOB is releasing the inspection reports for both firms inspected in 2022: KPMG Huazhen LLP in mainland China and PricewaterhouseCoopers in Hong Kong.

Both reports show unacceptable rates of Part I.A deficiencies, which are deficiencies of such significance that PCAOB staff believe the audit firm failed to obtain sufficient appropriate audit evidence to support its work on the public company’s financial statements or internal control over financial reporting.

The PCAOB inspected a total of eight engagements in 2022 – four at each of the two firms – including the types of engagements to which People’s

Republic of China (PRC) authorities had previously denied access, such as large state-owned enterprises and issuers in sensitive industries.

PCAOB inspectors found Part I.A deficiencies in 100% (four of four) of the audit engagements reviewed at KPMG Huazhen and 75% (three of four) of the audit engagements reviewed for PwC Hong Kong.

As I have said before, any deficiencies are unacceptable. At the same time, it is not unexpected to find such high rates of deficiencies in jurisdictions that are being inspected for the first time. And the deficiencies identified by PCAOB staff at the firms in mainland China and Hong Kong are consistent with the types and number of findings the PCAOB has encountered in other first-time inspections around the world.

The fact that our inspectors found these deficiencies is a sign that the HFCAA was effective and the inspection process worked as it is supposed to. We identified problems so now we can begin the work of holding firms accountable to fix them.

Today's reports are a powerful first step toward accountability. By shining a light on deficiencies, our inspection reports provide investors, audit committees, and potential clients with important information so they can make informed decisions and hold firms accountable. And the power of transparency applies public pressure for firms to improve.

The remediation process is another tool we use to hold firms accountable for fixing deficiencies. By law, public inspection reports do not initially include quality control deficiencies that inspectors find. Instead, firms have one year to remediate those deficiencies. If they don't remediate those deficiencies to the Board's satisfaction, we make them public.

Finally, where appropriate, our inspectors will refer inspection findings to our enforcement team for possible action. If violations are found, our enforcement staff will not hesitate to recommend sanctions, including imposing significant money penalties and barring bad actors from performing future audits.

Last year was only the beginning of our work to inspect and investigate firms in mainland China and Hong Kong.

Our enforcement teams continue to pursue investigations, and inspectors have begun fieldwork for 2023's inspections. We anticipate fieldwork will continue off and on throughout most of the year, which is common practice for inspections such as these in jurisdictions around the world.

The two firms we inspected in 2022 audited 40% of the total market share of U.S.-listed companies audited by Hong Kong and mainland China firms,

and we are on track to hit 99% of the total market share by the end of this year. So, there is no question that the PCAOB is prioritizing inspections that are the most relevant to investors on U.S. markets – because protecting investors is what this is all about.

Indeed, the release of today's reports is yet another sign that investors are more protected because of Congress' leadership in passing the HFCAA. And last year's legislation, which shortened the timeline from three years to two years, provided important leverage as the PCAOB continues demanding complete access to inspect and investigate firms headquartered in mainland China and Hong Kong – with no loopholes and no exceptions.

As I have said before, should PRC authorities obstruct or otherwise fail to facilitate the PCAOB's access – in any way and at any time – the Board will act immediately to consider the need to issue a new determination.

I want to thank the hardworking inspectors, investigators, and PCAOB staff who continue this important work on behalf of investors every day.

**2022 Inspection**  
**KPMG Huazhen LLP**  
(Headquartered in Beijing, People's Republic of China)  
March 28, 2023

THIS IS A PUBLIC VERSION OF A PCAOB INSPECTION REPORT

PORTIONS OF THE COMPLETE REPORT ARE OMITTED FROM THIS DOCUMENT IN ORDER TO COMPLY WITH SECTIONS 104(g)(2) AND 105(b)(5)(A) OF THE SARBANES-OXLEY ACT OF 2002

PCAOB RELEASE NO. 104-2023-049



# 2022 Inspection PricewaterhouseCoopers

(Headquartered in Hong Kong Special  
Administrative Region of the People's Republic  
of China)

March 28, 2023

**THIS IS A PUBLIC VERSION OF A PCAOB INSPECTION REPORT**

PORTIONS OF THE COMPLETE REPORT ARE OMITTED FROM THIS DOCUMENT IN ORDER TO COMPLY WITH SECTIONS 104(g)(2) AND 105(b)(5)(A) OF THE SARBANES-OXLEY ACT OF 2002

PCAOB RELEASE NO. 104-2023-050



To read more: <https://pcaobus.org/news-events/news-releases/news-release-detail/pcaob-releases-2022-inspection-reports-for-mainland-china-hong-kong-audit-firms>

<https://pcaobus.org/oversight/inspections/firm-inspection-reports>

## PCAOB Enhances Transparency of Inspection Reports With New Section on Auditor Independence and More

Eight 2022 inspection reports released today include new transparency enhancements



The Public Company Accounting Oversight Board (PCAOB) announced it has enhanced its inspection reports with a new section on auditor independence and a range of other improvements that increase transparency by making publicly available more information that is relevant, reliable, and useful for investors and other stakeholders.

The changes will appear in reports for PCAOB inspections completed in 2022, beginning with eight reports released today, which can be found at the Firm Inspection Reports page.

“We are committed to making our inspection reports as valuable as possible for investors, audit committees, and others, and today we take another significant step in advancing that goal by shining a greater light on independence violations and more,” said PCAOB Chair Erica Y. Williams. “These enhancements will provide relevant information that investors have asked for and support improvements in overall audit quality.”

The enhanced inspection reports will include:

1. *A new section of the report focused on independence violations:* Reports will feature a new independence section (Part I.C) that will discuss instances of noncompliance with PCAOB rules related to maintaining independence, as well as potential noncompliance with U.S. Securities and Exchange Commission independence rules.
2. *More information related to fraud procedures and the identification and assessment of the risks of material misstatements:* Reports will expand Part I.B to include deficiencies related to AS 2401, Consideration of Fraud in a Financial Statement Audit, and AS 2110, Identifying and Assessing Risks of Material Misstatement.
3. *More commentary:* Reports will provide additional commentary in Part I.A for certain situations, such as whether the audit was the firm’s first audit of the issuer or whether the firm had identified significant risks, including fraud, for areas in which PCAOB inspection staff identified deficiencies.

