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

Sarbanes Oxley News, November 2022

Dear members and friends,

The Public Company Accounting Oversight Board (PCAOB) issued for public comment a proposed standard that the Board believes would, if adopted, lead registered public accounting firms to significantly improve their quality control (QC) systems. The Board requests public comment on the proposal by February 1, 2023.

"Quality control systems set the foundation for how firms perform their audits, so making sure those systems are effective in today's economy is essential to protecting investors," said PCAOB Chair Erica Y. Williams.

Current QC standards were developed and issued by the American Institute of Certified Public Accountants before the PCAOB was established in 2002. The auditing environment has changed significantly since that time, so QC is a pressing area for modernization. The Board has carefully considered the potential for improvements to PCAOB QC standards, including through discussion with the PCAOB's former advisory groups.

In December 2019, the Board issued a concept release that generated comment letters from firms, investors, investor advocates, academics, trade groups, and others. This input, along with the PCAOB's own quantitative and qualitative economic analysis, helped to inform the proposal.

The proposed standard, if adopted, would replace the current QC standards in their entirety and would provide a framework for a firm's QC system that is grounded in proactively identifying and managing risks to quality, with a feedback loop from ongoing monitoring and remediation designed to drive continuous improvement.

Among other provisions, the proposal would foster a more structured approach where a firm would annually evaluate its QC system and report the results of its evaluation on new Form QC.

Detailed questions are included throughout the proposal, and commenters are encouraged to:

(1) comment on any or all topics,

(2) respond to any or all questions,

(3) provide feedback in areas not covered by specific questions, and

(4) provide any evidence that informs commenters' views.

The proposal would:

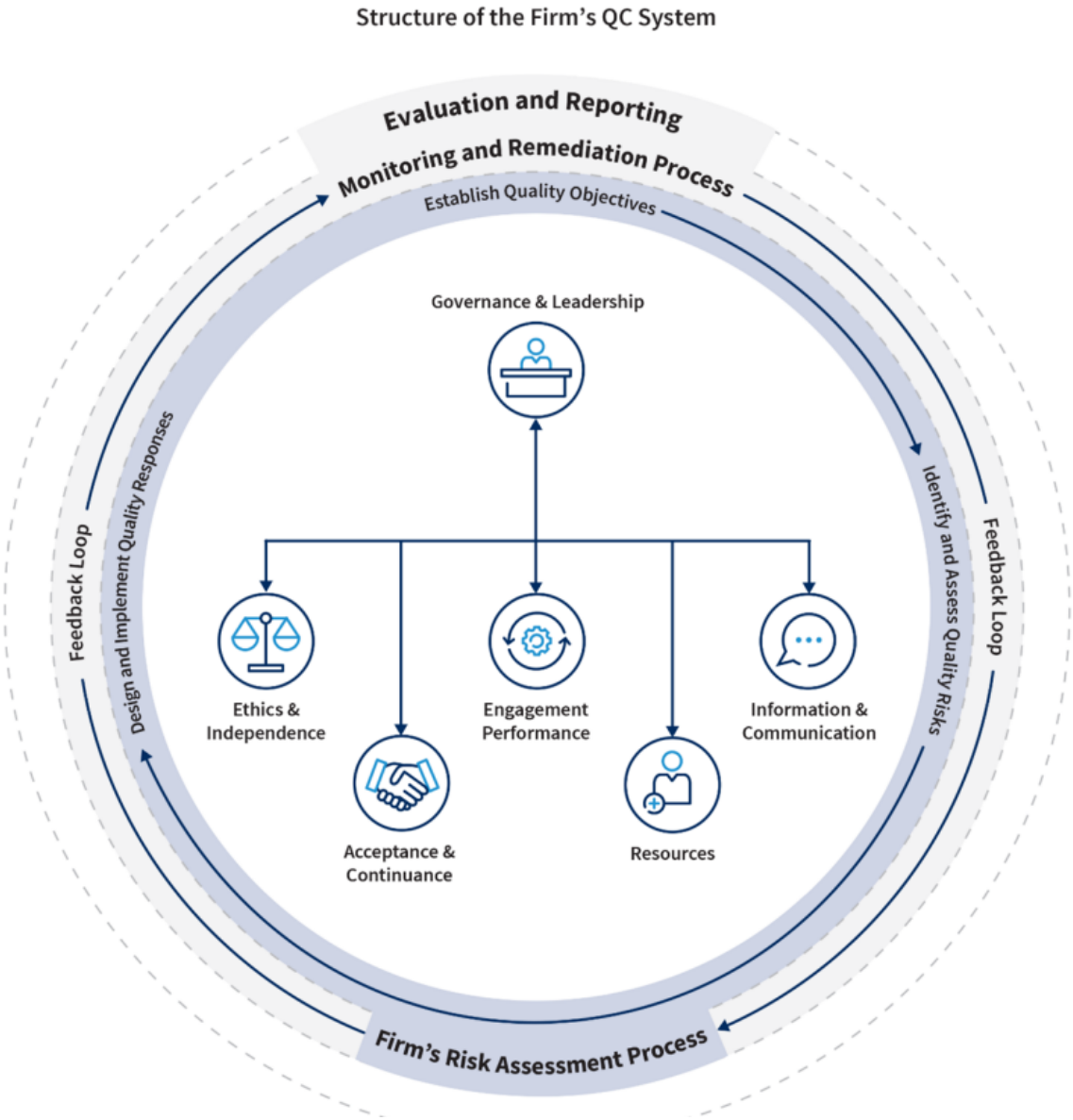
(1) supersede current PCAOB quality control standards with an integrated, risk-based standard, QC 1000, A Firm's System of Quality Control, that would apply to all registered public accounting firms;

(2) create reporting requirements on quality control matters and a new, nonpublic reporting form, Form QC;

(3) expand the auditor's responsibility to respond to deficiencies on completed engagements under an amended and retitled AS 2901, Responding to Engagement Deficiencies After Issuance of the Audit Report, and related amendments to our attestation standards for broker-dealer engagements;

(4) supersede our existing standard ET 102 with a new standard, EI 1000, Integrity and Objectivity, to better align our ethics requirements with the scope, approach, and terminology of QC 1000; and

(5) make additional changes to PCAOB standards, rules, and forms.



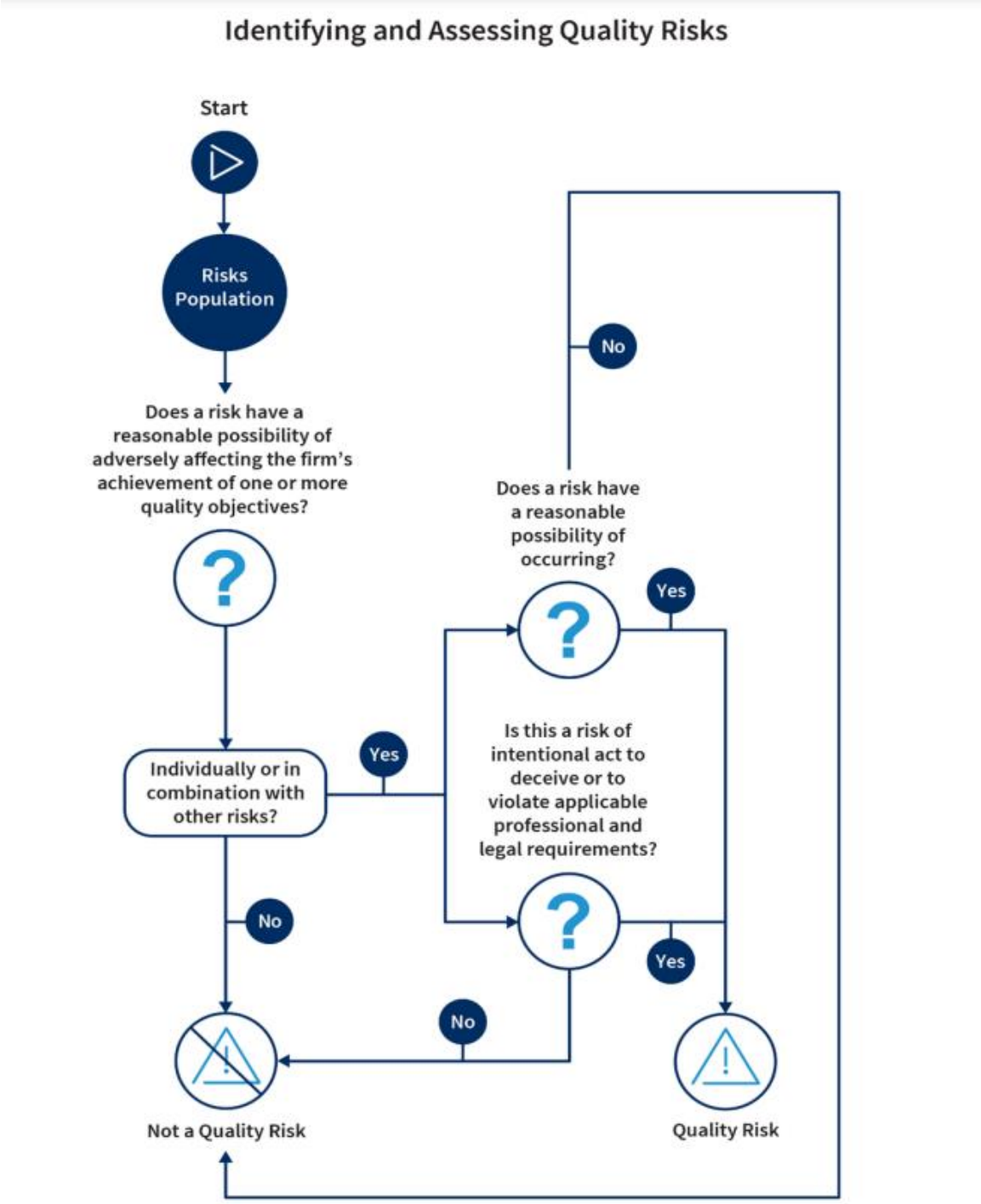
The Sarbanes-Oxley Act of 2002, as amended ("Sarbanes-Oxley"), requires the Board to establish certain professional standards, including quality control standards, to be used by registered public accounting firms in the preparation and issuance of audit reports for issuers, brokers, and dealers.

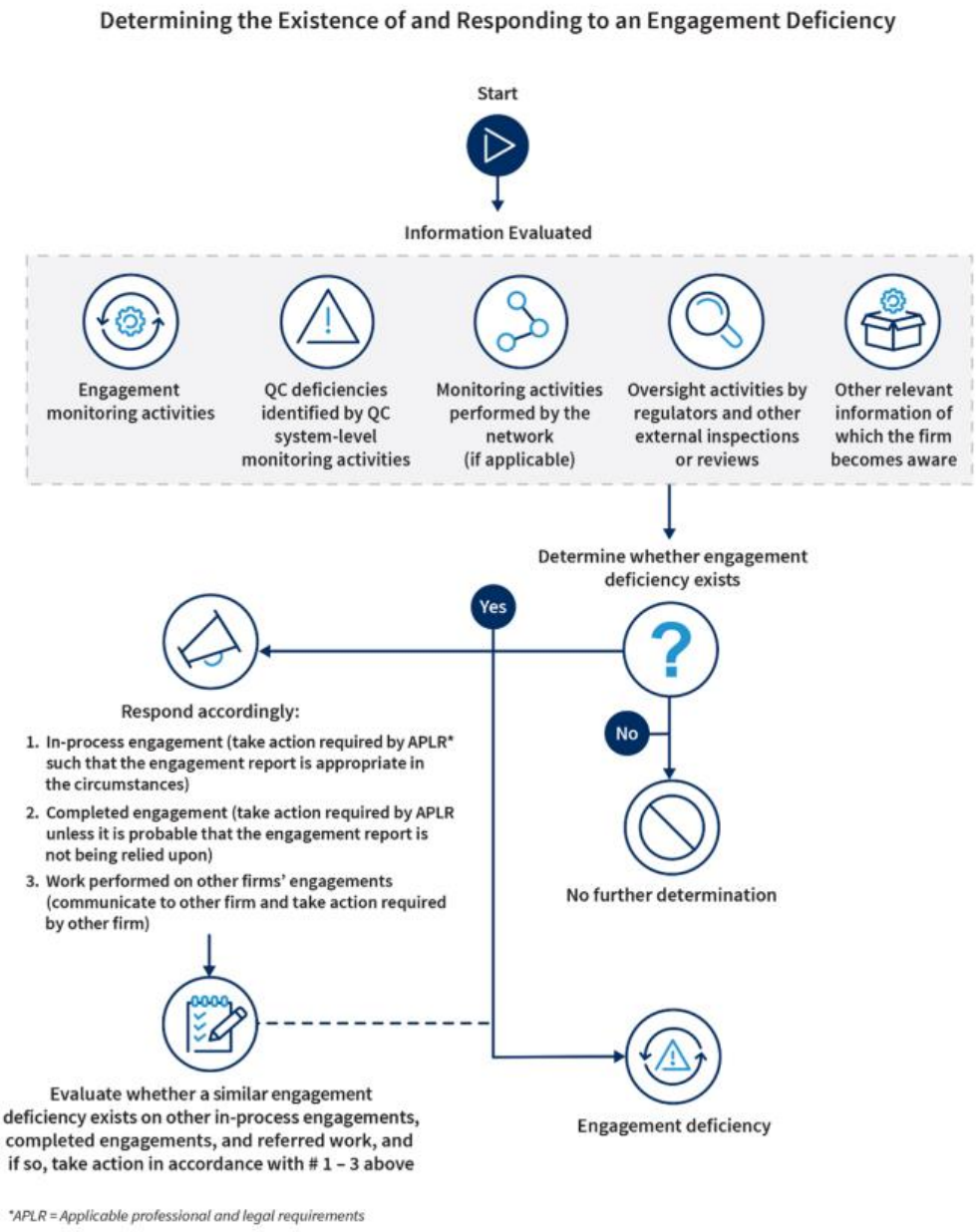
Furthermore, Sarbanes-Oxley requires the PCAOB's QC standards to address:

• Monitoring of professional ethics and independence from issuers, brokers, and dealers on behalf of which the firm issues audit reports;

• Consultation within the firm on accounting and auditing questions; • Supervision of audit work;

- Hiring, professional development, and advancement of personnel;
- Acceptance and continuation of engagements;
- Internal inspection; and
- Such other requirements as the Board may prescribe.





