



Sarbanes Oxley News, March 2024

The Securities and Exchange Commission adopted rules to enhance and standardize **climate-related disclosures** by public companies and in public offerings.



The final rules reflect the Commission’s efforts to respond to investors’ demand for more consistent, comparable, and reliable information about the financial effects of climate-related risks on a registrant’s operations and how it manages those risks while balancing concerns about mitigating the associated costs of the rules.

“Our federal securities laws lay out a basic bargain. Investors get to decide which risks they want to take so long as companies raising money from the public make what President Franklin Roosevelt called ‘complete and truthful disclosure,’” said SEC Chair Gary Gensler.

“Over the last 90 years, the SEC has updated, from time to time, the disclosure requirements underlying that basic bargain and, when necessary, provided guidance with respect to those disclosure requirements.”

Chair Gensler added, “These final rules build on past requirements by mandating material climate risk disclosures by public companies and in public offerings. The rules will provide investors with consistent, comparable, and decision-useful information, and issuers with clear reporting requirements. Further, they will provide specificity on what companies must disclose, which will produce more useful information than what investors see today.

They will also require that climate risk disclosures be included in a company's SEC filings, such as annual reports and registration statements rather than on company websites, which will help make them more reliable."

Specifically, the final rules will require a registrant to **disclose**:

- Climate-related risks that have had or are reasonably likely to have a material impact on the registrant's business strategy, results of operations, or financial condition;
- The actual and potential material impacts of any identified climate-related risks on the registrant's strategy, business model, and outlook;
- If, as part of its strategy, a registrant has undertaken activities to mitigate or adapt to a material climate-related risk, a quantitative and qualitative description of material expenditures incurred and material impacts on financial estimates and assumptions that directly result from such mitigation or adaptation activities;
- Specified disclosures regarding a registrant's activities, if any, to mitigate or adapt to a material climate-related risk including the use, if any, of transition plans, scenario analysis, or internal carbon prices;
- Any oversight by the board of directors of climate-related risks and any role by management in assessing and managing the registrant's material climate-related risks;
- Any processes the registrant has for identifying, assessing, and managing material climate-related risks and, if the registrant is managing those risks, whether and how any such processes are integrated into the registrant's overall risk management system or processes;
- Information about a registrant's climate-related targets or goals, if any, that have materially affected or are reasonably likely to materially affect the registrant's business, results of operations, or financial condition. Disclosures would include material expenditures and material impacts on financial estimates and assumptions as a direct result of the target or goal or actions taken to make progress toward meeting such target or goal;
- For large accelerated filers (LAFs) and accelerated filers (AFs) that are not otherwise exempted, information about material Scope 1 emissions and/or Scope 2 emissions;
- For those required to disclose Scope 1 and/or Scope 2 emissions, an assurance report at the limited assurance level, which, for an LAF, following an additional transition period, will be at the reasonable assurance level;
- The capitalized costs, expenditures expensed, charges, and losses incurred as a result of severe weather events and other natural conditions, such as hurricanes, tornadoes, flooding, drought, wildfires, extreme temperatures,

- and sea level rise, subject to applicable one percent and de minimis disclosure thresholds, disclosed in a note to the financial statements;
- The capitalized costs, expenditures expensed, and losses related to carbon offsets and renewable energy credits or certificates (RECs) if used as a material component of a registrant's plans to achieve its disclosed climate-related targets or goals, disclosed in a note to the financial statements; and
 - If the estimates and assumptions a registrant uses to produce the financial statements were materially impacted by risks and uncertainties associated with severe weather events and other natural conditions or any disclosed climate-related targets or transition plans, a qualitative description of how the development of such estimates and assumptions was impacted, disclosed in a note to the financial statements.

Before adopting the final rules, the Commission considered more than 24,000 comment letters, including more than 4,500 unique letters, submitted in response to the rules' proposing release issued in March 2022.

The adopting release is published on SEC.gov at:
<https://www.sec.gov/files/rules/final/2024/33-11275.pdf>

SECURITIES AND EXCHANGE COMMISSION

17 CFR 210, 229, 230, 232, 239, and 249

[Release Nos. 33-11275; 34-99678; File No. S7-10-22]

RIN 3235-AM87

The Enhancement and Standardization of Climate-Related Disclosures for Investors

AGENCY: Securities and Exchange Commission

ACTION: Final rules.