4. *New graphs:* For annually inspected firms, reports will include charts to clearly show firm and engagement partner tenure.

“These enhancements will further drive audit quality and make our inspection reports even more useful for the public,” said George R. Botic, Director of the PCAOB’s Division of Registration and Inspections. “We are especially pleased to provide more information on auditor independence, which is essential to audit quality and underpins the objectivity, credibility, and integrity of the audit.”

Learn more about PCAOB inspection reports and the inspection process at our Inspections page, at: <https://pcaobus.org/oversight/inspections>



The screenshot shows a web browser window displaying the PCAOB website. The URL in the address bar is <https://pcaobus.org/oversight/inspections/firm-inspection-reports>. The page features a dark blue header with the PCAOB logo (Public Company Accounting Oversight Board) on the left and navigation links for 'About', 'Oversight', 'Resources', 'News & Events', 'Careers', and 'Subscribe' on the right. Below the header, a breadcrumb trail reads 'Home > Oversight > Inspections'. The main heading is 'Firm Inspection Reports'. The text below explains that the Sarbanes-Oxley Act authorizes the PCAOB to inspect registered firms for compliance with laws, rules, and professional standards. It notes that registered firms with 100 or fewer audit reports are inspected every three years, while those with more than 100 are inspected annually. It also states that the Board inspects firms with a substantial role in issuer audits, but not those that perform no issuer audit work. A note at the bottom indicates that more information on broker-dealer inspections is available on a dedicated page.

To read more: <https://pcaobus.org/news-events/news-releases/news-release-detail/pcaob-enhances-transparency-of-inspection-reports-with-new-section-on-auditor-independence-and-more>

## Cybersecurity: Protecting Investors

Commissioner Jaime Lizárraga - Remarks before the Digital Directors Network 2023 Conference



U.S. SECURITIES AND  
EXCHANGE  
COMMISSION

Good morning. Thank you, Bob [Zukis]. It is a pleasure to be here today, and I thank the Digital Directors Network for hosting this discussion about cybersecurity. This topic is so essential for the safety and resiliency of our capital markets.

My special thanks to former Commissioner Luis Aguilar for initially inviting me to speak to you today. Commissioner Aguilar had a distinguished career in public service. As the eighth longest-serving Commissioner in SEC history, he was one of only three Commissioners to have been nominated by two U.S. Presidents from different parties. A remarkable accomplishment.

It is exciting to speak to an audience of cybersecurity professionals and directors like yourselves, who share a deep commitment to robust policies and practices in cyber governance.

Since 2017, the Digital Directors Network has served as a resource to the wide variety of members it represents – that is, those responsible for designing, implementing, and testing cyber governance policies and procedures.

Over the next two days, you will hear a range of views on how best to address the complex and rapidly evolving cyber challenges that all market participants are confronting in our capital markets today.

At the SEC, we are at the forefront of addressing these challenges. In the face of rapid technological change and increased cyber threats at home and abroad, the Commission is taking action to require that market participants strengthen their cybersecurity practices.

Consistent with our congressional mandates, one of our key aims is to protect the investing public against potentially significant financial and reputational costs from cyberattacks and data breaches.

Because once victims' identities are stolen or their personal information is compromised, the damage can be irreparable and irreversible.

The Commission's actions go hand-in-hand with our ongoing efforts to modernize and update some of our outdated rules. As part of our mission

to protect investors, facilitate capital formation, and promote fair and efficient markets, we have a responsibility to update our regulatory framework to keep pace with emerging risks, whether driven by technological change or any other factor.

The Commission has proposed several rules that are designed to protect investors in our capital markets from cyber risks. These rules will require covered market entities to implement practices that will make their operations more secure and will mitigate risks to themselves, their customers, and our markets.

Why does robust cybersecurity matter? Cyberattacks and data breaches can have devastating impacts on companies and their customers and undermine investor and market confidence. In the last decade, cyberattacks of all sizes have resulted in hundreds of millions of records stolen and billions in damages to victims.

The interagency U.S. Financial Stability Oversight Counsel, or FSOC, noted in its 2021 annual report, that a major cyber incident could threaten the stability of U.S. markets in at least three ways: by

- (1) disrupting a single point of failure in our financial markets, such as a key financial service provider or utility;
- (2) compromising the integrity of a critical dataset; or
- (3) causing a significant loss of confidence in our capital markets, resulting in market participants withdrawing from the markets.

Our capital markets are nearly \$100 trillion in size – representing 40 percent of the world’s total – and process over a trillion dollars of transactions per day.

By facilitating capital raising by businesses large and small, they play an instrumental role in our economy. And they serve working families who invest their savings as an optimistic way of channeling their hopes and dreams for the future – to build long-term wealth.

In light of this, it is critical that we do everything in our power to strengthen cyber practices, so that our financial markets can be more resilient and so that investors can be protected – in the most effective way possible.

The use of, and reliance on, technology in our capital markets has increased exponentially in recent years. A variety of factors have contributed to this trend. Digital innovations have led to greater interconnectedness, increased computing power and lower overall costs.



Expanded opportunities for the public to access financial services through smartphones is another factor. The COVID-19 pandemic also contributed to this digital transformation by accelerating the shift to online services to replace in-person interactions.

While these developments and innovations have the potential to increase competition, efficiency, and participation in the capital markets, they may also increase cyber risks.

Last year, the Financial Stability Board (FSB), noted in a key report that cyber incidents are “rapidly growing in frequency and sophistication,” take place in the context of “growing interconnectedness of the financial system,” and create greater risk of “spillover effects across borders and sectors.”

To read more: <https://www.sec.gov/news/speech/lizarraga-remarks-cybersecurity-051623>

## 2023 State of Homeland Security Remarks: Tackling an Evolving Threat Landscape – Homeland Security in 2023

Secretary Mayorkas delivered the State of Homeland Security address at the Council on Foreign Relations



Good morning, everybody. Margaret, thank you for the introduction and for the discussion we are going to have in just a few minutes. My thanks to the Council on Foreign Relations for hosting us and thanks to all of you for being here. I would like to recognize two individuals, if I may, who have special meaning to our department. Our second Secretary of Homeland Security, Michael Chertoff. And former United States Congresswoman Jane Harman.