To read more: https://pcaob-assets.azureedge.net/pcaob-dev/docs/default-source/rulemaking/docket046/2022-006-qc.pdf?sfvrsn=b89546e2_2

Remarks at PCAOB Conference on Auditing and Capital Markets

Erica Y. Williams, Chair, Public Company Accounting Oversight Board

Thank you, Michael [Gurbutt]. And congratulations to you and your colleagues in the Office of Economic and Risk Analysis (OERA) on putting together another great program for our guests today and tomorrow.

To our guests: thank you for being here and for the important work you do every day.

Before we begin, I want to issue the standard disclaimer that the views that I express here are my own and are not necessarily the views of the other Board Members or the PCAOB staff.

This summer marked 20 years since Congress created the PCAOB.

In the early 2000s major accounting scandals from Enron to WorldCom rocked our markets. Corporations were lying about their earnings and hiding their debt. And when it all came crashing down, investors lost billions, workers lost jobs and retirement savings, and trust in our markets was eroded.

So, Congress acted. Led by Senator Paul Sarbanes and Representative Michael Oxley, both parties came together to pass the law that we affectionally refer to as “SOX” with near unanimous bipartisan support.

The world has changed over the last 20 years. And, like all of you, I am looking forward to learning more from our distinguished speakers about what those changes mean for the future of auditing.

But one thing that has not changed is PCAOB’s mission to protect investors.

Protecting investors prompted our creation 20 years ago, and protecting investors is what continues to drive us forward today.

Reflecting on SOX in the years after it was signed, Senator Sarbanes warned: “When things get better, companies tend to forget what happened or how serious it was at the time. Trying to maintain high standards is a difficult job.”

The PCAOB is up to the task. But we need your help.

We depend on Michael and his incredible team for high-quality, evidence-based analysis that helps us ensure that our decision-making is infused with the best available data, information, and research. And they depend on you for expanding our knowledge and understanding of the economic impact of auditing and audit regulation on our capital markets.

As Michael mentioned, we have identified three key goals:

- Modernizing our standards,

- Enhancing inspections, and

- Strengthening enforcement.

High-quality economic analysis plays a critical role in each one.

Goal number one: Modernizing our standards.

High standards are the foundation for quality audits. That's why earlier this year, the Board announced one of the most ambitious standard-setting agendas in the PCAOB's history.

Less than a year into this Board's term, we are working actively to update more than 30 standards within 10 standard-setting projects.

And every single one of them requires economic analysis to ensure we get it right.

Our evidence-based approach starts with understanding the current environment – asking what is needed to ensure investors are best protected and what changes may be needed to achieve that goal.

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. Our current short-term and mid-term projects will address more than half of them.

We know the world has changed since 2003. Robust economic analysis will help us understand those changes, so we can adapt our standards to keep up with developments in auditing and the capital markets.

Economic analysis also helps us see around the corner and anticipate a standard's impact. Among other things, we review a standard in terms of its likely economic benefits, costs, competitive effects, and potential unintended consequences.

But simply anticipating impact isn't the end of the story.

After a standard is approved, we often continue to examine its impact through our post-implementation review process by analyzing public and non-public data.

We also conduct surveys and interviews to collect quantitative and qualitative information about the impact of standards on key stakeholders, such as investors, audit committees, and audit firms.

And, of course, we rely on researchers like you. Reviewing the work of academics outside the PCAOB is critical to shaping our understanding of the audit and its role in supporting trust in our capital markets.

If our evidence-based approach sounds like a lot of work, I can promise you that it certainly is. And I want to thank the dedicated staff who carry this work out every day.

Their work has proven its worth in helping us to understand whether our standards are effective once they are applied by the firms.

Let's take a specific example: critical audit matters, or CAMs, where auditors communicate to investors certain matters arising from an audit of the financial statements that involved especially challenging, subjective, or complex auditor judgment.

In 2017, the PCAOB adopted a new CAMs standard, bringing the most significant changes to the auditor's report in decades.

The centerpiece of the new standard, of course, was the requirement for the auditor to determine and communicate CAMs in the auditor's report.

During the comment process prior to adoption, we heard concerns and questions about the potential impact of CAMs.

Some people wondered, for example:

- How would identifying and communicating CAMs affect the workload of audit engagement teams?

- Would CAMs lead to reduced communication between audit committees and auditors?

- Would investors find CAMs useful?

When the PCAOB adopted the standard, the team studied the best available evidence and acknowledged the potential impact on workloads. The PCAOB's view was that the standard was scalable, and the PCAOB expressed doubt that CAMs would chill communications. The PCAOB also described several types of anticipated direct and indirect benefits to investors of CAMs.

But our team was not content with just resting on these predictions. They wanted to know – were they right? What were the benefits and costs of the standard, and did any of the unintended consequences play out?

And so, our economists got to work.

They conducted quantitative and qualitative analyses and reported out initial findings in an interim report released two years ago, with a follow-up report that we plan to release in the coming months.

One of the findings in their 2020 analysis was that individual audit engagement teams spent, on average, 1% of total audit hours identifying, developing, and communicating CAMs.

Additionally, they found no evidence of CAMs inhibiting or chilling the communications between the auditors and audit committees. In fact, less than 2% of the 900 audit engagement partners surveyed reported that CAMs constrained communications with the audit committee, while 41% reported that CAMs enhanced them.

As for investors, our economists found that investor awareness of CAMs was still a work in progress. But they also observed that some investors were using CAMs — and finding the information beneficial.

And benefitting investors is what this project — and all our standard-setting projects — are all about.

Of course, standard setting is just one pillar of the PCAOB's oversight. Another critical component of our work is inspections. That's why our second major strategic goal is to enhance our inspections.
Our team likes to say that "the sun never sets on PCAOB inspections," because each year, the PCAOB inspects approximately 250 audit firms and reviews 900 audits from across the globe.

This reach means that our inspections team must constantly adjust to stay responsive to new and emerging risks and issues around the world – whether it's SPACs and de-SPAC transactions, cryptocurrencies, or how

firms are addressing the effects of supply chain disruptions and rising costs.

To stay responsive, our inspectors need data, analysis, and high-quality economic research.

So, Michael and his team help our inspectors with that. They collect data from the information provided to us by firms, from third-party data providers, and from internal sources, and aggregate and analyze that data to help identify areas of risk and point our inspectors in the right direction.

They also develop economic models to further guide how we direct our inspections resources. For example, our economists have developed a portfolio of models that predict the probability of future financial restatements, which, as you know, can have a huge impact on investors.

This portfolio includes models focused on size, as well as models for specific industries and audit firms.

Our modeling team economists use academic research to identify potential inputs for their models and to guide their modeling design. They stay up to date with all the latest research you produce, which helps us improve our accuracy of our models over time.

For our inspectors, all this work makes a big difference. It helps inspectors adjust their inspections approach, whether that's focusing their selections on relevant risks or making changes to the way they look at crucial concepts, such as auditor materiality judgments.

That brings me to our third key strategic goal: strengthening enforcement.

This Board is approaching enforcement with a renewed vigilance.

We are rethinking how we identify cases, the types of cases we pursue, and the sanctions we impose.

We've more than doubled our average penalties against individuals compared to the last five years. This includes the largest civil money penalty against an individual in PCAOB history, which we announced earlier this week.

In the past five years, the PCAOB assessed penalties against individuals less than half of the time and firms only about 86% of the time. This year it's 100%.

We intend to use every tool in our enforcement toolbox.

And one of those tools is high-quality research and data analysis.

Specifically, our enforcement team works with OERA's Risk Analysis team to develop a list of risk factors to focus on.

Using these risk factors and other criteria, our analysts develop lists of audit engagements that our enforcement team can use to find the most likely enforcement matters, ensuring those that fail to comply with our standards and laws are identified and action is taken to promote audit quality and investor protection.

Examples of the screening criteria used to develop these lists include significant corporate events, auditor events, or characteristics of the issuer, among others.

Economic research is critical to achieving our mission and keeping investors protected.

And we can't do that without you.

Michael mentioned our speaker series and our fellowship program, which allows the PCAOB to hire academics for a one-year appointment to work on staff projects and to perform original research using our non-public data.

I encourage you to get involved. We'd love to work with you.

We are also fortunate to receive the benefit of the insights and knowledge of academics participating on our two new advisory groups: the Investor Advisory Group and the Standards and Emerging Issues Advisory Group. Both groups bring together extraordinary experts from across the world of auditing and financial reporting.

Before I close, I want to ask one favor of you: help us engage the next generation of auditors and public servants.

As academics, whether in the classroom or the research field, you have an outstanding platform to reach the best and brightest minds – young people who are on the cusp of their careers.

When I was practicing law, I noticed there was not enough of a pipeline of diverse law students going into certain areas of securities law. So, I went to the Dean of Howard Law School and offered to create a class on investment management.

She agreed, but only after telling me I had to come up with a catchy title, or no one would sign up. So, we called it "More Money, More Problems:

Regulating Private Equity and Hedge Funds." And I am proud to report our class was full all four years I taught it.

I am still in touch with many of those students, and many of them chose to make careers in securities law.

So, I have experienced just a tiny fraction of the influence you all have on the next generation of young professionals, and it is powerful.

Your students and research assistants are the future of accounting and auditing. Through them, we will continue to improve audit quality, to uphold the integrity of our markets, and to protect investors.

To do that, we need to bring more young people into the field and expand the types of young people who see accounting as a path for them.

At the PCAOB we are working to do our part through our scholarship program. This academic year, we awarded 250 students from U.S. colleges and universities with $10,000 each to pursue accounting degrees.

More than half of the scholarships in the last five years went to diverse applicants. These scholarships help make careers in auditing possible for the best and brightest students, no matter their backgrounds.

But we must do more. Just last week, the Board heard an important presentation about diversity from one of the academics on the advisory panels I mentioned: Jennifer Joe of the University of Delaware.

And we want to hear from you too.

Bring us your ideas for ways the PCAOB can help build a strong, diverse pipeline of students choosing to make a career in accounting and help protect the next generation of investors.

Thank you very much for joining us today, and for all the work you do to help inform the work of the PCAOB.

We look forward to our continued partnership. I wish you all a productive conference.

To read more: https://pcaobus.org/news-events/news-releases/news-release-detail/pcaob-chair-williams-delivers-remarks-at-pcaob-conference-on-auditing-and-capital-markets

Statement on the 2022-2026 Strategic Plan and the 2023 Budget Erica Y. Williams, Chair, PBAOB

I am pleased to support the 2022 – 2026 Strategic Plan and the 2023 Budget to support our mission to protect investors.

Our strategic plan is the product of extensive analysis and outreach.

We crafted the strategic plan with input from investors and other stakeholders, including our two newly established advisory groups – the Investor Advisory Group and Standards and Emerging Issues Advisory Group; perspectives from our staff of expert professionals; and the Securities and Exchange Commission. Then we issued a draft of the plan in August for public comment.