It will be published in the Federal Register. The final rules will become effective 60 days following publication of the adopting release in the Federal Register, and compliance dates for the rules will be phased in for all registrants, with the compliance date dependent on the registrant's filer status.

To read more: <https://www.sec.gov/news/press-release/2024-31>

Tailoring, Fidelity to the Rule of Law, and Unintended Consequences

Governor Michelle W. Bowman, at the Harvard Law School Faculty Club, Cambridge, Massachusetts



Thank you for the invitation to join you this evening at Harvard Law School.¹ It is an honor and a pleasure to speak to this distinguished group. To kick off our conversation, I would like to frame the discussion by offering my views on a key element underpinning the U.S. bank regulatory framework: the role of tailoring.

While the principle itself is simple—setting regulatory priorities and allocating supervisory resources in a risk-based way—the consequences of tailoring (or not) can reverberate throughout the banking system, the broader U.S. financial system, and the economy.

I see a clear nexus between tailoring and fidelity to the law, including a targeted focus within our statutorily mandated prudential responsibilities.

Tailoring as a Grounding Principle

I have long been a proponent of tailoring and continue to consider it a strong foundational principle upon which to apply bank regulation and supervision.

This approach ensures a focus on the most critical risks over time, avoiding the over-allocation of resources or imposition of unnecessary costs on the banking system.

When we approach rulemaking with a commitment to tailoring, and to our broader prudential mandates, the public can judge our actions by how well they serve these ends, and they should rightly be concerned when regulatory actions seem to serve other goals.

In this sense, tailoring keeps policymakers grounded and facilitates appropriate prioritization. Tailoring also allows us to allocate limited supervisory resources to most effectively support safety and soundness of the banking system and U.S. financial stability.

In accordance with the law, the Federal Reserve, both in its monetary policy function and in the execution of its bank regulatory and supervisory responsibilities, is meant to operate independently and apolitically. But banking regulators have a responsibility to act in a way that proves this independence is warranted. We earn the right to operate with this independence when we consistently follow the law and achieve our prudential objectives.

One of the most effective ways we accomplish this goal is through the appropriate prioritization of risks in the financial system. Regardless of the approach to bank regulation and supervision, bank regulators should be subject to oversight and accountability, to both Congress and the public.

The principles that guide the execution of prudential responsibilities matter, especially when they further efficiency and effectiveness. Congress has embedded the concept of tailoring within the Federal Reserve's regulatory mandates, including the Economic Growth, Regulatory Relief, and Consumer Protection Act, commonly referred to as S. 2155.

This law revised provisions of the Dodd-Frank Act, amending the threshold for tailored application of enhanced prudential standards on certain regulated institutions.

Notably, S. 2155 did not introduce tailoring to these standards; it merely modified tailoring thresholds and mandated the Board implement this approach. To be clear, tailoring is not a pretext for deregulation but rather a principle that allows regulators to pursue required statutory objectives in the most efficient and effective way.

Does Tailoring Need a Defender?

I suppose one could view my support for tailoring as merely setting up a straw man; surely everyone agrees with tailoring in principle?

On a superficial level, it is hard to argue with the principle that regulatory tailoring—matching regulation and supervision to risk—is a prudent approach for bank regulators. And yet the rhetoric supporting tailoring and risk-based supervision often does not match regulatory reform efforts or supervisory approaches.

The criticisms rarely manifest as skepticism of the principle itself. Rather, they are implicit in the approach to regulation and supervisory guidance or are disguised as a criticism of the execution of tailoring.

Both the pending capital reform proposals and the final climate guidance illustrate how regulatory actions can deviate from the principle of tailoring without any express recognition of this effect.

The federal banking agencies have proposed several reforms to the capital framework, among them the Basel III "endgame" and new long-term debt requirements that would apply to all banks with over \$100 billion in assets.

I have expressed concern with both of these proposals on the merits, in terms of striking the right balance between safety and soundness and efficiency and fairness, and out of concern for potential unintended consequences. Another concern is whether these proposals show fidelity to the law, which requires regulatory tailoring above the \$100 billion asset threshold.