Reflecting on the state of our homeland security in 2023, it seemed fitting to pose a fundamental question to a generative AI model: “in one sentence, describe how the homeland security threat environment has evolved over the past 20 years.”

We are, after all, confronting a dramatically changed environment compared to the one we faced in March 2003. One that could change even more dramatically, as AI grips our imaginations and accelerates into our lives in uncharted and basically unmanaged fashion.

Deeply fascinated by generative AI’s promise of new advances and discoveries, greatly concerned for its capacity for error and its impact on our humanity, and keenly alert to its potential for harm in the hands of an adversary, I waited only seconds for the AI model’s answer:

“The homeland security threat environment has evolved from a primarily focused counterterrorism posture to a complex and diverse landscape of challenges that include cyberattacks, domestic extremism, and the COVID-19 pandemic, among others.”

A straightforward answer to an important question that addresses the evolved threat landscape that our Department of Homeland Security must now confront. Its evolution is about to accelerate.

Only about six months ago, engaging with an AI chatbot was reserved for a few in Silicon Valley and universities. Today about 100 million users per

month are asking an AI chatbot just about anything, from recipe recommendations to requests for scientific analyses.

The exponential growth of internet technology and the change it has driven has been extraordinary. As we reflect on the state of our homeland security today, that explosive growth compels the question: what will this growth mean for our safety and security over the next 20 years?

We stand at the outset of what President Biden has aptly described as a “decisive decade” for our world. It is the same for our homeland security. Revolutionizing technological innovations, growing political and economic instability, widening wealth inequality, a rapidly changing climate, increasingly aggressive nation states, emerging infectious diseases, and other forces are transforming the global landscape, challenging and sometimes rendering moot a nation’s borders, and bringing national and international threats to any community’s doorstep.

Our Department was founded to protect us in the wake of the tragedy and devastation inflicted by the terrorist attacks of 9/11, bringing together 22 agencies from across the Federal Government charged with the mission of securing our homeland.

Back then, our country was focused on the threat of foreign terrorists who sought to enter the United States and do us harm. Over the next ten years emerged the threat of the homegrown violent extremist, the individual already resident here who was radicalized to violence by a foreign terrorist ideology.

While those threats certainly persist, today lone offenders and small cells of individuals motivated by a wide range of grievances and violent extremist ideologies – from white supremacy and anti-Semitism to anti-government attitudes – pose the most persistent and lethal terrorism-related threat in the United States.

The effects of climate change have intensified. Wildfire season is no longer confined to the summer months but is now year-round. Tornadoes and named hurricanes in the United States are more frequent and more destructive.

Just a few weeks ago in Mississippi, I surveyed the devastation wrought by a tornado that, in 20 seconds and at speeds up to 200 miles per hour, ripped through a small town, destroying multiple communities and taking the lives of more than 20 people.

Not for a century have we confronted the calamity of an infectious disease as we have over the past three years. COVID-19 took more than one million lives here in the United States, impacted every aspect of our daily life, and

forced on us a new understanding of the threat pandemic diseases can pose as they spread through paths of international trade and travel.

Globally, the impacts of disasters coupled with the rise of authoritarianism, corruption, conflict, violence, and persecution have resulted in an historic displacement and migration of people around the world and a consequent strain on immigration systems ill-equipped to address it.

According to the United Nations High Commissioner for Refugees, at the end of 2021, 89.3 million people worldwide had fled their homes due to conflict, violence, fear of persecution and human rights violations. This is the most since World War II and more than double the number of people who remained forcibly displaced a decade ago.

Criminal organizations have capitalized on this surge. The reach and growing ruthlessness of smuggling organizations have changed how people migrate. Drug trafficking organizations have grown in sophistication and power, creating new means of manufacturing and selling death and destruction.

From late 1989 through early 2001, I prosecuted federal drug trafficking crimes, from the trafficking of cocaine to methamphetamine to black tar heroin and more. Nothing I saw then matches the scourge of fentanyl that we have confronted for over the past five years. 46,802 overdose deaths in 2018; 57,834 in 2020, and 71,238 in 2021.

Over that same time, those seeking to exploit the most vulnerable have taken their depravity to an unimaginable level. The National Center for Missing and Exploited Children, the nation's clearinghouse for child sexual abuse material, received over 32 million cyber tips in 2022, corresponding to more than 88 million images and videos of child sexual abuse, a roughly 75 percent increase in the last five years.

88 million images and videos of child sexual abuse.

As threats of the past have changed in form, complexity, and magnitude, so too have new threats emerged. This is perhaps nowhere more acute than in cyberspace.

Some estimate that roughly 14.4 billion devices are connected as part of the Internet of Things, everything from our home thermostats and doorbells to our electric grid and fuel pipelines. This has brought significant advances in capabilities and conveniences, but it also has exponentially increased the ways our interconnected, digital world can be exploited to do us harm.

Today, malicious cyber actors are capable of disrupting gasoline supplies across an entire region of the country, preventing hospitals from delivering

critical care, and causing disruption in some of the school systems around our country.

Nation states like the People's Republic of China and Russia upend our rules-based international order and threaten our security at home, whether through cyberattacks, abuse of our trade and travel systems, or through disinformation campaigns that seek to undermine our democratic institutions. Our homeland security has converged with our broader national security.

The profound evolution in the homeland security threat environment, changing at a pace faster than ever before, has required our Department of Homeland Security to evolve along with it.

We have built new institutions, modernized our approach and processes, developed new capabilities, and are harnessing innovation as we deliver critical services that are more in demand than ever before.

Our overarching strategy is one of partnership. Homeland security cannot be accomplished by government alone; it requires collective action.

To meet the threat of domestic violent extremism, we created the Center for Prevention Programs and Partnerships to share with local communities the best practice models of identification and intervention when an individual is exhibiting signs of moving towards violence.

Through our grant programs we are helping communities build threat prevention capabilities where previously they did not exist, responding to the reality that major metropolitan areas are no longer our adversaries' only targets.

Across the Federal Government, we are working with communities impacted by unprecedented extreme weather events to strengthen their long-term recovery.