Thank you to everyone who has provided valuable input throughout this process. We have considered your thoughts, priorities, and ideas, and you will see many of them reflected in the plan.

Today we will move forward as we finalize the strategic plan guided by our mission to protect investors and further the public interest in the preparation of informative, accurate, and independent audit reports – the same mission Congress created the PCAOB to fulfill 20 years ago.

At the heart of our mission are the people who invest in public companies. Whether they are workers saving for retirement or parents saving to put their kids through college, people depend on a sound capital market system to build for their futures.

When we talk about protecting investors, this is who we mean. When we strive to uphold the highest standards in audit quality, it is with investors' families, savings, and futures in mind.

The people we serve are top of mind in everything we do at the PCAOB – including the four goals in this plan:

1. Modernizing our standards,
2. Enhancing our inspections,
3. Strengthening our enforcement, and
4. Improving our organizational effectiveness.

The goals outlined in this plan are as fundamental as they are ambitious and will lead us to achieve our core mission.

I look forward to working with my fellow Board Members and the talented staff at the PCAOB as we execute this strategic plan.

Of course, achieving these goals will require appropriate resources. The 2023 budget provides those resources to allow us to effectively use the tools Congress gave the PCAOB under the law to advance our investor protection mission.

This budget provides for an increase in staff in our Office of the Chief Auditor to assist in the execution of our ambitious standard-setting agenda. As we advance our mission, it is imperative that we evaluate the standards that were adopted by the Board in 2003 on an interim basis to determine if changes are necessary to keep up with developments in the auditing profession and the capital markets.

Stakeholder feedback is also a critical component of standard setting. Therefore, this budget includes funding necessary to engage with our advisory groups on a regular basis throughout the year.

As it pertains to inspections, the budget provides resources that will allow us to enhance our work to assess whether accounting firms are complying with applicable laws, rules, and standards.

As part of our inspection process, and consistent with our strategic plan, these resources will also assist us as we consider ways to provide greater transparency in our inspection reports, improve the timeliness of issuing such reports, identify opportunities to share useful guidance with the auditing profession, and increase our focus on firms' remediation efforts.

From an enforcement perspective, there must be accountability for those who violate laws, rules, and standards.

The budget provides us the resources to strengthen our enforcement program by using all the tools in our regulatory toolbox to conduct investigations and bring enforcement actions, to make sure the consequences are commensurate with the violations, to increase the transparency of our enforcement process where possible, and to work with other regulators as part of our enforcement efforts.

This budget also provides the resources necessary to improve the effectiveness of our organization. We would not be able to execute our mission without our talented staff, which is why this budget includes resources to enhance professional development, foster a diverse and inclusive workplace culture, and promote employee well-being.

With these resources, we will also look for ways to improve our coordination across the organization and engage in more efficient decision making.

In closing, I would like to thank everyone who played a role in developing our strategic plan and finalizing the 2023 budget. I would like to specifically thank my fellow Board Members and PCAOB staff for their collaboration on developing the strategic plan.

I would also like to recognize our new Chief Operations Officer, Jamey McNamara, our Chief Financial Officer, Holly Greaves, our Budget Officer, Jim Hearn, and the rest of their team – Yoss Missaghian, Alfredo Azocar, Marcia Saavedra, and Lorene Rosenberg – along with the leadership of each of the Divisions and Offices for their efforts on the budget.

Lastly, I would like to thank the Commissioners and staff at the Securities and Exchange Commission for their support and guidance.

You may visit: https://pcaobus.org/news-events/speeches/speech-detail/pcaob-chair-williams-statement-on-the-2022-2026-strategic-plan-and-the-2023-budget

https://pcaob-assets.azureedge.net/pcaob-dev/docs/default-source/about/administration/documents/strategic_plans/strategic-plan-2022-2026.pdf?sfvrsn=b2ec4b6a_2

Meeting Investor Demand for High Quality ESG Data

SEC Commissioner Jaime Lizárraga. the Future of ESG Data 2022, London, United Kingdom

Thank you, Peter, for that kind introduction. It is a pleasure to be here with you today. I look forward to learning from today's discussion, and appreciate the opportunity to participate in this important exchange of ideas and perspectives.

It's an exciting time for ESG. You are working in a dynamic, fast-growing sector of our capital markets that is grabbing headlines and continuing to generate enormous interest among investors and the general public.

You're directly involved with some of the most consequential scientific challenges of our time – from climate change, to artificial intelligence, to big data analytics.

As active participants in this space, your contributions and innovative ideas can enrich the conversation.

I'd like to share with you a snapshot of what's happening in the U.S. ESG has become a lively topic that has moved beyond strictly financial circles. Several states are making headlines for their push against ESG investing, while other states are proactive in their ESG investments.

Against this backdrop, the SEC issued three rule proposals that would each help facilitate comparable ESG disclosures and focus on ensuring statements made to investors are not false or misleading:

- Enhanced climate risk disclosures by issuers.
- Enhanced ESG disclosures by registered funds and investment advisers.
- Modernized rules governing ESG-related fund names.

The common thread that binds these proposals and that guides my work as Commissioner is ensuring investors receive the information they need to make the most informed investment decisions.

We are in the process of reviewing thousands of comments submitted. None of us yet know what the final versions of these rules will look like. We

continue to meet with stakeholders and to receive robust public feedback that informs our economic analysis.

To me, the SEC's disclosure framework is most effective when investors benefit from objective, quantitative metrics that provide the highest degree of comparability. I believe the proposed rules are a significant step forward in getting investors this information. I look forward to working to ensure that the final rules are as robust as possible.

The SEC proposed these rules prior to my swearing in. Had I been a Commissioner at the time, I would have voted in favor of them.

Which brings me to the first of the SEC's disclosure initiatives, on climate. Last year, for the first time, the U.S. Financial Stability Oversight Council identified climate change as an "emerging and increasing threat to U.S. financial stability."

A recent climate risk assessment from the Office of Management and Budget found that the U.S. government will need to spend an additional $25 billion to $128 billion annually for policies to mitigate climate-related financial risks. And, an analysis by the Network for Greening the Financial System estimated that, under current policy pathways, climate change could reduce U.S. GDP by 3 to 10 percent by the end of this century.

It is thus not surprising that there's been strong investor demand for climate-related disclosures. Investors with $130 trillion in assets under management have requested that companies disclose their climate risks. And 5,000-plus signatories to the UN Principles for Responsible Investment—a group with a core goal of helping investors protect their portfolios from climate-related risks—manage more than $121 trillion as of June 2022.

To read more: https://www.sec.gov/news/speech/lizarraga-speech-meeting-investor-demand-high-quality-esg-data

Progress Report on Climate-Related Disclosures

FSB FINANCIAL STABILITY BOARD

Executive summary

Work to strengthen the comparability, consistency and decision-usefulness of climate-related financial disclosures has moved forward rapidly over the past year.

A milestone has been the publication in March 2022 by the newly established International Sustainability Standards Board (ISSB) under the IFRS Foundation of two Exposure Draft standards, on general sustainability-related and climate-related disclosures, for public consultation with the aim to issue the final standards by early 2023, subject to feedback.

The timely issuance of a final global baseline climate reporting standard, ready for adoption across jurisdictions, is critical to provide decision-useful information to investors and other stakeholders on climate-related risks and opportunities.

Interoperability between the common global baseline and national and regional jurisdictionspecific requirements is essential.

The ISSB standards aim to establish a common global baseline that is interoperable with jurisdictions' frameworks through a building block approach that will drive more comparability and consistency on common climate disclosures across jurisdictions.

This will help avoid harmful fragmentation and unnecessary costs for preparers of disclosures. It can also ensure that disclosures by different firms are made on a common basis, and that users can compare and aggregate exposures across jurisdictions.

Alongside a global baseline reporting standard on climate, there is a growing recognition of the importance of global assurance standards to drive reliability of disclosures.

The International Auditing and Assurance Standards Board (IAASB) is working to develop a new sustainabilityrelated assurance framework and the International Ethics Standards Board for Accountants (IESBA) is developing sustainability-related ethics and independence standards, in both cases supported by IOSCO.

The FSB's July 2021 Report on Promoting Climate-Related Disclosures had reported that, already, a large majority of FSB jurisdictions had set or planned to set requirements, guidance or expectations for both financial institutions and non-financial corporates.

Since then most FSB jurisdictions have taken additional actions. In particular, several emerging market and developing economies (EMDEs) have taken active steps to incorporate climate-related information in mainstream disclosures.

More broadly, the Task Force on Climate-related Financial Disclosures (TCFD) Recommendations continue to be referenced as the common basis in most FSB jurisdictions, and many jurisdictions have set out specific metrics or guidance that provide additional detail beyond the recommendations.

Steps to improve the reliability of climate-related disclosures by firms are still at an early stage in most jurisdictions.

Looking ahead to the finalisation of ISSB standards, more than half of FSB jurisdictions state that they already have or are putting in place structures and processes to bring the ISSB standards into local requirements, once finalised.

Authorities note a number of challenges to be addressed in the implementation of the ISSB climate standard, such as consistency and comparability of disclosures across jurisdictions and across firms, data availability, proportionality, transition arrangements, and materiality.

This report highlights the findings of the 2022 TCFD Status Report that reports encouraging further progress in companies' disclosure practices across a wide range of types of firms including asset managers and asset owners as well as non-financial companies.

The percentage of companies disclosing information aligned with TCFD Recommendations and the amount of climate-relevant information in such disclosures has increased.

Even with this continued progress, the TCFD remains concerned that not enough companies are disclosing decisionuseful climate-related financial information, which may hinder investors, lenders, and insurance underwriters' efforts to appropriately assess and price climate-related risks. During the period until the ISSB global baseline standard is agreed and the implementation of that standard across jurisdictions begins to be monitored, there is a continuing need to maintain momentum by monitoring and reporting on progress in firms' climate disclosures.

The FSB therefore requests TCFD to prepare another progress report on firms' disclosures in 2023.

Table of Contents

To read more: https://www.fsb.org/wp-content/uploads/P131022-2.pdf

The U.S. Dollar and Central Bank Digital Currencies

Governor Christopher J. Waller, Board of Governors of the Federal Reserve System, at "Digital Currencies and National Security Tradeoffs," a symposium presented by the Harvard National Security Journal, Cambridge, Massachusetts.

Thank you, Professor Jackson, and thank you to the Harvard National Security Journal for the invitation to speak at this symposium.

As the payment system continues to evolve rapidly and the volume of digital assets continues to grow, it is critical to ensure that we keep both the benefits and risks of digital assets in the policy conversation, including the implications for America's role in the global economy and its place in the world.

My speech today focuses on exactly this issue and on an aspect of the digital asset world that is now the center of domestic and international attention—central bank digital currencies (CBDCs) and how they relate to the substantial international role of the U.S. dollar.

In January 2022, the Federal Reserve Board published a discussion paper on CBDCs to foster a broad and transparent public dialogue, including the potential benefits and risks of a U.S. CBDC.

To date, no decisions have been made by the Board on whether to move forward with a CBDC. But my views are well known.

As I have said before, I am highly skeptical of whether there is a compelling need for the Fed to create a digital currency.

I am not a national security expert. But one area where economics, CBDCs, and national security dovetail is the role of the dollar.

Advocates for creating a U.S. CBDC often assert how it is important to the long-term status of the dollar, particularly if other major jurisdictions adopt a CBDC. I disagree. As I will discuss, the underlying reasons for why the dollar is the dominant currency have little to do with technology, and I believe the introduction of a CBDC would not affect those underlying reasons.

I offer this view, again, in the spirit of dialogue, knowing how important these issues are, and I am very happy to engage in vigorous debate regarding my view. I remain open to the arguments advanced by others in this space.

The Role of the U.S. Dollar

After World War II and the creation of the Bretton Woods system, the U.S. dollar served as the central currency for the international monetary system.

Other countries agreed to keep the exchange value of their currencies fixed to the dollar, and eventually, countries came to settle international balances in dollars. That role has continued long after the Bretton Woods system dissolved.

By any measure, the dollar is the dominant global currency—for funding markets, foreign exchange transactions, and invoicing. It also is the world's predominant reserve currency.

In terms of the dollar's reserve currency status, 60 percent of disclosed official foreign reserves are held in dollars, far surpassing the shares of other currencies, with the majority of these dollar reserves held in safe and liquid U.S. Treasury securities.

Even in a world of largely floating exchange rates, many countries either implicitly or explicitly anchor their currencies to the dollar; together, these countries account for about half of world gross domestic product.

The dollar is by far the dominant currency for international trade. Apart from intra-European trade, dollar invoicing is used in more than three-fourths of global trade, including 96 percent of trade in the Americas.