In 2019, the Board published its regulatory tailoring rule and included a compelling visual (PDF) that depicts in table form how a series of requirements—capital, single counterparty credit limits, liquidity, and the requirement to form a U.S. Intermediate Holding Company for foreign banking organizations—worked collectively to establish a tiered framework.

If you superimpose the pending capital reform proposals on the table, there is a "flattening" of requirements in the capital bucket.

Of course, this simple exercise does not reflect the unknown end state of the bank regulatory framework, and the current desire among some policymakers to modify liquidity requirements.

These individual efforts highlight the hazard of piecemeal reforms, especially those that are closely related in their end-state operation, like capital and long-term debt requirements.

When regulators pursue reforms by creating separate rulemaking silos, we limit our capacity to not only ensure fidelity to tailoring but also fidelity to our prudential mandates. Even when proposals have concurrent comment periods, the danger is that the final regulations will be miscalibrated and not appropriately tailored.

Tailoring underpins not only effective regulation, but also effective bank supervision. The effectiveness of the interagency principles used by the Federal Reserve, the Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency for the management of climate-related financial risks could be evaluated as a supervisory tool through the lens of tailoring, which requires us to consider both the regulatory threshold for applicability and the content of the guidance.

One approach to evaluate the merit and effectiveness of these principles as a supervisory tool is through the lens of tailoring, which requires us to consider both the regulatory threshold for applicability and the content of the guidance.

On its face, it applies to banks with \$100 billion or more in consolidated assets. What does this threshold mean in practice? Guidance serves the role of illuminating supervisory priorities and expectations. These informal communications help bridge the divide between regulators and regulated entities.

When guidance notes that "all financial institutions, regardless of size, may have material exposures to climate-related financial risks...", my intuition is that banks will take little comfort from the nominal carveout in light of this language. Apart from the general concern with the "cliff effect" threshold at \$100 billion, I question whether any size threshold will apply in practice.

The content of the guidance—and its expectations for larger banks—suggests that the motivation behind the principles is neither prudential considerations nor to further regulatory tailoring, as it has a somewhat tenuous connection to core safety and soundness considerations and seems destined to trickle down to smaller firms over time.

Banks have long been exposed to climate- and weather-related financial risks and have long been required to manage all of their material risks, including these. But the principles seem oriented toward contributing to a policy matter that extends well beyond prudential bank regulation—namely how the U.S. and other governments around the world should address climate change. And the principles seem focused on highly uncertain risks well outside the normal temporal horizon of a bank supervisor.

One could reasonably ask, do the principles result in appropriate, risk-based prioritization of supervisory concerns? It is possible that they prioritize risks that may not be the most relevant for safety and soundness and may effectively influence credit allocation decisions through regulations that are not driven primarily by prudential considerations.

Bank regulators can acknowledge the importance of questions around climate change while also hewing to their statutory responsibilities. Promoting safety and soundness and U.S. financial stability is a weighty enough task without taking on other causes.

The current regulatory agenda includes many other examples where similar arguments can be made that regulatory reform proposals lack sufficient attention to regulatory tailoring and thereby fail to further statutory directives to tailor certain requirements and, more importantly, to address the condition of the banking system.

Apart from substantive deviations from regulatory tailoring, there are also indirect attacks on the value of tailoring as a principle to guide bank regulatory reforms.

For example, one prominent argument raised shortly after the failure of Silicon Valley Bank, and which has become a driving force in regulatory reform efforts, is that the Board's approach to tailoring was to blame for the bank failures and broader banking stress.

The argument is that a major factor contributing to the bank failures was the implementation of S. 2155, the statutory mandate to tailor regulation and an accompanying shift in supervisory policy.

As I have noted many times in the past, I find little evidence to support this claim. While couched as a critique of the execution of tailoring, this argument also seems to challenge the value of tailoring, asserting that a simple solution would be to unwind regulatory tailoring and eliminate risk-based tailoring in supervision.

Taking ownership and accountability of the supervisory issues that significantly contributed to the banking system stress last spring enables us to look critically at the approach to regulation and supervision in the lead-up to these failures, and appropriately address the shortcomings.