We have developed for the first time Department-wide incident management teams to lead all-of-government responses to emergent challenges, from vaccinating millions of Americans against COVID-19 and resettling Afghan nationals in Operation Allies Welcome, to providing protection for fleeing Ukrainians in Uniting for Ukraine.

We are coordinating and sharing intelligence with our partner nations and executing whole of government disruption and dismantlement campaigns to attack cartels.

In collaboration with diaspora communities here in the United States, we are building lawful pathways, so that migrants fleeing persecution can

access safe and orderly avenues to obtain the humanitarian relief that our laws provide.

We are working collaboratively with our partners across government, at home and abroad, and with industry and academia, to manage and reduce risk to the cyber and physical infrastructure Americans rely on every day.

We are partnering across the U.S. government to protect the most vulnerable from exploitation, whether they are migrants being trafficked by unscrupulous employers or children who are being abused online. Exploitation of the vulnerable.

In fact, yesterday we released the Third Quadrennial Homeland Security Review, our new vision for securing the homeland, and in it we included this work of combatting crimes of exploitation – such as human trafficking, child exploitation, and labor exploitation – as a dedicated homeland security mission alongside our work countering terrorism, securing our borders, administering our immigration system, securing cyberspace and critical infrastructure, and building resilience and responding to disasters. This reflects the overriding importance of supporting victims and stopping the perpetrators of these abhorrent crimes.

But, what of the threats as they could materialize tomorrow? I want to highlight new initiatives in two key areas that cut across all the Department's missions.

The People's Republic of China poses an especially grave threat to the homeland, one that indeed does touch all of our Department's missions.

Beijing has the capability and the intent to undermine our interests at home and abroad and is leveraging every instrument of its national power to do so, from its increasingly aggressive presence in the South China Sea to the overseas police stations used to harass and intimidate dissenters.

A PRC invasion of Taiwan would have profound reverberations in the homeland, putting our civilian critical infrastructure at risk of a disruptive cyberattack. We must ensure we are poised to guard against this threat today and into the future.

I have directed a 90-day Department-wide sprint to assess how the threats posed by the PRC will evolve and how we can be best positioned to guard against future manifestations of this threat:

One critical area we will assess, for example, involves the defense of our critical infrastructure against PRC or PRC-sponsored attacks designed to disrupt or degrade provision of national critical functions, sow discord and panic, and prevent mobilization of U.S. military capabilities.

Another area of assessment will involve how we can bolster our screening and vetting to identify illicit travelers from the PRC who exploit our lawful immigration and travel systems to collect intelligence, steal intellectual property, and harass dissidents, while still we must facilitate lawful travel.

Informed by engagements with subject matter experts and our stakeholders, we will take immediate action to drive down risk, lay the foundation for ongoing public-private collaboration, and work with Congress to ensure we continue to invest in these vital capabilities.

Next, and returning to where I began, we must address the many ways in which artificial intelligence will drastically alter the threat landscape and augment the arsenal of tools we possess to succeed in the face of these threats.

Our Department will lead in the responsible use of AI to secure the homeland and in defending against the malicious use of this transformational technology. As we do this, we will ensure that our use of AI is rigorously tested to avoid bias and disparate impact, and is clearly explainable to the people we serve.

I recently asked our Homeland Security Advisory Council, co-chair Jamie Gorelick is here, to study the intersection of AI and homeland security and deliver findings that will help guide our use of it and defense against it. The rapid pace of technological change – the pivotal moment we are now in – requires that we also act today.

To that end, I am directing the creation of our Department's first Artificial Intelligence Task Force that will drive specific applications of AI to advance our critical homeland security missions. The Task Force will, for example:

Integrate AI into our efforts to enhance the integrity of our supply chains and the broader trade environment. We will seek to deploy AI to more ably screen cargo, identify the importation of goods produced with forced labor, and manage risk.

The Task Force will also, among other charged, leverage AI to counter the flow of fentanyl into the United States.

We will explore using this technology to better detect fentanyl shipments, identify and interdict the flow of precursor chemicals around the world, and target for disruption key nodes in the criminal networks.

Countering the multi-faceted threat posed by the PRC, learning from major cyber incidents, and harnessing the power of AI to advance our security will draw on the entirety of the capabilities and expertise the 260,000 personnel of DHS bring to bear every single day.

It will require continued investment in our operational cohesion, our ability to work together in ways our founders never imagined.

We must never allow ourselves to be susceptible to ‘failures of imagination,’ which, as the 9/11 Commission concluded nearly 20 years ago, held us back from connecting the dots and preparing for the destruction that was being planned on that tragic day.

We must instead look to the future and imagine the otherwise unimaginable, to ensure that whatever threats we face, our Department – our country – will be positioned to meet the moment.

It is an especially challenging imperative to fulfill at a time not only of rapid change, but also of acute political divisiveness; when issues of homeland security that traditionally were unifying no longer are so, and when our adversaries continue to exploit innovations designed to bring us closer together, like social media, to push us apart.

We must imagine a world where even more potent and lethal synthetic opioids or infectious diseases plague our communities. Where an earthquake or catastrophic storm intensifies already historic levels of migration in our hemisphere.

Where criminals 3D print weapons or modify consumer technologies like drones to evade law enforcement. Where cyber criminals are emboldened to the point of holding for ransom the critical services of an entire city.

At the Department of Homeland Security, we have the tools and talent to meet the moment today. We are taking the actions and making the investments to ensure we will continue to adapt and meet the moment into the future. We are more fit for purpose than at any time in our 20-year history.

This is a collective effort: we must all come together in the service of our homeland security. We must call upon our collective imagination, our commitment to a better future, and our fundamental love of country that binds us together, to protect our homeland.

Thank you.

To read more: <https://www.dhs.gov/news/2023/04/21/2023-state-homeland-security-remarks-tackling-evolving-threat-landscape-homeland>



## Review of the Federal Reserve's Supervision and Regulation of Silicon Valley Bank



Silicon Valley Bank (SVB) failed because of a textbook case of mismanagement by the bank. Its senior leadership failed to manage basic interest rate and liquidity risk. Its board of directors failed to oversee senior leadership and hold them accountable. And Federal Reserve supervisors failed to take forceful enough action, as detailed in the report.