Approximately 60 percent of international and foreign currency liabilities—international banking loans and deposits as well as international debt securities—are denominated in dollars.

And the dollar remains the single most widely used currency in foreign exchange transactions. Why does this matter to the United States?

As indicated in the Board's CBDC discussion paper, the dollar's international role lowers transaction and borrowing costs for U.S. households, businesses, and government.
It widens the pool of creditors and investors for U.S. investments. It may insulate the U.S. economy from shocks from abroad.

It also allows the United States to influence standards for the global monetary system.

The dollar's role doesn't only benefit the United States. The dollar serves as a safe, stable, and dependable form of money around the world. It serves as a reliable common denominator for global trade and a dependable settlement instrument for cross-border payments.

In the process, it reduces the cost of transferring capital and smooths the world of global payments, including for households and businesses outside of America.

For example, consider the dollar's role in foreign exchange markets. To make a foreign exchange transaction between two lightly traded currencies, it is often less expensive to trade the first currency with the dollar, and then to trade the dollar with the second currency, rather than to trade the two currencies directly.

The factors driving the dollar's role as a reserve currency are well researched and well demonstrated, including the depth and liquidity of U.S. financial markets, the size and openness of the U.S. economy, and international trust in U.S. institutions and the rule of law.

We must keep these factors in mind in any debate regarding the long-term importance of the dollar.

To read more:
https://www.federalreserve.gov/newsevents/speech/waller20221014a.htm

International Regulation of Crypto-asset Activities - Questions for consultation

FSB FINANCIAL STABILITY BOARD

The FSB is inviting comments on its proposed set of recommendations and on the questions set out below. Responses should be sent to fsb@fsb.org by 15 December 2022. Responses will be published on the FSB's website unless respondents expressly request otherwise.

General

1. Are the FSB's proposals sufficiently comprehensive and do they cover all crypto-asset activities that pose or potentially pose risks to financial stability?

2. Do you agree that the requirements set out in the CA Recommendations should apply to any type of crypto-asset activities, including stablecoins, whereas certain activities, in particular those undertaken by GSC, need to be subject to additional requirements?

3. Is the distinction between GSC and other types of crypto-assets sufficiently clear or should the FSB adopt a more granular categorisation of crypto-assets (if so, please explain)?

4. Do the CA Recommendations and the GSC Recommendations each address the relevant regulatory gaps and challenges that warrant multinational responses?

5. Are there any financial stability issues that remain unaddressed that should be covered in the recommendations?

Crypto-assets and markets (CA Recommendations)

FSB FINANCIAL STABILITY BOARD

International Regulation of Crypto-asset Activities

A proposed framework – questions for consultation

6. Does the report accurately characterise the functions and activities within the crypto-ecosystem that pose or may pose financial stability risk? What, if any, functions, or activities are missing or should be assessed differently?

(The report: https://www.fsb.org/wp-content/uploads/P111022-2.pdf)

7. Do you agree with the analysis of activity patterns and the associated potential risks?

8. Have the regulatory, supervisory and oversight issues and challenges as relate to financial stability been identified accurately? Are there other issues that warrant consideration at the international level?

9. Do you agree with the differentiated requirements on crypto-asset issuers and service providers in the proposed recommendations on risk management, data management and disclosure?

10. Should there be a more granular differentiation within the recommendations between different types of intermediaries or service providers in light of the risks they pose? If so, please explain.

Global stablecoins (GSC Recommendations)

11. Does the report provide an accurate analysis of recent market developments and existing stablecoins? What, if anything, is missing in the analysis or should be assessed differently?

FSB FINANCIAL STABILITY BOARD

Review of the FSB High-level Recommendations of the Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements

Consultative report

(The report: https://www.fsb.org/wp-content/uploads/P111022-4.pdf)
12. Are there other changes or additions to the recommendations that should be considered?

13. Do you have comments on the key design considerations for cross-border cooperation and information sharing arrangements presented in

Annex 2? Should Annex 2 be specific to GSCs, or could it be also applicable to crypto-asset activities other than GSCs?

14. Does the proposed template for common disclosure of reserve assets in Annex 3 identify the relevant information that needs to be disclosed to users and stakeholders?

15. Do you have comments on the elements that could be used to determine whether a stablecoin qualifies as a GSC presented in Annex 4?

To read more: https://www.fsb.org/2022/10/international-regulation-of-crypto-asset-activities-questions-for-consultation/

Executive Order On Enhancing Safeguards For United States Signals Intelligence Activities

THE WHITE HOUSE

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Purpose.

The United States collects signals intelligence so that its national security decisionmakers have access to the timely, accurate, and insightful information necessary to advance the national security interests of the United States and to protect its citizens and the citizens of its allies and partners from harm.

Signals intelligence capabilities are a major reason we have been able to adapt to a dynamic and challenging security environment, and the United States must preserve and continue to develop robust and technologically advanced signals intelligence capabilities to protect our security and that of our allies and partners.

At the same time, the United States recognizes that signals intelligence activities must take into account that all persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside, and that all persons have legitimate privacy interests in the handling of their personal information. Therefore, this order establishes safeguards for such signals intelligence activities.

Sec. 2. Signals Intelligence Activities.

(a) Principles. Signals intelligence activities shall be authorized and conducted consistent with the following principles:

(i) Signals intelligence activities shall be authorized by statute or by Executive Order, proclamation, or other Presidential directive and undertaken in accordance with the Constitution and with applicable statutes and Executive Orders, proclamations, and other Presidential directives.

(ii) Signals intelligence activities shall be subject to appropriate safeguards, which shall ensure that privacy and civil liberties are integral considerations in the planning and implementation of such activities so that:
(A) signals intelligence activities shall be conducted only following a determination, based on a reasonable assessment of all relevant factors, that the activities are necessary to advance a validated intelligence priority,

although signals intelligence does not have to be the sole means available or used for advancing aspects of the validated intelligence priority; and

(B) signals intelligence activities shall be conducted only to the extent and in a manner that is proportionate to the validated intelligence priority for which they have been authorized, with the aim of achieving a proper balance between the importance of the validated intelligence priority being advanced and the impact on the privacy and civil liberties of all persons, regardless of their nationality or wherever they might reside.

(iii) Signals intelligence activities shall be subjected to rigorous oversight in order to ensure that they comport with the principles identified above.

(b) Objectives. Signals intelligence collection activities shall be conducted in pursuit of legitimate objectives.

(i) Legitimate objectives.

(A) Signals intelligence collection activities shall be conducted only in pursuit of one or more of the following objectives:

(1) understanding or assessing the capabilities, intentions, or activities of a foreign government, a foreign military, a faction of a foreign nation, a foreign-based political organization, or an entity acting on behalf of or controlled by any such foreign government, military, faction, or political organization, in order to protect the national security of the United States and of its allies and partners;

(2) understanding or assessing the capabilities, intentions, or activities of foreign organizations, including international terrorist organizations, that pose a current or potential threat to the national security of the United States or of its allies or partners;

(3) understanding or assessing transnational threats that impact global security, including climate and other ecological change, public health risks, humanitarian threats, political instability, and geographic rivalry;

(4) protecting against foreign military capabilities and activities;

(5) protecting against terrorism, the taking of hostages, and the holding of individuals captive (including the identification, location, and rescue of hostages and captives) conducted by or on behalf of a foreign government, foreign organization, or foreign person;

(6) protecting against espionage, sabotage, assassination, or other intelligence activities conducted by, on behalf of, or with the assistance of a foreign government, foreign organization, or foreign person;

(7) protecting against threats from the development, possession, or proliferation of weapons of mass destruction or related technologies and threats conducted by, on behalf of, or with the assistance of a foreign government, foreign organization, or foreign person;

(8) protecting against cybersecurity threats created or exploited by, or malicious cyber activities conducted by or on behalf of, a foreign government, foreign organization, or foreign person;

(9) protecting against threats to the personnel of the United States or of its allies or partners;

(10) protecting against transnational criminal threats, including illicit finance and sanctions evasion related to one or more of the other objectives identified in subsection (b)(i) of this section;

(11) protecting the integrity of elections and political processes, government property, and United States infrastructure (both physical and electronic) from activities conducted by, on behalf of, or with the assistance of a foreign government, foreign organization, or foreign person; and

(12) advancing collection or operational capabilities or activities in order to further a legitimate objective identified in subsection (b)(i) of this section.

(B) The President may authorize updates to the list of objectives in light of new national security imperatives, such as new or heightened threats to the national security of the United States, for which the President determines that signals intelligence collection activities may be used. The Director of National Intelligence (Director) shall publicly release any updates to the list of objectives authorized by the President, unless the President determines that doing so would pose a risk to the national security of the United States.

(ii) Prohibited objectives.

(A) Signals intelligence collection activities shall not be conducted for the purpose of:

(1) suppressing or burdening criticism, dissent, or the free expression of ideas or political opinions by individuals or the press;

(2) suppressing or restricting legitimate privacy interests;

(3) suppressing or restricting a right to legal counsel; or

(4) disadvantaging persons based on their ethnicity, race, gender, gender identity, sexual orientation, or religion.

(B) It is not a legitimate objective to collect foreign private commercial information or trade secrets to afford a competitive advantage to United States companies and United States business sectors commercially. The collection of such information is authorized only to protect the national security of the United States or of its allies or partners.

(iii) Validation of signals intelligence collection priorities.

(A) Under section 102A of the National Security Act of 1947, as amended (50 U.S.C. 3024), the Director must establish priorities for the Intelligence Community to ensure the timely and effective collection of national intelligence, including national intelligence collected through signals intelligence. The Director does this through the National Intelligence Priorities Framework (NIPF), which the Director maintains and presents to the President, through the Assistant to the President for National Security Affairs, on a regular basis.

In order to ensure that signals intelligence collection activities are undertaken to advance legitimate objectives, before presenting the NIPF or any successor framework that identifies intelligence priorities to the President, the Director shall obtain from the Civil Liberties Protection Officer of the Office of the Director of National Intelligence (CLPO) an assessment as to whether, with regard to anticipated signals intelligence collection activities, each of the intelligence priorities identified in the NIPF or successor framework:

(1) advances one or more of the legitimate objectives set forth in subsection (b)(i) of this section;

(2) neither was designed nor is anticipated to result in signals intelligence collection in contravention of the prohibited objectives set forth in subsection (b)(ii) of this section; and

(3) was established after appropriate consideration for the privacy and civil liberties of all persons, regardless of their nationality or wherever they might reside.

(B) If the Director disagrees with any aspect of the CLPO's assessment with respect to any of the intelligence priorities identified in the NIPF or successor framework, the Director shall include the CLPO's assessment and the Director's views when presenting the NIPF to the President.

(c) Privacy and civil liberties safeguards. The following safeguards shall fulfill the principles contained in subsections (a)(ii) and (a)(iii) of this section.

(i) Collection of signals intelligence.

(A) The United States shall conduct signals intelligence collection activities only following a determination that a specific signals intelligence collection activity, based on a reasonable assessment of all relevant factors, is necessary to advance a validated intelligence priority, although signals intelligence does not have to be the sole means available or used for advancing aspects of the validated intelligence priority; it could be used, for example, to ensure alternative pathways for validation or for maintaining reliable access to the same information.

In determining whether to collect signals intelligence consistent with this principle, the United States — through an element of the Intelligence Community or through an interagency committee consisting in whole or in part of the heads of elements of the Intelligence Community, the heads of departments containing such elements, or their designees — shall consider the availability, feasibility, and appropriateness of other less intrusive sources and methods for collecting the information necessary to advance a validated intelligence priority, including from diplomatic and public sources, and shall prioritize such available, feasible, and appropriate alternatives to signals intelligence.

(B) Signals intelligence collection activities shall be as tailored as feasible to advance a validated intelligence priority and, taking due account of relevant factors, not disproportionately impact privacy and civil liberties. Such factors may include, depending on the circumstances, the nature of the pursued objective; the feasible steps taken to limit the scope of the collection to the authorized purpose; the intrusiveness of the collection activity, including its duration; the probable contribution of the collection to the objective pursued; the reasonably foreseeable consequences to individuals, including unintended third parties; the nature and sensitivity of the data to be collected; and the safeguards afforded to the information collected.

(C) For purposes of subsection (c)(i) of this section, the scope of a specific signals intelligence collection activity may include, for example, a specific line of effort or target, as appropriate.

(ii) Bulk collection of signals intelligence.

(A) Targeted collection shall be prioritized. The bulk collection of signals intelligence shall be authorized only based on a determination — by an element of the Intelligence Community or through an interagency

committee consisting in whole or in part of the heads of elements of the Intelligence Community, the heads of departments containing such elements, or their designees — that the information necessary to advance a validated intelligence priority cannot reasonably be obtained by targeted collection.