To read more:

<https://www.federalreserve.gov/newsevents/speech/bowman20240305a.htm>

NIST Releases Version 2.0 of Landmark Cybersecurity Framework



- NIST's cybersecurity framework (CSF) now explicitly aims to help all organizations — not just those in critical infrastructure, its original target audience — to manage and reduce risks.
- NIST has updated the CSF's core guidance and created a suite of resources to help all organizations achieve their cybersecurity goals, with added emphasis on governance as well as supply chains.
- This update is the outcome of a multiyear process of discussions and public comments aimed at making the framework more effective.

The National Institute of Standards and Technology (NIST) has updated the widely used Cybersecurity Framework (CSF), its landmark guidance document for reducing cybersecurity risk.

The new 2.0 edition is designed for all audiences, industry sectors and organization types, from the smallest schools and nonprofits to the largest agencies and corporations — regardless of their degree of cybersecurity sophistication.

In response to the numerous comments received on the draft version, NIST has expanded the CSF's core guidance and developed related resources to help users get the most out of the framework. These resources are designed to provide different audiences with tailored pathways into the CSF and make the framework easier to put into action.

“The CSF has been a vital tool for many organizations, helping them anticipate and deal with cybersecurity threats,” said Under Secretary of Commerce for Standards and Technology and NIST Director Laurie E. Locascio.

“CSF 2.0, which builds on previous versions, is not just about one document. It is about a suite of resources that can be customized and used individually or in combination over time as an organization's cybersecurity needs change and its capabilities evolve.”

The CSF 2.0, which supports implementation of the National Cybersecurity Strategy, has an expanded scope that goes beyond protecting critical infrastructure, such as hospitals and power plants, to all organizations in any sector.

It also has a new focus on governance, which encompasses how organizations make and carry out informed decisions on cybersecurity strategy. The CSF's governance component emphasizes that cybersecurity is a major source of enterprise risk that senior leaders should consider alongside others such as finance and reputation.

“Developed by working closely with stakeholders and reflecting the most recent cybersecurity challenges and management practices, this update aims to make the framework even more relevant to a wider swath of users in the United States and abroad,” according to Kevin Stine, chief of NIST’s Applied Cybersecurity Division.

Following a presidential Executive Order, NIST first released the CSF in 2014 to help organizations understand, reduce and communicate about cybersecurity risk. The framework’s core is now organized around six key functions: Identify, Protect, Detect, Respond and Recover, along with CSF 2.0’s newly added Govern function. When considered together, these functions provide a comprehensive view of the life cycle for managing cybersecurity risk.

The updated framework anticipates that organizations will come to the CSF with varying needs and degrees of experience implementing cybersecurity tools. New adopters can learn from other users’ successes and select their topic of interest from a new set of implementation examples and quick-start guides designed for specific types of users, such as small businesses, enterprise risk managers, and organizations seeking to secure their supply chains.

A new CSF 2.0 Reference Tool now simplifies the way organizations can implement the CSF, allowing users to browse, search and export data and details from the CSF’s core guidance in human-consumable and machine-readable formats.

In addition, the CSF 2.0 offers a searchable catalog of informative references that shows how their current actions map onto the CSF. This catalog allows an organization to cross-reference the CSF’s guidance to more than 50 other cybersecurity documents, including others from NIST, such as SP 800-53 Rev. 5, a catalog of tools (called controls) for achieving specific cybersecurity outcomes.

Organizations can also consult the Cybersecurity and Privacy Reference Tool (CPRT), which contains an interrelated, browsable and downloadable set of NIST guidance documents that contextualizes these NIST resources, including the CSF, with other popular resources. And the CPRT offers ways to communicate these ideas to both technical experts and the C-suite, so that all levels of an organization can stay coordinated.

NIST plans to continue enhancing its resources and making the CSF an even more helpful resource to a broader set of users, Stine said, and feedback from the community will be crucial.

“As users customize the CSF, we hope they will share their examples and successes, because that will allow us to amplify their experiences and help others,” he said. “That will help organizations, sectors and even entire nations better understand and manage their cybersecurity risk.”

The CSF is used widely internationally; Versions 1.1 and 1.0 have been translated into 13 languages, and NIST expects that CSF 2.0 also will be translated by volunteers around the world. Those translations will be added to NIST’s expanding portfolio of CSF resources.

Over the last 11 years, NIST's work with the International Organization for Standardization (ISO), in conjunction with the International Electrotechnical Commission (IEC), has helped to align multiple cybersecurity documents.