Our banking system is sound and resilient, with strong capital and liquidity. And in some respects, SVB was an outlier because of the extent of its highly concentrated business model, interest rate risk, and high level of reliance on uninsured deposits; however, SVB's failure demonstrates that there are weaknesses in regulation and supervision that must be addressed.

Regulatory standards for SVB were too low, the supervision of SVB did not work with sufficient force and urgency, and contagion from the firm's failure posed systemic consequences not contemplated by the Federal Reserve's tailoring framework.

Following SVB's failure, [we must strengthen the Federal Reserve's supervision and regulation](#) based on what we have learned. This report represents the first step in that process—a self-assessment that takes an unflinching look at the conditions that led to the bank's failure, including the role of Federal Reserve supervision and regulation.

Individuals who were not involved in the supervision of SVB conducted the review, and I oversaw it.

The four key takeaways of the report are:

1. Silicon Valley Bank's board of directors and management failed to manage their risks.
2. Supervisors did not fully appreciate the extent of the vulnerabilities as Silicon Valley Bank grew in size and complexity.
3. When supervisors did identify vulnerabilities, they did not take sufficient steps to ensure that Silicon Valley Bank fixed those problems quickly enough.

4. The Board's tailoring approach in response to the Economic Growth, Regulatory Relief, and Consumer Protection Act (EGRRCPA) and a shift in the stance of supervisory policy impeded effective supervision by reducing standards, increasing complexity, and promoting a less assertive supervisory approach.



BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM  
WASHINGTON, D. C. 20551

MICHAEL S. BARR  
VICE CHAIR FOR SUPERVISION

April 28, 2023

**Re: Review of the Federal Reserve's Supervision and Regulation of Silicon Valley Bank**

Before discussing specific supervisory and regulatory changes that we should consider, I would like to touch on broader issues exposed by the failure of the bank.

First, the combination of social media, a highly networked and concentrated depositor base, and technology may have fundamentally changed the speed of bank runs. Social media enabled depositors to instantly spread concerns about a bank run, and technology enabled immediate withdrawals of funding.

Second, as I have previously stated, a firm's distress may have systemic consequences through contagion—where concerns about one firm spread to other firms—even if the firm is not extremely large, highly connected to other financial counterparties, or involved in critical financial services.

Third, this experience has emphasized why strong bank capital matters. While the proximate cause of SVB's failure was a liquidity run, the underlying issue was concern about its solvency.

As risks in the financial system continue to evolve, we need to continuously evaluate our supervisory and regulatory framework and be humble about our ability to assess and identify new and emerging risks.

That is why we need to bolster resiliency broadly in the financial system, and not focus solely on specific risk drivers.

Some steps already in progress include the holistic review of our capital framework; implementation of the Basel III endgame rules; the use of multiple scenarios in stress testing; and a long-term debt rule to improve the resiliency and resolvability of large banks.

We plan to seek comment on these proposals soon. Other possible steps based on what we have learned from the SVB report, SVB's failure, and its contagion, will follow later.

<b>Preface</b> .....	vii
<b>Executive Summary</b> .....	1
Silicon Valley Bank Financial Group .....	2
Federal Reserve Oversight .....	5
Other Findings .....	13
Issues for Consideration .....	14
<b>Evolution of Silicon Valley Bank</b> .....	17
Overview .....	17
SVBFG's Rapid Growth .....	18
SVBFG and the Tech Sector .....	19
SVBFG Relative to Peers .....	22
SVB's Failure .....	22
External Views .....	25
<b>Federal Reserve Supervision</b> .....	27
Overview .....	27
Supervisory Portfolio Structure and Supervisory Activities .....	29
Overview of Supervisory Views .....	39
<b>Supervision of SVBFG by Critical Risk Areas</b> .....	45
Governance and Risk Management .....	45
Liquidity Supervision .....	51
Interest Rate Risk and Investment Portfolio Supervision .....	60
<b>Additional Topics</b> .....	67
Federal Reserve Surveillance and Risk Analysis .....	67
Incentive Compensation .....	72
Assessment of the Federal Reserve Approval of SVB Financial Group Applications .....	76
Regulation K Notices .....	78
Tying .....	78
Volcker Rule .....	79
<b>Federal Reserve Regulation</b> .....	81
Regulatory Framework .....	81
Regulations that Applied to SVBFG .....	83
Pro Forma Impact of EGRRCPA and Tailoring .....	86
Conclusions .....	91

---

<b>Observations for Federal Reserve Oversight</b> .....	<b>93</b>
Lessons Learned from Earlier Bank Failures .....	<b>93</b>
Issues for Consideration .....	<b>95</b>
Conclusions .....	<b>98</b>
 <b>Glossary</b> .....	 <b>99</b>

To read more: <https://www.federalreserve.gov/publications/files/svb-review-20230428.pdf>

## The European Commission adopted the first designation decisions under the Digital Services Act (DSA).



The European Commission designated 17 Very Large Online Platforms (VLOPs) and 2 Very Large Online Search Engines (VLOSEs) that reach at least 45 million monthly active users.

### *Very Large Online Platforms:*

- Alibaba AliExpress
- Amazon Store
- Apple AppStore
- Booking.com
- Facebook
- Google Play
- Google Maps
- Google Shopping
- Instagram
- LinkedIn
- Pinterest
- Snapchat
- TikTok
- Twitter
- Wikipedia
- YouTube
- Zalando

### *Very Large Online Search Engines:*

- Bing
- Google Search

Following their designation, the companies will now have to comply, within four months, with the full set of new obligations under the DSA.

These aim at empowering and protecting users online, including minors, by requiring the designated services to assess and mitigate their systemic risks and to provide robust content moderation tools.

This includes:

### *More user empowerment:*

- Users will get clear information on why they are recommended certain information and will have the right to opt-out from recommendation systems based on profiling;
- Users will be able to report illegal content easily and platforms have to process such reports diligently;
- Advertisements cannot be displayed based on the sensitive data of the user (such as ethnic origin, political opinions or sexual orientation);
- Platforms need to label all ads and inform users on who is promoting them;
- Platforms need to provide an easily understandable, plain-language summary of their terms and conditions, in the languages of the Member States where they operate.