When it is determined to be necessary to engage in bulk collection in order to advance a validated intelligence priority, the element of the Intelligence Community shall apply reasonable methods and technical measures in order to limit the data collected to only what is necessary to advance a validated intelligence priority, while minimizing the collection of non-pertinent information.

(B) Each element of the Intelligence Community that collects signals intelligence through bulk collection shall use such information only in pursuit of one or more of the following objectives:

(1) protecting against terrorism, the taking of hostages, and the holding of individuals captive (including the identification, location, and rescue of hostages and captives) conducted by or on behalf of a foreign government, foreign organization, or foreign person;

(2) protecting against espionage, sabotage, assassination, or other intelligence activities conducted by, on behalf of, or with the assistance of a foreign government, foreign organization, or foreign person;

(3) protecting against threats from the development, possession, or proliferation of weapons of mass destruction or related technologies and threats conducted by, on behalf of, or with the assistance of a foreign government, foreign organization, or foreign person;

(4) protecting against cybersecurity threats created or exploited by, or malicious cyber activities conducted by or on behalf of, a foreign government, foreign organization, or foreign person;

(5) protecting against threats to the personnel of the United States or of its allies or partners; and

(6) protecting against transnational criminal threats, including illicit finance and sanctions evasion related to one or more of the other objectives identified in subsection (c)(ii) of this section.

(C) The President may authorize updates to the list of objectives in light of new national security imperatives, such as new or heightened threats to the national security of the United States, for which the President determines that bulk collection may be used.

The Director shall publicly release any updates to the list of objectives authorized by the President, unless the President determines that doing so would pose a risk to the national security of the United States.

(D) In order to minimize any impact on privacy and civil liberties, a targeted signals intelligence collection activity that temporarily uses data acquired without discriminants (for example, without specific identifiers or selection terms) shall be subject to the safeguards described in this subsection, unless such data is:

(1) used only to support the initial technical phase of the targeted signals intelligence collection activity;

(2) retained for only the short period of time required to complete this phase; and

(3) thereafter deleted.

(iii) Handling of personal information collected through signals intelligence.

(A) Minimization. Each element of the Intelligence Community that handles personal information collected through signals intelligence shall establish and apply policies and procedures designed to minimize the dissemination and retention of personal information collected through signals intelligence.

(1) Dissemination. Each element of the Intelligence Community that handles personal information collected through signals intelligence:
(a) shall disseminate non-United States persons' personal information collected through signals intelligence only if it involves one or more of the comparable types of information that section 2.3 of Executive Order 12333 of December 4, 1981 (United States Intelligence Activities), as amended, states may be disseminated in the case of information concerning United States persons;

(b) shall not disseminate personal information collected through signals intelligence solely because of a person's nationality or country of residence;

(c) shall disseminate within the United States Government personal information collected through signals intelligence only if an authorized and appropriately trained individual has a reasonable belief that the personal information will be appropriately protected and that the recipient has a need to know the information;

(d) shall take due account of the purpose of the dissemination, the nature and extent of the personal information being disseminated, and the

potential for harmful impact on the person or persons concerned before disseminating personal information collected through signals intelligence to recipients outside the United States Government, including to a foreign government or international organization; and

(e) shall not disseminate personal information collected through signals intelligence for the purpose of circumventing the provisions of this order.

(2) Retention. Each element of the Intelligence Community that handles personal information collected through signals intelligence:

(a) shall retain non-United States persons' personal information collected through signals intelligence only if the retention of comparable information concerning United States persons would be permitted under applicable law and shall subject such information to the same retention periods that would apply to comparable information concerning United States persons;

(b) shall subject non-United States persons' personal information collected through signals intelligence for which no final retention determination has been made to the same temporary retention periods that would apply to comparable information concerning United States persons; and

(c) shall delete non-United States persons' personal information collected through signals intelligence that may no longer be retained in the same manner that comparable information concerning United States persons would be deleted.

(B) Data security and access. Each element of the Intelligence Community that handles personal information collected through signals intelligence:

(1) shall process and store personal information collected through signals intelligence under conditions that provide appropriate protection and prevent access by unauthorized persons, consistent with the applicable safeguards for sensitive information contained in relevant Executive Orders, proclamations, other Presidential directives, Intelligence Community directives, and associated policies;

(2) shall limit access to such personal information to authorized personnel who have a need to know the information to perform their mission and have received appropriate training on the requirements of applicable United States law, as described in policies and procedures issued under subsection (c)(iv) of this section; and

(3) shall ensure that personal information collected through signals intelligence for which no final retention determination has been made is

accessed only in order to make or support such a determination or to conduct authorized administrative, testing, development, security, or oversight functions.

(C) Data quality. Each element of the Intelligence Community that handles personal information collected through signals intelligence shall include such personal information in intelligence products only as consistent with applicable Intelligence Community standards for accuracy and objectivity, with a focus on applying standards relating to the quality and reliability of the information, consideration of alternative sources of information and interpretations of data, and objectivity in performing analysis.

(D) Queries of bulk collection. Each element of the Intelligence Community that conducts queries of unminimized signals intelligence obtained by bulk collection shall do so consistent with the permissible uses of signals intelligence obtained by bulk collection identified in subsection (c)(ii)(B) of this section and according to policies and procedures issued under subsection (c)(iv) of this section, which shall appropriately take into account the impact on the privacy and civil liberties of all persons, regardless of their nationality or wherever they might reside.

(E) Documentation. In order to facilitate the oversight processes set forth in subsection (d) of this section and the redress mechanism set forth in section 3 of this order, each element of the Intelligence Community that engages in signals intelligence collection activities shall maintain documentation to the extent reasonable in light of the nature and type of collection at issue and the context in which it is collected. The content of any such documentation may vary based on the circumstances but shall, to the extent reasonable, provide the factual basis pursuant to which the element of the Intelligence Community, based on a reasonable assessment of all relevant factors, assesses that the signals intelligence collection activity is necessary to advance a validated intelligence priority.

(iv) Update and publication of policies and procedures. The head of each element of the Intelligence Community:

(A) shall continue to use the policies and procedures issued pursuant to Presidential Policy Directive 28 of January 17, 2014 (Signals Intelligence Activities) (PPD-28), until they are updated pursuant to subsection (c)(iv)(B) of this section;

(B) shall, within 1 year of the date of this order, in consultation with the Attorney General, the CLPO, and the Privacy and Civil Liberties Oversight Board (PCLOB), update those policies and procedures as necessary to implement the privacy and civil liberties safeguards in this order; and

(C) shall, within 1 year of the date of this order, release these policies and procedures publicly to the maximum extent possible, consistent with the protection of intelligence sources and methods, in order to enhance the public's understanding of, and to promote public trust in, the safeguards pursuant to which the United States conducts signals intelligence activities.

(v) Review by the PCLOB.

(A) Nature of review. Consistent with applicable law, the PCLOB is encouraged to conduct a review of the updated policies and procedures described in subsection (c)(iv)(B) of this section once they have been issued to ensure that they are consistent with the enhanced safeguards contained in this order.

(B) Consideration of review. Within 180 days of completion of any review by the PCLOB described in subsection (c)(v)(A) of this section, the head of each element of the Intelligence Community shall carefully consider and shall implement or otherwise address all recommendations contained in such review, consistent with applicable law.

(d) Subjecting signals intelligence activities to rigorous oversight. The actions directed in this subsection are designed to build on the oversight mechanisms that elements of the Intelligence Community already have in place, in order to further ensure that signals intelligence activities are subjected to rigorous oversight.

(i) Legal, oversight, and compliance officials. Each element of the Intelligence Community that collects signals intelligence:

(A) shall have in place senior-level legal, oversight, and compliance officials who conduct periodic oversight of signals intelligence activities, including an Inspector General, a Privacy and Civil Liberties Officer, and an officer or officers in a designated compliance role with the authority to conduct oversight of and ensure compliance with applicable United States law;

(B) shall provide such legal, oversight, and compliance officials access to all information pertinent to carrying out their oversight responsibilities under this subsection, consistent with the protection of intelligence sources or methods, including their oversight responsibilities to ensure that any appropriate actions are taken to remediate an incident of non-compliance with applicable United States law; and

(C) shall not take any actions designed to impede or improperly influence such legal, oversight, and compliance officials in carrying out their oversight responsibilities under this subsection.

(ii) Training. Each element of the Intelligence Community shall maintain appropriate training requirements to ensure that all employees with access to signals intelligence know and understand the requirements of this order and the policies and procedures for reporting and remediating incidents of non-compliance with applicable United States law.

(iii) Significant incidents of non-compliance.

(A) Each element of the Intelligence Community shall ensure that, if a legal, oversight, or compliance official, as described in subsection (d)(i) of this section, or any other employee, identifies a significant incident of non-compliance with applicable United States law, the incident is reported promptly to the head of the element of the Intelligence Community, the head of the executive department or agency (agency) containing the element of the Intelligence Community (to the extent relevant), and the Director.

(B) Upon receipt of such report, the head of the element of the Intelligence Community, the head of the agency containing the element of the Intelligence Community (to the extent relevant), and the Director shall ensure that any necessary actions are taken to remediate and prevent the recurrence of the significant incident of non-compliance.

(e) Savings clause. Provided the signals intelligence collection is conducted consistent with and in the manner prescribed by this section of this order, this order does not limit any signals intelligence collection technique authorized under the National Security Act of 1947, as amended (50 U.S.C. 3001 et seq.), the Foreign Intelligence Surveillance Act of 1978, as amended (50 U.S.C. 1801 et seq.) (FISA), Executive Order 12333, or other applicable law or Presidential directive.

Sec. 3. Signals Intelligence Redress Mechanism.

(a) Purpose. This section establishes a redress mechanism to review qualifying complaints transmitted by the appropriate public authority in a qualifying state concerning United States signals intelligence activities for any covered violation of United States law and, if necessary, appropriate remediation.

(b) Process for submission of qualifying complaints. Within 60 days of the date of this order, the Director, in consultation with the Attorney General and the heads of elements of the Intelligence Community that collect or handle personal information collected through signals intelligence, shall establish a process for the submission of qualifying complaints transmitted by the appropriate public authority in a qualifying state.

(c) Initial investigation of qualifying complaints by the CLPO.

(i) Establishment. The Director, in consultation with the Attorney General, shall establish a process that authorizes the CLPO to investigate, review, and, as necessary, order appropriate remediation for qualifying complaints. This process shall govern how the CLPO will review qualifying complaints in a manner that protects classified or otherwise privileged or protected information and shall ensure, at a minimum, that for each qualifying complaint the CLPO shall:

(A) review information necessary to investigate the qualifying complaint;

(B) exercise its statutory and delegated authority to determine whether there was a covered violation by:

(i) taking into account both relevant national security interests and applicable privacy protections;

(ii) giving appropriate deference to any relevant determinations made by national security officials; and

(iii) applying the law impartially;

(C) determine the appropriate remediation for any covered violation;

(D) provide a classified report on information indicating a violation of any authority subject to the oversight of the Foreign Intelligence Surveillance Court (FISC) to the Assistant Attorney General for National Security, who shall report violations to the FISC in accordance with its rules of procedure;

(E) after the review is completed, inform the complainant, through the appropriate public authority in a qualifying state and without confirming or denying that the complainant was subject to United States signals intelligence activities, that:

(1) "the review either did not identify any covered violations or the Civil Liberties Protection Officer of the Office of the Director of National Intelligence issued a determination requiring appropriate remediation";

(2) the complainant or an element of the Intelligence Community may, as prescribed in the regulations issued by the Attorney General pursuant to section 3(d)(i) of this order, apply for review of the CLPO's determinations by the Data Protection Review Court described in subsection (d) of this section; and

(3) if either the complainant or an element of the Intelligence Community applies for review by the Data Protection Review Court, a special advocate

will be selected by the Data Protection Review Court to advocate regarding the complainant's interest in the matter;

(F) maintain appropriate documentation of its review of the qualifying complaint and produce a classified decision explaining the basis for its factual findings, determination with respect to whether a covered violation occurred, and determination of the appropriate remediation in the event there was such a violation, consistent with its statutory and delegated authority;

(G) prepare a classified ex parte record of review, which shall consist of the appropriate documentation of its review of the qualifying complaint and the classified decision described in subsection (c)(i)(F) of this section; and

(H) provide any necessary support to the Data Protection Review Court.

(ii) Binding effect. Each element of the Intelligence Community, and each agency containing an element of the Intelligence Community, shall comply with any determination by the CLPO to undertake appropriate remediation pursuant to subsection (c)(i)(C) of this section, subject to any contrary determination by the Data Protection Review Court.