ISO/IEC resources now allow organizations to build cybersecurity frameworks and organize controls using the CSF functions. NIST plans to continue working with ISO/IEC to continue this international alignment.



<p>CSF 2.0</p> <p>For industry, government, and organizations to reduce cybersecurity risks</p> <p>Read the Document</p>	<p>Quick Start Guides</p> <p>For users with specific common goals</p> <p>View the Quick Start Guides</p>
<p>CSF 2.0 Profiles</p> <p>Templates and useful resources for creating and using both CSF profiles</p> <p>See the Profiles</p>	<p>Informative References (Mappings)</p> <p>See how NIST's resources overlap and share themes</p> <p>See the Mappings</p>

To read more: <https://www.nist.gov/cyberframework>

WhatsApp, text messages, Off-Channel Communications – Be careful

This time the compliance failure comes from Broker-Dealers and Investment Advisers



Sixteen Firms to Pay More Than \$81 Million Combined to Settle Charges for Widespread Recordkeeping Failures.

The Securities and Exchange Commission announced charges against five broker-dealers, seven dually registered broker-dealers and investment advisers, and four affiliated investment advisers for widespread and longstanding failures by the firms and their employees to **maintain and preserve electronic communications**.

The firms admitted the facts set forth in their respective SEC orders, acknowledged that their conduct violated recordkeeping provisions of the federal securities laws, agreed to pay combined civil penalties of more than \$81 million, as outlined below, and have begun implementing improvements to their compliance policies and procedures to address these violations.

“Today’s actions against these 16 firms result from our continuing efforts to ensure that all regulated entities comply with the recordkeeping requirements, which are essential to our ability to monitor and enforce compliance with the federal securities laws,” said Gurbir S. Grewal, Director of the SEC’s Division of Enforcement. “Once again, one of these orders is not like the others: Huntington’s penalty reflects its voluntary self-report and cooperation.”

The SEC’s investigations uncovered pervasive and longstanding uses of **unapproved communication** methods, known as off-channel communications, at all 16 firms. As described in the SEC’s orders, the broker-dealer firms admitted that, from at least 2019 or 2020, their employees communicated through **personal text messages** about the business of their employers.

The investment adviser firms admitted that their employees sent and received **off-channel** communications related to **recommendations** made or proposed to be made and advice given or proposed to be given.

The firms did not maintain or preserve the substantial majority of these off-channel communications, in violation of the federal securities laws. By failing to maintain and preserve required records, some of the firms likely deprived the SEC of these off-channel communications in various SEC investigations.

The failures involved employees at multiple levels of authority, including supervisors and senior managers.

In addition to the significant financial penalties, each of the firms was ordered to cease and desist from future violations of the relevant recordkeeping provisions and was censured.

The firms also agreed to retain independent compliance consultants to, among other things, conduct comprehensive reviews of their policies and procedures relating to the retention of electronic communications found on personal devices and their respective frameworks for addressing non-compliance by their employees with those policies and procedures.

To read more: <https://www.sec.gov/news/press-release/2024-18>

FCC Makes AI-Generated Voices in Robocalls Illegal



The Federal Communications Commission regulates U.S. interstate and international communications by radio, television, wire, satellite, and cable in all 50 states, the District of Columbia and U.S. territories. An independent U.S. government agency overseen by Congress, the Commission is the federal agency responsible for implementing and enforcing America's communications law and regulations.

The Federal Communications Commission announced the unanimous adoption of a Declaratory Ruling that recognizes calls made with AI-generated voices are “artificial” under the Telephone Consumer Protection Act (TCPA).

The ruling, which takes effect immediately, [makes voice cloning technology used in common robocall scams targeting consumers illegal](#). This would give State Attorneys General across the country new tools to go after bad actors behind these nefarious robocalls.

“Bad actors are using AI-generated voices in unsolicited robocalls to extort vulnerable family members, imitate celebrities, and misinform voters. We’re putting the fraudsters behind these robocalls on notice,” said FCC Chairwoman Jessica Rosenworcel. “State Attorneys General will now have new tools to crack down on these scams and ensure the public is protected from fraud and misinformation.”

The rise of these types of calls has escalated during the last few years as this technology now has the potential to confuse consumers with misinformation by imitating the voices of celebrities, political candidates, and close family members.