*Strong protection of minors:*

- Platforms will have to redesign their systems to ensure a high level of privacy, security, and safety of minors;
- Targeted advertising based on profiling towards children is no longer permitted;
- Special risk assessments including for negative effects on mental health will have to be provided to the Commission 4 months after designation and made public at the latest a year later;
- Platforms will have to redesign their services, including their interfaces, recommender systems, terms and conditions, to mitigate these risks.

*More diligent content moderation, less disinformation:*

- Platforms and search engines need to take measures to address risks linked to the dissemination of illegal content online and to negative effects on freedom of expression and information;
- Platforms need to have clear terms and conditions and enforce them diligently and non-arbitrarily;
- Platforms need to have a mechanism for users to flag illegal content and act upon notifications expeditiously;
- Platforms need to analyse their specific risks, and put in place mitigation measures – for instance, to address the spread of disinformation and inauthentic use of their service.

### *More transparency and accountability:*

- Platforms need to ensure that their risk assessments and their compliance with all the DSA obligations are externally and independently audited;
- They will have to give access to publicly available data to researchers; later on, a special mechanism for vetted researchers will be established;
- They will need to publish repositories of all the ads served on their interface;
- Platforms need to publish transparency reports on content moderation decisions and risk management.

By 4 months after notification of the designated decisions, the designated platforms and search engines need to adapt their systems, resources, and processes for compliance, set up an independent system of compliance and carry out, and report to the Commission, their first annual risk assessment.

### *Risk assessment*

Platforms will have to identify, analyse and mitigate a wide array of systemic risks ranging from how illegal content and disinformation can be amplified on their services, to the impact on the freedom of expression and media freedom.

Similarly, specific risks around gender-based violence online and the protection of minors online and their mental health must be assessed and mitigated.

The risk mitigation plans of designated platforms and search engines will be subject to an independent audit and oversight by the Commission.

To read more:

[https://ec.europa.eu/commission/presscorner/detail/en/ip\\_23\\_2413](https://ec.europa.eu/commission/presscorner/detail/en/ip_23_2413)

## Meta's Q1 2023 Security Reports: Protecting People and Businesses

Guy Rosen, Chief Information Security Officer



### *Takeaways*

1. As part of our quarterly integrity reporting, we're sharing Q1 updates on our work to combat a range of threats.
2. We detected and took action against malware campaigns targeting people and businesses online, shared our findings with other technology companies and rolled out new security features to help protect people.
3. We took actions against nine separate adversarial networks around the world for engaging in covert influence operations and cyber espionage, and shared our threat insights with industry peers, researchers and governments.

We know that safety and security are top of mind for people using our apps, including businesses and advertisers. Today, as part of our quarterly integrity reporting, we're sharing updates on our work to combat a range of threats, including covert influence operations, cyber espionage and malware campaigns.

In my first year as Meta's chief information security officer, my focus has been bringing together teams working on integrity, security, support, and operations so that we can work together in the most effective way possible.

Each of these efforts has been ongoing for many years, and a key focus for us has been sharing progress, bringing in outside experts and working with other companies to tackle industry-wide threats.

It's been more than 10 years since our bug bounty program began working with the security research community, 10 years since we first published transparency reports on government data requests, over five years since we started sharing takedowns of covert influence operations and five years since we published our first community standards enforcement report.

We've learned a lot through this work, including the importance of sharing both qualitative and quantitative insights into our integrity work. And it's been encouraging to see our peers join us in expanding their trust and safety reporting. We're committed to continuing these efforts, and today's updates are good examples of this work.



## *Countering Malware Campaigns Across the Internet*

My teams track and take action against hundreds of threat actors around the world, including malware campaigns. Here are a few things that stood out from our latest malware work.

*First*, our threat research has shown time and again that malware operators, just like spammers, are very attuned to what's trendy at any given moment. They latch onto hot-button issues and popular topics to get people's attention. The latest wave of malware campaigns have taken notice of generative AI technology that's captured people's imagination and excitement.

Since March alone, our security analysts have found around 10 malware families posing as ChatGPT and similar tools to compromise accounts across the internet. For example, we've seen threat actors create malicious browser extensions available in official web stores that claim to offer ChatGPT-related tools.

In fact, some of these malicious extensions did include working ChatGPT functionality alongside the malware. This was likely to avoid suspicion from the stores and from users.

We've detected and blocked over 1,000 of these unique malicious URLs from being shared on our apps, and reported them to our industry peers at file-sharing services where malware was hosted so they, too, can take appropriate action.

This is not unique to the generative AI space. As an industry, we've seen this across other topics popular in their time, such as crypto scams fueled by the interest in digital currency. The generative AI space is rapidly evolving and bad actors know it, so we should all be vigilant.

*Second*, we've seen that our and industry's efforts are forcing threat actors to rapidly evolve their tactics in attempts to evade detection and enable persistence.

One way they do this is by spreading across as many platforms as they can to protect against enforcement by any one service. For example, we've seen malware families leveraging services like ours and LinkedIn, browsers like Chrome, Edge, Brave and Firefox, link shorteners, file-hosting services like Dropbox and Mega, and more. When they get caught, they mix in more services including smaller ones that help them disguise the ultimate destination of links.

Another example is when some malware families masquerading as ChatGPT apps switched their lures to other popular themes like Google's Bard or TikTok marketing support, in response to detection.

These changes are likely an attempt by threat actors to ensure that any one service has only limited visibility into the entire operation. When bad actors count on us to work in silos while they target people far and wide across the internet, we need to work together as an industry to protect people.

That's why we designed our threat research to help us scale our security work in a number of ways — it disrupts malicious operations on our platform and helps inform our industry's defenses against threats that rarely target one platform. The insights we gain from this research help drive our continuous product development to protect people and businesses.

In the months and years ahead, we'll continue to highlight how these malicious campaigns operate, share threat indicators with our industry peers and roll out new protections to address new tactics. For instance, we're launching a new support flow for businesses impacted by malware. Read more about our work to help businesses stay safe on our apps.

### *Disrupting Cyber Espionage and Covert Influence Operations*

In today's Q1 Adversarial Threat report, we shared findings about nine adversarial networks we took action against for various security violations.