(iii) Assistance. Each element of the Intelligence Community shall provide the CLPO with access to information necessary to conduct the reviews described in subsection (c)(i) of this section, consistent with the protection of intelligence sources and methods, and shall not take any actions designed to impede or improperly influence the CLPO's reviews. Privacy and civil liberties officials within elements of the Intelligence Community shall also support the CLPO as it performs the reviews described in subsection (c)(i) of this section.

(iv) Independence. The Director shall not interfere with a review by the CLPO of a qualifying complaint under subsection (c)(i) of this section; nor shall the Director remove the CLPO for any actions taken pursuant to this order, except for instances of misconduct, malfeasance, breach of security, neglect of duty, or incapacity.

(d) Data Protection Review Court.

(i) Establishment. The Attorney General is authorized to and shall establish a process to review determinations made by the CLPO under subsection (c)(i) of this section. In exercising that authority, the Attorney General shall, within 60 days of the date of this order, promulgate regulations establishing a Data Protection Review Court to exercise the Attorney General's authority to review such determinations. These regulations shall, at a minimum, provide that:

(A) The Attorney General, in consultation with the Secretary of Commerce, the Director, and the PCLOB, shall appoint individuals to serve as judges on the Data Protection Review Court, who shall be legal practitioners with appropriate experience in the fields of data privacy and national security law, giving weight to individuals with prior judicial experience, and who shall not be, at the time of their initial appointment, employees of the United States Government.

During their term of appointment on the Data Protection Review Court, such judges shall not have any official duties or employment within the United States Government other than their official duties and employment as judges on the Data Protection Review Court.

(B) Upon receipt of an application for review filed by the complainant or an element of the Intelligence Community of a determination made by the CLPO under subsection (c) of this section, a three-judge panel of the Data Protection Review Court shall be convened to review the application. Service on the Data Protection Review Court panel shall require that the judge hold the requisite security clearances to access classified national security information.

(C) Upon being convened, the Data Protection Review Court panel shall select a special advocate through procedures prescribed in the Attorney General's regulations. The special advocate shall assist the panel in its consideration of the application for review, including by advocating regarding the complainant's interest in the matter and ensuring that the Data Protection Review Court panel is well informed of the issues and the law with respect to the matter.

Service as a special advocate shall require that the special advocate hold the requisite security clearances to access classified national security information and to adhere to restrictions prescribed in the Attorney General's regulations on communications with the complainant to ensure the protection of classified or otherwise privileged or protected information.

(D) The Data Protection Review Court panel shall impartially review the determinations made by the CLPO with respect to whether a covered violation occurred and the appropriate remediation in the event there was such a violation. The review shall be based at a minimum on the classified ex parte record of review described in subsection (c)(i)(F) of this section and information or submissions provided by the complainant, the special advocate, or an element of the Intelligence Community.

In reviewing determinations made by the CLPO, the Data Protection Review Court panel shall be guided by relevant decisions of the United States Supreme Court in the same way as are courts established under

Article III of the United States Constitution, including those decisions regarding appropriate deference to relevant determinations of national security officials.

(E) In the event that the Data Protection Review Court panel disagrees with any of the CLPO's determinations with respect to whether a covered violation occurred or the appropriate remediation in the event there was such a violation, the panel shall issue its own determinations.

(F) The Data Protection Review Court panel shall provide a classified report on information indicating a violation of any authority subject to the oversight of the FISC to the Assistant Attorney General for National Security, who shall report violations to the FISC in accordance with its rules of procedure.

(G) After the review is completed, the CLPO shall be informed of the Data Protection Review Court panel's determinations through procedures prescribed by the Attorney General's regulations.

(H) After a review is completed in response to a complainant's application for review, the Data Protection Review Court, through procedures prescribed by the Attorney General's regulations, shall inform the complainant, through the appropriate public authority in a qualifying state and without confirming or denying that the complainant was subject to United States signals intelligence activities, that "the review either did not identify any covered violations or the Data Protection Review Court issued a determination requiring appropriate remediation."

(ii) Binding effect. Each element of the Intelligence Community, and each agency containing an element of the Intelligence Community, shall comply with any determination by a Data Protection Review Court panel to undertake appropriate remediation.

(iii) Assistance. Each element of the Intelligence Community shall provide the CLPO with access to information necessary to conduct the review described in subsection (d)(i) of this section, consistent with the protection of intelligence sources and methods, that a Data Protection Review Court panel requests from the CLPO and shall not take any actions for the purpose of impeding or improperly influencing a panel's review.

(iv) Independence. The Attorney General shall not interfere with a review by a Data Protection Review Court panel of a determination the CLPO made regarding a qualifying complaint under subsection (c)(i) of this section; nor shall the Attorney General remove any judges appointed as provided in subsection (d)(i)(A) of this section, or remove any judge from service on a Data Protection Review Court panel, except for instances of misconduct, malfeasance, breach of security, neglect of duty, or incapacity,

after taking due account of the standards in the Rules for Judicial-Conduct and Judicial-Disability Proceedings promulgated by the Judicial Conference of the United States pursuant to the Judicial Conduct and Disability Act (28 U.S.C. 351 et seq.).

(v) Record of determinations. For each qualifying complaint transmitted by the appropriate public authority in a qualifying state, the Secretary of Commerce shall:

(A) maintain a record of the complainant who submitted such complaint;

(B) not later than 5 years after the date of this order and no less than every 5 years thereafter, contact the relevant element or elements of the Intelligence Community regarding whether information pertaining to the review of such complaint by the CLPO has been declassified and whether information pertaining to the review of any application for review submitted to the Data Protection Review Court has been declassified, including whether an element of the Intelligence Community filed an application for review with the Data Protection Review Court; and

(C) if informed that such information has been declassified, notify the complainant, through the appropriate public authority in a qualifying state, that information pertaining to the review of their complaint by the CLPO or to the review of any application for review submitted to the Data Protection Review Court may be available under applicable law.

Sec. 4. Definitions. For purposes of this order:

(a) "Appropriate remediation" means lawful measures designed to fully redress an identified covered violation regarding a specific complainant and limited to measures designed to address that specific complainant's complaint, taking into account the ways that a violation of the kind identified have customarily been addressed.

Such measures may include, depending on the specific covered violation at issue, curing through administrative measures violations found to have been procedural or technical errors relating to otherwise lawful access to or handling of data, terminating acquisition of data where collection is not lawfully authorized, deleting data that had been acquired without lawful authorization, deleting the results of inappropriately conducted queries of otherwise lawfully collected data, restricting access to lawfully collected data to those appropriately trained, or recalling intelligence reports containing data acquired without lawful authorization or that were otherwise disseminated in a manner inconsistent with United States law.

Appropriate remediation shall be narrowly tailored to redress the covered violation and to minimize adverse impacts on the operations of the Intelligence Community and the national security of the United States.

(b) "Bulk collection" means the authorized collection of large quantities of signals intelligence data that, due to technical or operational considerations, is acquired without the use of discriminants (for example, without the use of specific identifiers or selection terms).

(c) "Counterintelligence" shall have the same meaning as it has in Executive Order 12333.

(d) "Covered violation" means a violation that:

(i) arises from signals intelligence activities conducted after the date of this order regarding data transferred to the United States from a qualifying state after the effective date of the Attorney General's designation for such state, as provided in section 3(f)(i) of this order;

(ii) adversely affects the complainant's individual privacy and civil liberties interests; and

(iii) violates one or more of the following:

(A) the United States Constitution;

(B) the applicable sections of FISA or any applicable FISC-approved procedures;

(C) Executive Order 12333 or any applicable agency procedures pursuant to Executive Order 12333;

(D) this order or any applicable agency policies and procedures issued or updated pursuant to this order (or the policies and procedures identified in section 2(c)(iv)(A) of this order before they are updated pursuant to section 2(c)(iv)(B) of this order);

(E) any successor statute, order, policies, or procedures to those identified in section 4(d)(iii)(B)-(D) of this order; or

(F) any other statute, order, policies, or procedures adopted after the date of this order that provides privacy and civil liberties safeguards with respect to United States signals intelligence activities within the scope of this order, as identified in a list published and updated by the Attorney General, in consultation with the Director of National Intelligence.

(e) "Foreign intelligence" shall have the same meaning as it has in Executive Order 12333.

(f) "Intelligence" shall have the same meaning as it has in Executive Order 12333.

(g) "Intelligence Community" and "elements of the Intelligence Community" shall have the same meaning as they have in Executive Order 12333.

(h) "National security" shall have the same meaning as it has in Executive Order 13526 of December 29, 2009 (Classified National Security Information).

(i) "Non-United States person" means a person who is not a United States person.

(j) "Personnel of the United States or of its allies or partners" means any current or former member of the Armed Forces of the United States, any current or former official of the United States Government, and any other person currently or formerly employed by or working on behalf of the United States Government, as well as any current or former member of the military, current or former official, or other person currently or formerly employed by or working on behalf of an ally or partner.

(k) "Qualifying complaint" means a complaint, submitted in writing, that:

(i) alleges a covered violation has occurred that pertains to personal information of or about the complainant, a natural person, reasonably believed to have been transferred to the United States from a qualifying state after the effective date of the Attorney General's designation for such state, as provided in section 3(f)(i) of this order;

(ii) includes the following basic information to enable a review: information that forms the basis for alleging that a covered violation has occurred, which need not demonstrate that the complainant's data has in fact been subject to United States signals intelligence activities; the nature of the relief sought; the specific means by which personal information of or about the complainant was believed to have been transmitted to the United States; the identities of the United States Government entities believed to be involved in the alleged violation (if known); and any other measures the complainant pursued to obtain the relief requested and the response received through those other measures;

(iii) is not frivolous, vexatious, or made in bad faith;

(iv) is brought on behalf of the complainant, acting on that person's own behalf, and not as a representative of a governmental, nongovernmental, or intergovernmental organization; and

(v) is transmitted by the appropriate public authority in a qualifying state, after it has verified the identity of the complainant and that the complaint satisfies the conditions of section 5(k)(i)-(iv) of this order.

(l) "Significant incident of non-compliance" shall mean a systemic or intentional failure to comply with a principle, policy, or procedure of applicable United States law that could impugn the reputation or integrity of an element of the Intelligence Community or otherwise call into question the propriety of an Intelligence Community activity, including in light of any significant impact on the privacy and civil liberties interests of the person or persons concerned.

(m) "United States person" shall have the same meaning as it has in Executive Order 12333.

(n) "Validated intelligence priority" shall mean, for most United States signals intelligence collection activities, a priority validated under the process described in section 2(b)(iii) of this order; or, in narrow circumstances (for example, when such process cannot be carried out because of a need to address a new or evolving intelligence requirement), shall mean a priority set by the President or the head of an element of the Intelligence Community in accordance with the criteria described in section 2(b)(iii)(A)(1)-(3) of this order to the extent feasible.

(o) "Weapons of mass destruction" shall have the same meaning as it has in Executive Order 13526.

To read more: https://www.whitehouse.gov/briefing-room/presidential-actions/2022/10/07/executive-order-on-enhancing-safeguards-for-united-states-signals-intelligence-activities/

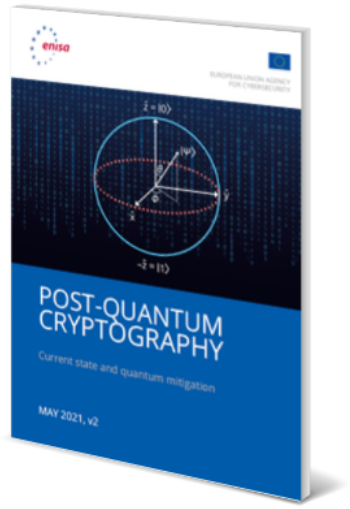
Post-Quantum Cryptography, Integration study

EUROPEAN UNION AGENCY FOR CYBERSECURITY

With this report ENISA seeks to give insight on post-standardisation challenges. A follow-up to ENISA's 2021 Post-Quantum Cryptography: Current state and quantum mitigation study.

Post-Quantum Cryptography: Current state and quantum mitigation

This study provides an overview of the current state of affairs on the standardization process of Post-Quantum Cryptography (PQC). It presents the 5 main families of PQ algorithms; viz. code-based, isogeny-based, hash-based, lattice-based and multivariate-based. It also describes the NIST Round 3 finalists for encryption and signature schemes, as well as the alternative candidate schemes. Given that the NIST process will still run for a few years, the last chapter offers 2 proposals that system owners can implement now in order to protect the confidentiality of their data against a quantum capable attacker; namely hybrid implementations that use a combination of pre-quantum and post-quantum schemes, and the mixing of pre-shared keys into all keys established via public-key cryptography.