While currently State Attorneys General can target the outcome of an unwanted AI-voice generated robocall—such as the scam or fraud they are seeking to perpetrate—this action now makes the act of using AI to generate the voice in these robocalls itself illegal, expanding the legal avenues through which state law enforcement agencies can hold these perpetrators accountable under the law.

In November of 2023, the FCC launched a Notice of Inquiry to build a record on how the agency can combat illegal robocalls and how AI might be involved.

The agency asked questions on how AI might be used for scams that arise out of junk calls, by mimicking the voices of those we know, and whether this technology should be subject to oversight under the TCPA.

Similarly, the FCC also asked about how AI can help us with pattern recognition so that we turn this technology into a force for good that can recognize illegal robocalls before they ever reach consumers on the phone. The Telephone Consumer Protection Act is the primary law the FCC uses to help limit junk calls.

It restricts the making of telemarketing calls and the use of automatic telephone dialing systems and artificial or prerecorded voice messages. Under FCC rules, it also requires telemarketers to obtain prior express written consent from consumers before robocalling them.

This Declaratory Ruling ensures AI-generated voices in calls are also held to those same standards. The TCPA gives the FCC civil enforcement authority to fine robocallers.

The Commission can also take steps to block calls from telephone carriers facilitating illegal robocalls. In addition, the TCPA allows individual consumers or an organization to bring a lawsuit against robocallers in court.

Lastly, State Attorneys General have their own enforcement tools which may be tied to robocall definitions under the TCPA. A coalition of 26 State Attorneys General—more than half of the nation’s AGs—recently wrote to the FCC supporting this approach.

By taking this step, the FCC is building on its work to establish partnerships with law enforcement agencies in states across the country to identify and eliminate illegal robocalls.

These partnerships can provide critical resources for building cases and coordinating efforts to protect consumers and businesses nationwide. The FCC offers partner states not only the expertise of its enforcement staff but also important resources and remedies to support state investigations.

To read more: <https://www.fcc.gov/document/fcc-makes-ai-generated-voices-robocalls-illegal>

Basel Committee agrees to revisions to Basel Core Principles



- Basel Committee approves revisions to Core principles for effective banking supervision.
- Decides to consult on potential measures to address window-dressing behaviour by some banks in the context of the framework for global systemically important banks.
- Reaffirms expectation that all aspects of Basel III will be implemented in full, consistently and as soon as possible.

The Basel Committee on Banking Supervision met on 28–29 February 2024 in Madrid to take stock of recent market developments and risks to the global banking system, and to discuss a range of policy and supervisory initiatives.

Risks and vulnerabilities to the global banking system

The Committee discussed the outlook for the global banking system in the light of recent economic and financial market developments. It discussed risks to banks from sectors facing headwinds, including segments of commercial real estate.

Members also discussed banks' interconnections with non-bank financial intermediaries, including the growing role of private credit. Banks and supervisors need to remain vigilant to emerging risks in these areas.

Basel Core Principles

The Committee discussed the comments received to its consultation on revisions to the Core principles for effective banking supervision (Basel Core Principles). Drawing on the inputs received from a wide range of stakeholders, the Committee [approved](#) the final revisions to the Core Principles, which draw on supervisory insights and structural changes to the banking system since the previous update in 2012.

[The final standard will be published following the International Conference of Banking Supervisors on 24–25 April 2024.](#)

Global systemically important banks and window-dressing

Building on the discussion at its previous meeting, the Committee looked at a range of empirical analyses that highlight window-dressing behaviour by some banks in the context of the framework for global systemically important banks (G-SIBs).

Such regulatory arbitrage behaviour seeks to temporarily reduce banks' perceived systemic footprint around the reference dates used for the reporting and public disclosure of the G-SIB scores.

As noted previously by the Committee, window-dressing by banks undermines the intended policy objectives of the Committee's standards and risks disrupting the operations of financial markets. To that end, the Committee agreed to consult on potential measures aimed at reducing window-dressing behaviour.

The consultation paper, and an accompanying working paper summarising the empirical analyses, will be published next month. The Committee also agreed to publish a working paper on an assessment of the G-SIB score dynamics over the past decade.