Six of these networks engaged in coordinated inauthentic behavior (CIB) that originated in the US, Venezuela, Iran, China, Georgia, Burkina Faso and Togo, and primarily targeted people outside of their countries. We removed the majority of these networks before they were able to build authentic audiences.

Nearly all of them ran fictitious entities — news media organizations, hacktivist groups and NGOs — across the internet, including on Facebook, Twitter, Telegram, YouTube, Medium, TikTok, Blogspot, Reddit, WordPress, Freelancer[.]com, hacking forums and their own websites.

Half of these operations were linked to private entities including an IT company in China, a US marketing firm and a political marketing consultancy in the Central African Republic.

We also disrupted three cyber espionage operations in South Asia, including an advanced persistent threat (APT) group we attributed to state-linked actors in Pakistan, a threat actor in India known in the security

industry as Patchwork APT, and the threat group known as Bahamut APT in South Asia.

Each of these APTs relied heavily on social engineering to trick people into clicking on malicious links, downloading malware or sharing personal information across the internet.

This investment in social engineering meant that these threat actors did not have to invest as much on the malware side. In fact, for at least two of these operations, we saw a reduction in the malicious capabilities in their apps, likely to ensure they can be published in official app stores.

In response to the security community continuing to disrupt these malicious efforts, we've seen these APTs to be forced to set up new infrastructure, change tactics and invest more in hiding and diversifying their operations, which likely degraded their operations. Read more about this threat research in our Q1 Adversarial Threat Report (at Number 10, below).

To read more: <https://about.fb.com/news/2023/05/metasploit-2023-security-reports/>

## Quarterly Adversarial Threat Report



Our public threat reporting began about six years ago when we first shared our findings about [coordinated inauthentic behavior \(CIB\)](#) by a Russian influence operation.

Since then, we have expanded our ability to respond to a wider range of adversarial behaviors as global threats have continued to evolve.

To provide a more comprehensive view into the risks we tackle, we've also expanded our regular threat reports to include cyber espionage and other emerging threats — all in one place, as part of the quarterly reporting series.

In addition to sharing our analysis and threat research, we're also publishing threat indicators to contribute to the efforts by the security community to detect and counter malicious activity elsewhere on the internet (See Appendix).

We expect the make-up of these reports to continue to evolve in response to the changes we see in the threat environment and as we expand to cover new areas of our Trust & Safety work.

This report is not meant to reflect the entirety of our security enforcements, but to share notable trends and investigations to help inform our community's understanding of the evolving security threats we see.

We welcome ideas from our peers across the defender community to help make these reports more informative, and we'll adjust as we learn from feedback.

For a quantitative view into our Community Standards' enforcement, including content-based actions we've taken at scale and our broader integrity work, please visit Meta's Transparency Center here: <https://transparency.fb.com/data/>

### *Summary of our findings*

1. Our quarterly threat report provides a view into the risks we see across multiple adversarial behaviors including CIB and cyber espionage.
2. We took action against three cyber espionage operations in South Asia. One was linked to a group of hackers known in the security industry as

Bahamut APT (advanced persistent threat), the other to the group known as Patchwork APT and one to the state-linked actors in Pakistan. Here is what stood out from our threat research (See Section 1 for details):

**2a. Diversifying social engineering efforts:** These APTs relied heavily on social engineering and invested in making some of their fake accounts into more varied and elaborate fictitious personas with backstops across the internet so they can withstand scrutiny by their targets, platforms and researchers.

While we saw them continue using traditional lures like women looking for a romantic connection, they also developed personas posing as recruiters, journalists or military personnel.

**2b. Continued reliance on low-sophistication malware:** This investment in social engineering to trick people into clicking on malicious links or sharing sensitive information means that threat actors did not have to invest as much on the malware side.

In fact, our investigations showed that cheaper, low-sophistication malware can be effective in targeting people when used together with social engineering. For at least two of these operations, we observed a reduction in the malicious capabilities in their apps, likely to ensure they can be published in official app stores.

**2c. Impact of public disruptions and threat reporting:** As the security community continued to disrupt these APTs, they have been forced to set up new infrastructure, change tactics, and invest more in hiding and diversifying their operations in order to persist, which likely degraded their operations.

3. In our Q1 Adversarial Threat report, we're sharing findings about six separate covert influence operations we took down for violating our policy against CIB. They originated in the United States and Venezuela, Iran, China, Georgia, Burkina Faso and Togo.

More than half of them targeted audiences outside of their countries. We removed the majority of these networks before they were able to build authentic audiences. Here is what stood out from our CIB threat research (See Section 2 for details):

**4. Creating fictitious entities across the internet:** In an attempt to build credibility, nearly all of these operations invested in creating fictitious entities across the internet, including news media organizations, hacktivist groups, and NGOs.

They operated on many platforms, including on Facebook, Twitter, Telegram, YouTube, Medium, TikTok, Blogspot, Reddit, Wordpress, freelancer[.]com, hacking forums and their own websites.

**5. Fake hacktivists from Iran:** The operation from Iran posted claims of having hacked organizations in Israel, Bahrain and France, including news media, logistics and transport companies, educational institutions, an airport, a dating service and a government institution.

Some of these individual claims have been reported by the press in these countries, but we cannot confirm if any of them are credible. This is not the first time an Iran-origin operation claimed to have hacked government systems; a similar claim was promoted by another CIB network we removed ahead of the US 2020 election.

**6. For-hire operations:** As we called out in our past reporting, we continue to see for-hire organizations behind covert influence operations globally, with half of the operations in this report attributed to private entities. This included an IT company in China, a marketing firm in the United States and a political marketing consultancy in the Central African Republic.

**7. The evolution of China-origin operations:** Finally, this report brings the total of the China-origin CIB networks we removed since 2017 to six, with half of them reported in the last seven months.


These latest takedowns signal a shift in the nature of the China-based CIB activity we've found with new threat actors, novel geographic targeting, and new adversarial tactics. Yet, we continue to find and remove them before they are able to build their audience.

These latest networks experimented with a range of tactics we haven't seen in China-based operations before (though we've observed them elsewhere over the years, including in operations linked to troll farms, and marketing and PR firms).

The latest behaviors included creating a front media company in the West, hiring freelance writers around the world, offering to recruit protesters, and co-opting an NGO in Africa.