Download
PDF document, 1.05 MB

You may visit: https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation

The new report elaborates on the topic to address the following points:

- Integrating post-quantum systems into existing protocols
- New protocols designed around post-quantum systems
- Double encryption and double signatures using post-quantum systems
- Seccurity proofs in the presence of quantum attackers
- Standardisation efforts for post-quantum enabled protocols

The 2021 study provided an overview of the current state of play on the standardisation process of Post-Quantum Cryptography (PQC).

It introduced a framework for analysing existing PQC proposals, presented the five (5) main families of PQC algorithms, and the NIST Round 3 finalists for encryption and signature schemes.

It also sketched two proposals that proactive system owners can implement right now – before a standard is published – in order to protect the confidentiality of their data against a quantum capable attacker.

While agreeing on PQC cryptoalgorithms for encryption and signing is an important milestone, by itself it is not enough. Any new cryptoalgorithm will need to interplay with existing protocols or even require entirely new protocols to be designed and implemented.

Furthermore, PQC proposals are a solution to a still unrealised vulnerability – there are currently no publicly known quantum computers, strong enough to break encryption, and not all scientists believe this will ever be the case.

Whether we should implement protections against a threat that might not materialise would be a moot question if said implementations were cost free. However, PQC algorithms are often more costly, e.g. in terms of size and computations.

In addition, changing to a new cryptographic paradigm might provide new opportunities for software bugs and our understanding of the security of the PQC algorithms is often less mature.

Introduction

Cryptography is a crucial tool for the security of our digital society and is used virtually everywhere. For example, it secures our online communications, keeps the data on our devices secret even if we lose them, and protects the integrity and authenticity of digital records.

The security of cryptographic solutions deployed today is threatened by the development of quantum computers. To counter this threat, the area of post-quantum cryptography was initiated.
Post-quantum cryptography studies cryptosystems under the assumption that the attacker has access to a quantum computer, while the user is supposed to be a regular user of today's systems with no quantum capabilities.

Several classes of problems exist that are conjectured to withstand even attacks using quantum computers. At this point the US National Institute

for Standards and Technology (NIST) is running a selection process to select such systems for standardisation.

Given the success of NIST standards in the area of cryptography, it is likely that the systems selected by NIST will become the international standard for large parts of the world, including the European Union.

An overview of the process and the systems under consideration can be found in the recent Post-Quantum Cryptography: Current state and quantum mitigation study by ENISA.

In July 2022, NIST announced four candidates to be standardised, plus the four fourth round candidate Key-Establishment Mechanisms (KEMs).

In addition, NIST plans to issue a new Call for Proposals for public-key (quantum-resistant) digital signature algorithms by the end of summer 2022.

One might expect that with the end of this process, i.e. the publication of the standards, everything will have been solved. We simply replace the schemes that we are using today with the new systems and be done.

This unfortunately is not the case at all. Many challenges need to be overcome before our data and our systems are secured against attacks using quantum computers.

One challenge is the size of the artifacts produced by post-quantum cryptography. The reason that today's cryptographic systems are so efficient is also the reason why they are vulnerable to quantum computers – these problems are highly structured.

Systems secure against quantum attacks have far less structure and hence a less compact description. As a consequence, keys, ciphertexts and signatures are larger for post-quantum systems than for matching pre-quantum systems. This poses challenges to higher-level protocols. Protocol messages do not meet the size limitations of underlying protocols anymore, which at least leads to fragmentation, additional round-trips, and a more complicated state-machine if not treated carefully.

As a consequence, latency and data traffic increase. A related aspect is a decrease in the speed of some algorithms. This can significantly hurt the performance of protocols if not taken into consideration.

Both aspects can be dealt with by designing new protocols that take the new performance characteristics into account. However, this comes of course with all the challenges of designing new cryptographic protocols from assessing their security to standardising them.

The paper: https://www.enisa.europa.eu/publications/post-quantum-cryptography-integration-study

Defenders beware: A case for post-ransomware investigations

Microsoft Detection and Response Team (DART)

Microsoft

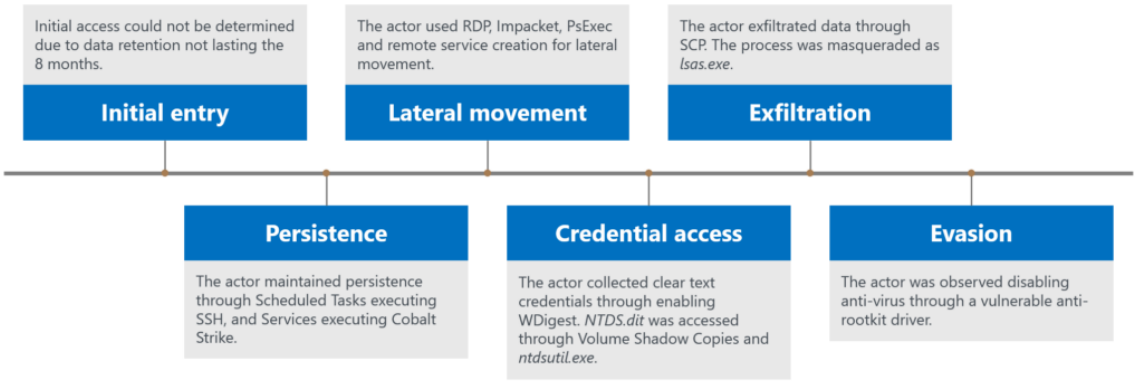
Ransomware is one of the most pervasive threats that Microsoft Detection and Response Team (DART) responds to today. The groups behind these attacks continue to add sophistication to their tactics, techniques, and procedures (TTPs) as most network security postures increase.

In this blog, we detail a recent ransomware incident in which the attacker used a collection of commodity tools and techniques, such as using living-off-the-land binaries, to launch their malicious code. Cobalt Strike was used for persistence on the network with NT AUTHORITY/SYSTEM (local SYSTEM) privileges to maintain access to the network after password resets of compromised accounts.

This incident highlights an attacker's ability to have a longstanding dwell time on a network before deploying ransomware. We will also discuss the various techniques used as well as the recommended detections and defense techniques that customers can use to increase protection against these types of attacks.

Microsoft recommends hunting proactively for pre-ransomware behaviors and hardening your network to prevent impact.

Refer to https://aka.ms/ransomware-as-a-service for more information about defending against ransomware-related incidents.



Initial access

DART was unable to determine the initial entry vector of this attack due to the age of this compromise and limited retention of security solutions, along with encrypted devices being reimaged before analysis. The earliest observed activity showed the actor with domain administrator credentials.

Persistence

In DART's post ransomware investigation of this engagement, the team found multiple instances of scheduled tasks and services being created by the attack for persistence after they had gained access to highly privileged credentials. Services and Scheduled Tasks have the option to run as NT AUTHORITY\System, allowing their malicious code to run with highly privileged access.

Because the actor created those tasks and services on a domain controller, the Local SYSTEM access allowed them to easily access domain administrator accounts. The deployment of a backdoor to a domain controller can help an actor bypass common incident response recovery activity, such as resetting compromised accounts, in the hope of staying resident on the network.

Service: Cobalt Strike

Cobalt Strike was seen on a large scale across the network, on domain controllers, servers, and administrator workstations. The actor created Windows services to persist their payload executing rundll32 to load the Cobalt Strike DLL through invoking the "AllocConsole" exported function of a variation of the Termite family of malware.

These services were observed to execute with a combination of SYSTEM and domain administrator credentials. Termite malware is often used by crimeware groups to load Cobalt Strike while bypassing antivirus detections. Further information on the Termite malware family can be found in this blog: https://www.mandiant.com/resources/blog/unc2596-cuba-ransomware

To read more: https://www.microsoft.com/en-us/security/blog/2022/10/18/defenders-beware-a-case-for-post-ransomware-investigations/

First phase of new supercomputer installed at Los Alamos National Laboratory

The critical first phase of Los Alamos National Laboratory's newest supercomputer, Crossroads, has been successfully installed.

Called Tycho, this machine is a stepping-stone to Crossroads, which will replace Trinity as the Laboratory's primary supercomputer in the coming year and will support next-generation weapons simulations.

"We're excited to be entering this new phase of supercomputing at the Lab," said Los Alamos' HPC Platforms Program Director Jim Lujan. "Early benchmarks indicate a four-times increase in speed over Trinity. All of the new efficiencies that are part of Tycho, and ultimately Crossroads, come together to reduce that crucial time to insight. Improving efficiencies in many areas for modeling and simulation is what this project is all about."

A Hewlett Packard Enterprise machine, based on the HPE Cray EX supercomputer, Crossroads will support critical maintenance and modernization of the U.S. nuclear stockpile, as well as other nuclear security missions.

Amanda Bonnie, project manager for Crossroads, has been with Tycho from when it was just a configuration diagram, all the way to rolling the 8,000-pound cabinets off trucks and seeing them through their installation on Los Alamos' Strategic Computing Complex floor, which is approximately the size of a football field.

"I think my favorite part of the entire process is the delivery and install week," said Bonnie. "Getting to be there and see it become something before your eyes is magical."

Tycho brings to bear emerging technologies including the first large-scale deployment of Intel's new Sapphire Rapids processor. Earlier this year, HPC tests helped Intel engineers configure the chip to best serve Laboratory-specific application performance.

Adding to overall efficiency, Solid State Drives will make up the entirety of Tycho's file system — a first for Los Alamos supercomputers. Additionally, warm water direct liquid cooling will mean significant energy savings over more traditional approaches.

Following in Trinity's footsteps, Crossroads gets its name from the second series of nuclear weapons tests conducted at Bikini Atoll in 1946.

Tycho, however, has a different origin. Key Crossroads components Tycho, Rocinante and Razorback are all named for spacecraft from The Expanse — a sci-fi TV series based on novels written by James S.A. Corey (pen name of authors Ty Franck and Daniel Abraham, both of whom have New Mexico ties).

In coming months, the Crossroads team will work to stabilize Tycho, calibrating the system's 2,600 Sapphire Rapids nodes for maximum efficiency. Software will be installed and functionality testing will take place — all in time to ensure Tycho's early use in the classified environment by the end of the year and full production status in March 2023.

This Advanced Technology System is funded by the Department of Energy's National Nuclear Security Administrations' Advanced Simulation and Computing program.

To read more: https://discover.lanl.gov/news/1020-supercomputer-tycho

Advances in digital currency experimentation

Michelle Neal, Executive Vice President and Head of Markets of the Federal Reserve Bank of New York, at the Singapore FinTech Festival 2022, Singapore.

Good afternoon. It is a pleasure to be here with you at the Singapore Fintech Festival. It is exciting to be a part of this gathering of industry professionals, policy leaders, and investors to discuss key developments in the fintech industry.

Digital innovation has the potential to benefit the financial system writ large by reducing transaction costs, increasing competition, and broadening access to a wider range of participants.

However, harnessing the full potential of financial innovation and related technologies – especially regarding cross-border settlements and payments – will require collaboration across a range of international partners.

In my remarks today I will discuss the landscape of digital assets and some of the ways that the Federal Reserve System is engaging in research and experimentation that support ongoing innovation.

As always, the views I express today are my own, and do not necessarily reflect those of the Federal Reserve Bank of New York or the Federal Reserve System.

Digital Assets and the Federal Reserve

We are all experiencing the incredible pace of growth and change within the digital asset domain, which encompasses a range of opportunities and risks. The market capitalization of digital assets reached $3 trillion in November 2021.

The rapid growth of digital assets presents opportunities to both reinforce the role of central banks and regulatory bodies in stewardship of the global financial system and be positioned at the technological frontier.
However, this growth is not without risks: in May, the crash of Terra, an unbacked algorithmic stablecoin, and the subsequent wave of insolvencies, wiped out over $600 billion of investor and consumer funds.

Currently, the total cryptoasset market capitalization rests around $1 trillion, a 66 percent decline from its November 2021 peak.

When I consider the ways in which digital assets impact the mission of the Federal Reserve, I see several channels – including monetary policy and the provision of an elastic currency, the preservation of financial stability, and the smooth operation of the payments system.

Regarding monetary policy and currency, in January, the Federal Reserve released a discussion paper that considers a future where digital assets may play a large role in our financial system, and in particular, establishes some broad principles and outlines some of the pros and cons of a central bank digital currency, or CBDC.

While at present the Federal Reserve has neither issued a CBDC nor plans to do so imminently, ongoing research improves our understanding of the risks and opportunities inherent to a CBDC.

Central bank money – a liability of the Federal Reserve – is the bedrock of the U.S. financial system. It is held by depository institutions as bank reserves or by individuals in the form of paper currency.

Demand for central bank money is driven by many fundamental factors, including the settlement of both retail and wholesale transactions and its role as a store of value.