Climate-related financial risks

As part of its holistic approach to addressing climate-related financial risks, the Committee discussed the role of scenario analysis in assessing the resilience of banks' business models, strategies and overall risk profile to a range of plausible climate-related pathways. Members noted that the field of scenario analysis is dynamic, with practices expected to evolve rapidly as climate science advances.

Building on its existing supervisory principles, the Committee agreed to publish a discussion paper on the use of climate scenario analysis by banks and supervisors to help inform potential future work in this area. The discussion paper will be published in the coming months.

Implementation of Basel III reforms

The Committee took stock of the implementation status of the outstanding Basel III standards, which were finalised in 2017. Committee members have continued to make good progress with implementation, though it remains uneven.

Members unanimously reaffirmed their expectation of implementing all aspects of the Basel III framework in full, consistently and as soon as possible. Members also approved a workplan for the jurisdictional assessments of the implementation of these standards as part of the Committee's Regulatory Consistency Assessment Programme.

To read more: <https://www.bis.org/press/p240229.htm>

Sources of Uncertainty in the Short Run and the Long Run

Governor Lisa D. Cook, at "Macrofinance in the Long Run: New Insights on the Global Economy" 2024 Annual Conference of the Julis-Rabinowitz Center for Public Policy & Finance at Princeton's School of Public and International Affairs, Princeton, New Jersey



Thank you, Gianluca, and thank you for the opportunity to speak to you today.

Let me begin by recognizing the Department of Economics at Princeton for its history of nurturing and supporting scholars in reaching their full potential.

Some of the most important, transformative conversations I have had in my career have happened on this campus and with economists making significant contributions to the field. Let me start with the last time I was here.

When I was a post doc at Stanford, I emailed Alan Krueger out of the blue and attached an early version of a new paper, asking him if he would meet with me for an hour to discuss it.

Because of his experience with large data sets, and his curiosity, thoughtfulness, and generosity, one hour turned into three hours. And he brought along a new assistant professor, Dean Karlan.

Not only did I learn a tremendous amount from Alan during that encounter, almost ten years later, I learned even more from him working as a senior economist at the Council of Economic Advisers when Alan was Chair.

It is a great legacy of your department that you provided the conditions and support for Alan to make his seminal contributions to economics.

I think similar conditions were in place at Princeton to allow Sir Arthur Lewis, the only person of African descent to receive the Nobel Prize in economics, to be productive and thrive.

While I never met him, Sir Arthur has been an inspiration throughout my career, and I am grateful for his contribution that was aided by Princeton.

The good work done here continues with the subject at hand today. The focus of this conference on macrofinance in the long run provides a good opportunity to reflect on what has changed and what has not changed since the onset of the pandemic four years ago.

A feature of the past few years has been heightened uncertainty about how the economy would emerge from the turmoil of the pandemic and the subsequent recovery.

I will talk about some types of uncertainty I see as having diminished recently and others that remain elevated. Then I will conclude with a discussion of my views on current monetary policy.

When the global pandemic hit in the spring of 2020, economies around the world shut down or sharply limited activity, especially for in-person services. Policymakers took action to support incomes and limit the scarring from those temporary shutdowns.

During the post-pandemic recovery in 2021 and 2022, as strong aggregate demand met still-constrained supply, inflation in many economies rose to levels not seen in decades.

Uncertainty about the future course of inflation and the supply side of the economy was high, both in the short run and in the longer run.

Would supply remain persistently depressed because of scarring from the pandemic? Would inflation become stuck well above the Fed's 2 percent target or even continue to rise?

To read more:

<https://www.federalreserve.gov/newsevents/speech/cook20240222a.htm>

Announcing Microsoft's open automation framework to red team generative AI Systems

By Ram Shankar Siva Kumar, Microsoft AI Red Team Lead



Today we are releasing an open automation framework, **PyRIT (Python Risk Identification Toolkit for generative AI)**, to empower security professionals and machine learning engineers to proactively find risks in their generative AI systems.

The Python Risk Identification Tool for generative AI (PyRIT) is an open access automation framework to empower security professionals and machine learning engineers to proactively find risks in their generative AI systems.

At Microsoft, we believe that security practices and generative AI responsibilities need to be a collaborative effort.

We are deeply committed to developing tools and resources that enable every organization across the globe to innovate responsibly with the latest artificial intelligence advances.

This tool, and the previous investments we have made in red teaming AI since 2019, represents our ongoing commitment to democratize securing AI for our customers, partners, and peers.