**M MOVIE DATE**      [HOME](#)   [ABOUT](#)   [WORKING](#)   [REVIEWS](#)   [CONTACT US](#)

# Host a **MOVIE DATE** with friends while social distancing




Movie Date is an entertainment app that provides you the comfort of cinema at home absolutely free of charge!

[DOWNLOAD](#)

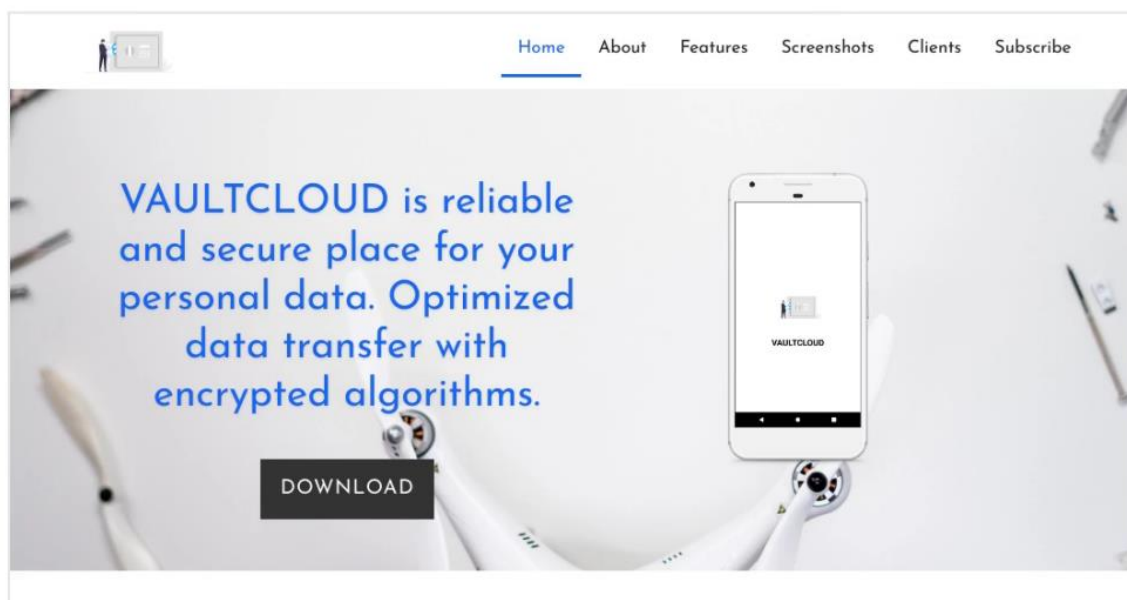
 **CV**  
**WRITER**

[DOWNLOAD](#)   [ABOUT US](#)   [OUR CLIENTS](#)   [OUR WORK](#)   [CONTACT US](#)



## Upgrade Your CV Upgrade Your Career.

• • •



## Coordinated inauthentic behavior (CIB)

**We view CIB** as coordinated efforts to manipulate public debate for a strategic goal, in which fake accounts are central to the operation. In each case, people coordinate with one another and use fake accounts to mislead others about who they are and what they are doing. When we investigate and remove these operations, we focus on behavior rather than content — no matter who's behind them, what they post or whether they're foreign or domestic.

**Continuous CIB enforcement:** We monitor for efforts to come back by the networks we previously removed. Using both automated and manual detection, we continuously remove accounts and Pages connected to networks we took down in the past.

The report: <https://about.fb.com/wp-content/uploads/2023/05/Meta-Quarterly-Adversarial-Threat-Report-Q1-2023.pdf>



## Disclaimer

The Association tries to enhance public access to information about risk and compliance management.

Our goal is to keep this information timely and accurate. If errors are brought to our attention, we will try to correct them.

This information:

- is of a general nature only and is not intended to address the specific circumstances of any particular individual or entity;
- should not be relied on in the particular context of enforcement or similar regulatory action;
- is not necessarily comprehensive, complete, or up to date;
- is sometimes linked to external sites over which the Association has no control and for which the Association assumes no responsibility;
- is not professional or legal advice (if you need specific advice, you should always consult a suitably qualified professional);
- is in no way constitutive of an interpretative document;
- does not prejudge the position that the relevant authorities might decide to take on the same matters if developments, including Court rulings, were to lead it to revise some of the views expressed here;
- does not prejudge the interpretation that the Courts might place on the matters at issue.

Please note that it cannot be guaranteed that these information and documents exactly reproduce officially adopted texts.

It is our goal to minimize disruption caused by technical errors. However, some data or information may have been created or structured in files or formats that are not error-free and we cannot guarantee that our service will not be interrupted or otherwise affected by such problems.

The Association accepts no responsibility with regard to such problems incurred as a result of using this site or any linked external sites.

## Sarbanes-Oxley Compliance Professionals Association (SOXCPA)

Welcome to the Sarbanes-Oxley Compliance Professionals Association (SOXCPA), the largest Association of Sarbanes-Oxley professionals in the world.

Join us. Stay current. Read our monthly newsletter with news, alerts, challenges and opportunities. Get certified and provide independent evidence that you are a Sarbanes-Oxley expert.

You can explore what we offer to our members:

1. Membership - Become a standard, premium or lifetime member.

You may visit: [https://www.sarbanes-oxley-association.com/How\\_to\\_become\\_member.htm](https://www.sarbanes-oxley-association.com/How_to_become_member.htm)

2. Monthly Updates - Visit the Reading Room of the SOXCPA at: [https://www.sarbanes-oxley-association.com/Reading\\_Room.htm](https://www.sarbanes-oxley-association.com/Reading_Room.htm)

3. Training and Certification - You may visit: [https://www.sarbanes-oxley-association.com/Distance\\_Learning\\_and\\_Certification.htm](https://www.sarbanes-oxley-association.com/Distance_Learning_and_Certification.htm)

[https://www.sarbanes-oxley-association.com/CJSOXE\\_Distance\\_Learning\\_and\\_Certification.htm](https://www.sarbanes-oxley-association.com/CJSOXE_Distance_Learning_and_Certification.htm)

For instructor-led training, you may contact us. We tailor all programs to meet specific requirements.