In addition to these factors, which are likely familiar to any of you who have studied monetary economics, demand for the U.S. dollar is also driven by international factors owing to the role of the dollar in the global economy.

In fact, while precise estimates are challenging to come by, available data suggests that more than half of all dollars in circulation may be held outside the United States.

As a result, innovation related to money provided by the Federal Reserve will have impacts that extend far beyond U.S. borders.

A U.S. CBDC – a digital form of the U.S. dollar that is a direct liability of the Federal Reserve– has the potential to offer significant benefits. It could enable a payment system that is more efficient, provide a foundation for further technological innovation, and facilitate faster cross-border transactions. It could promote financial inclusion and equity by enabling access for a broad set of consumers and foster economic growth and stability.

In order to fully realize benefits such as these, a digital dollar would need to be thoughtfully designed and implemented.

A CBDC would need to protect against cyber and operational risks, safeguard the privacy of sensitive data, and minimize risks of illicit financial transactions.

Additionally, one of the most important aspects in our deliberations is that any form of a CBDC in the future would need to be intermediated.

This means that the private sector would need to act as intermediaries in that system, and a direct account approach would not be contemplated.

While the Federal Reserve has made no decision on whether or how to issue a CBDC, we are actively conducting technical investigations into both retail and wholesale CBDC design.

Project Hamilton, which is a partnership between the Federal Reserve Bank of Boston and MIT, has experimented with potential approaches to a digital dollar, with work focused on retail uses and payment channels.

In the use case they explored, the Hamilton team was able to demonstrate the potential for usage at scale, which would be a key design element of a retail CBDC.

As a complement, and in line with the New York Fed's unique role in the Federal Reserve System with wholesale payments in both domestic payments and foreign exchange, the New York Innovation Center is researching technical aspects related to wholesale CBDCs.

In addition to CBDC, the broader digital assets landscape, which includes stablecoins – cryptoassets that are backed by assets such as U.S. Treasury securities to stabilize their value – and unbacked cryptoassets, has grown significantly in recent years, and continues to evolve quickly.

While many digital-asset-related activities fall within existing U.S. laws and regulations, the rapid evolution and adoption of digital assets highlight unique risks that warrant a more comprehensive and aligned approach by agencies across the U.S. government with different regulatory remits.

The Federal Reserve, as an independent central bank, is only one part of the puzzle. Many of these other stakeholders across the U.S. government, such as the Treasury Department, market regulators, and federal banking supervisors, will be involved in providing guidance and guardrails to the financial system as the universe of digital assets continues to evolve.

In the current environment of rapid technological change, it is crucial that innovation proceeds responsibly in order to safeguard the stability of the financial system.

To that end, on March 9 of this year, President Biden issued an Executive Order on Ensuring Responsible Development of Digital Assets.

This executive order outlined the first whole-of-government approach to addressing the risks and harnessing the potential benefits of digital assets and their underlying technology.

In response, over the past six months, agencies across the government have worked together to develop frameworks and policy recommendations that advance the six key priorities identified in the executive order: consumer and investor protection; promoting financial stability; countering illicit finance; U.S. leadership in the global financial system and economic competitiveness; financial inclusion; and responsible innovation.

The executive order will be a catalyst to increased coordination among U.S. regulators.

Last month, as part of the approach outlined in the executive order, the Financial Stability Oversight Council, or FSOC, released a report that considers the financial stability risks of crypto assets.

In the report, the FSOC noted that financial stability risks of crypto assets are drawn mainly from interconnections with the traditional financial system.

The report identified vulnerabilities unique to crypto assets and recommended approaches to regulation and supervision in the future, highlighting the importance of ongoing research to improve our understanding of risks and opportunities, and planning to ensure we can continue to achieve our mission including supporting safety and stability in this evolving domain.

The Fed also collaborates with other U.S. regulators on the topic of stability risks arising from digital assets, and coordinates with international authorities through forums including the Bank for International Settlements (BIS) and the Financial Stability Board.

Finally, a third key dimension through which innovation – both broadly and in digital assets specifically – impacts the mission of the Federal Reserve is in relation to the payments system.

On a daily basis, roughly $4 trillion of transactions are settled through FedWire, the real-time gross settlement (RTGS) service offered by the Federal Reserve.

FedNow, targeted for release in mid-2023, represents a key innovation to modernize the future of payments. This new cloud-based RTGS system will enable consumers and businesses to send payments instantly through their depository institutions on a 24-hour, 365-days-a-year basis.

Of course, payments do not always stay within national borders. The Federal Reserve is an active participant in international efforts regarding payment systems via the Committee on Payments and Markets Infrastructures (CPMI) at the BIS.

The CMPI collects best practices and issues recommendations for managing payments, clearing, and settlement risk across financial market utilities.

At present, a high-priority area of study for the CMPI is coordinating the development of 24/365 RTGS systems – like FedNow – globally.

Innovation in cross-border settlements will reduce liquidity outlays and settlement risks, leading in turn to cheaper cross-border payments.

The New York Innovation Center and Project Cedar

In the remainder of my remarks, I'd like to focus on an example of ongoing innovation research that is currently underway at the Federal Reserve Bank of New York.

To further enhance our ability to contribute to financial innovation globally, the New York Innovation Center, or NYIC, was established in 2021.

The NYIC bridges the worlds of finance, technology, and innovation. Through technical research, experimentation, and prototyping, our team generates insights into high-value central-bank-related opportunities, enabling stakeholders and the central bank community to enhance the functioning of the global financial system.
Project Cedar is the inaugural project of the NYIC and represents the first stage of the NYIC's research efforts into CBDCs, the NYIC's biggest focus area in 2022.

A goal of the NYIC is to progress CBDC research with an objective of defining a technical design for a CBDC addressing the wholesale market in the Federal Reserve context.

After taking a close look at the foreign exchange space with economists, traders, and market analysts, the NYIC team zeroed in on settlement of foreign exchange spot transactions as a first area of investigation.

FX spot transactions are critical in the context of cross-border payments, and serve as a building block for longer, more complex transactions.

Traditionally, settlement generally takes two days after a transaction, which leaves some room for improvement.

By demonstrating improvements in settlement of FX spot transactions, the NYIC could address settlement time and risk, which would have implications to speed and access for the broader cross-border market.

We are not the first to address this topic, of course, but the NYIC wanted to investigate it from the perspective of the Federal Reserve, through the lens of a wholesale CBDC.

The NYIC developed a hypothesis that there is a distributed ledger technology solution for wholesale FX settlement that results in instant and atomic settlement in which a wholesale CBDC is the settlement asset.

NYIC then built a working prototype and tested it.

Results from the experiment indicated that settlement could occur in fewer than 10 seconds on average and that horizontal scaling was possible.

This indicates that a modular ecosystem of ledgers has the potential for continued scalability, and that distributed ledger technology could enable settlement times well below the current industry standard of two days, with the added guarantee of atomic settlement.

Conclusion

Innovations in digital assets have the potential to impact financial markets in many fundamental ways; it is essential to understand these developments and the impact they may have on the mission of the Federal Reserve. Through ongoing investment in research, experimentation, and collaboration, leveraging the full potential of digital assets is possible. I look forward to building on the successes of Project Cedar and similar efforts.

To read more: https://www.bis.org/review/r221104c.htm

Privacy Policy

We're updating our Privacy Policy with effect from 2 December 2022.

Introduction

This privacy policy ("Privacy Policy") applies to the personal information that TikTok processes in connection with TikTok apps, websites, software and related services (the “Platform”), that link to or reference this Privacy Policy.

Data Controller: If you live in the European Economic Area (“EEA”), the United Kingdom (“UK”), or Switzerland, TikTok Technology Limited, an Irish company (“TikTok Ireland”), and TikTok Information Technologies UK Limited (“TikTok UK”), a UK company, ("TikTok," "our," "we," or "us") are the joint controllers of your information processed in connection with this Privacy Policy.

What Information We Collect

We collect your information in three ways: Information You Provide, Automatically Collected Information, and Information From Other Sources. More detail is provided below.

Information You Provide

Profile Information. We collect information that you provide when you set up an account, such as your date of birth, username, email address and/or telephone number, and password. You can add other information to your profile, such as a bio or a profile photo.

User Content. We collect the content you create or publish through the Platform, such as photographs, videos, audio recordings, livestreams, and comments, and the associated metadata (such as when, where, and by whom the content was created).

Even if you are not a user, information about you may appear in content created or published by users on the Platform. We collect User Content through pre-loading at the time of creation, import, or upload, regardless of whether you choose to save or upload that User Content, for example, to recommend music based on the video.

We also collect content (such as text, images, and video) from your device's clipboard if you choose to copy and paste content to or from the Platform or share content between it and a third party platform. In addition, we

collect location information (such as tourist attractions, shops, or other points of interest) if you choose to add the location information to your User Content.

Direct Messages. If you communicate with others using direct messages, we collect the content of the message and the associated metadata (such as the time the message was sent, received and/or read, as well as the participants in the communication). We do this to block spam, detect crime, and to safeguard our users.

Your Contacts. If you choose to import your contacts, we will collect information from your device's phone book or your social media contacts. We use this information to help you make connections, including when you are using our "Find Friends" function and to suggest accounts to you.

Purchase Information. We collect your payment card information or other third-party payment information (such as PayPal) where payment is required. We also collect your transaction and purchase history.

Surveys, Research, and Promotions. We collect information you provide if you choose to participate in a survey, research, promotion, contest, marketing campaign, or event conducted or sponsored by us.

Information When You Contact Us. When you contact us, we collect the information you send us, such as proof of identity or age, feedback or inquiries about your use of the Platform or information about possible violations of our Terms of Service (our "Terms"), Community Guidelines (our "Guidelines"), or other policies.

Automatically Collected Information

Technical Information. We collect certain device and network connection information when you access the Platform. This information includes your device model, operating system, keystroke patterns or rhythms, IP address, and system language.

We also collect service-related, diagnostic, and performance information, including crash reports and performance logs. We automatically assign you a device ID and user ID. Where you log-in from multiple devices, we use information such as your device ID and user ID to identify your activity across devices to give you a seamless log-in experience and for security purposes.

Location Information. We automatically collect information about your approximate location (e.g. country, state, or city) based on your Technical Information (such as SIM card and IP address).

Also, where you enable Location Services for the TikTok app within your device settings, we collect approximate location information from your device. Click here to learn more about how we collect Location Information.

Usage Information. We collect information about how you engage with the Platform, including information about the content you view, the duration and frequency of your use, your engagement with other users, your search history and your settings.

Content Characteristics and Features. We detect and collect characteristics and features about the videos, images, and audio recordings that are part of your User Content, for example, by identifying objects and scenery, the existence or location within an image of a face or other body parts; and the text of words spoken in your User Content. We do this, for example, for content moderation and to provide special effects (such as video filters and avatars) and captions.

Inferred Information. We infer your attributes (such as age-range and gender) and interests based on the information we have about you. We use inferences, for example, to keep the Platform safe, for content moderation and, where permitted, to serve you personalised ads based on your interests.

Cookies. We use cookies and similar tracking technologies to operate and provide the Platform. For example, we use cookies to remember your language preferences, make sure you don't see the same video more than once, and for security purposes.

We also use these technologies for marketing purposes. To learn more about our use of cookies, please see our Web Cookies Policy and Platform Cookies Policy. We will obtain your consent to our use of cookies where required by law.

Information From Other Sources

Advertising, Measurement and Data Partners. Advertisers, measurement and data partners share information with us such as mobile identifiers for advertising, hashed email addresses, and event information about the actions you've taken outside of the Platform.
Some of our advertisers and other partners enable us to collect similar information directly from their website or app by integrating our TikTok Advertiser Tools (such as TikTok Pixel).

Third Party Platforms and Partners. Third party platforms provide us with information (such as your email address, user ID, and public profile) when you choose to sign up for or log in to the Platform using sign-in features

provided by those third parties. We may also receive contact information that you hold or is held about you when contact information is synced with our Platform by you or another user.

When you interact with any third party service (such as third party apps, websites or products) that integrate TikTok Developer Tools, we will receive the information necessary to provide you with features like cross-service authentication or cross-posting. For example, this will happen if you log in to another platform with your TikTok account or if you use TikTok's "share" button on a third party platform to share content from there to the Platform.

Others. We may receive information about you from others, for example, where you are included or mentioned in User Content, Direct Messages, in a complaint, appeal, request or feedback submitted by a user or third party, or if your contact information is provided to us by a user.

To read more: https://www.tiktok.com/legal/page/eea/new-privacy-policy/en

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

2. Monthly Updates - Visit the Reading Room of the SOXCPA at: 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/CJSOXE_Distance_Learning_and_Certification.htm

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