The need for automation in AI Red Teaming

Red teaming AI systems is a complex, multistep process. Microsoft's AI Red Team leverages a dedicated interdisciplinary group of security, adversarial machine learning, and responsible AI experts.

The Red Team also leverages resources from the entire Microsoft ecosystem, including the Fairness center in Microsoft Research; AETHER, Microsoft's cross-company initiative on AI Ethics and Effects in Engineering and Research; and the Office of Responsible AI.

Our red teaming is part of our larger strategy to map AI risks, measure the identified risks, and then build scoped mitigations to minimize them.

Over the past year, we have proactively red teamed several high-value generative AI systems and models before they were released to customers.

Through this journey, we found that red teaming generative AI systems is markedly different from red teaming classical AI systems or traditional software in three prominent ways.

1. Probing both security and responsible AI risks simultaneously

We first learned that while red teaming traditional software or classical AI systems mainly focuses on identifying security failures, red teaming generative AI systems includes identifying both security risk as well as responsible AI risks.

Responsible AI risks, like security risks, can vary widely, ranging from generating content that includes fairness issues to producing ungrounded or inaccurate content. AI red teaming needs to explore the potential risk space of security and responsible AI failures simultaneously.

2. Generative AI is more probabilistic than traditional red teaming

Secondly, we found that red teaming generative AI systems is more probabilistic than traditional red teaming.

Put differently, executing the same attack path multiple times on traditional software systems would likely yield similar results. However, generative AI systems have multiple layers of non-determinism; in other words, the same input can provide different outputs.

This could be because of the app-specific logic; the generative AI model itself; the orchestrator that controls the output of the system can engage different extensibility or plugins; and even the input (which tends to be language), with small variations can provide different outputs.

Unlike traditional software systems with well-defined APIs and parameters that can be examined using tools during red teaming, we learned that generative AI systems require a strategy that considers the probabilistic nature of their underlying elements.

3. Generative AI systems architecture varies widely

Finally, the architecture of these generative AI systems varies widely: from standalone applications to integrations in existing applications to the input and output modalities, such as text, audio, images, and videos.

These three differences make a triple threat for manual red team probing.

To surface just one type of risk (say, generating violent content) in one modality of the application (say, a chat interface on browser), red teams need to try different strategies multiple times to gather evidence of potential failures. Doing this manually for all types of harms, across all modalities across different strategies, can be exceedingly tedious and slow.

This does not mean automation is always the solution. Manual probing, though time-consuming, is often needed for identifying potential blind spots.

Automation is needed for scaling but is not a replacement for manual probing. We use automation in two ways to help the AI red team: automating our routine tasks and identifying potentially risky areas that require more attention.

In 2021, Microsoft developed and released a red team automation framework for classical machine learning systems. Although Counterfit still delivers value for traditional machine learning systems, we found that for generative AI applications, Counterfit did not meet our needs, as the underlying principles and the threat surface had changed.

Because of this, we re-imagined how to help security professionals to red team AI systems in the generative AI paradigm and our new toolkit was born.

We like to acknowledge out that there have been work in the academic space to automate red teaming such as PAIR and open source projects including garak.

To read more: <https://www.microsoft.com/en-us/security/blog/2024/02/22/announcing-microsofts-open-automation-framework-to-red-team-generative-ai-systems/>

Digital Services Act starts applying to all online platforms in the EU



On 17 February, the Digital Services Act (DSA), the EU's landmark rulebook that aims to make the online environment safer, fairer and more transparent, starts applying to all online intermediaries in the EU.

Under the DSA, EU users are better protected against illegal goods and content and have their rights upheld on online platforms where they connect with other users, share information, or buy products.

New responsibilities for platforms and empowered users

All online platforms with users in the EU, with the exception of small and micro enterprises employing fewer than 50 persons and with an annual turnover below €10 million, must implement measures to:

- Counter illegal content, goods, and services: online platforms must provide users with means to flag illegal content, including goods and services. More so, online platforms will have to cooperate with 'trusted flaggers', specialised entities whose notices will have to be given priority by platforms.
- Protect minors: including a complete ban of targeting minors with ads based on profiling or on their personal data.
- Empower users with information about advertisements they see, such as why the ads are being shown to them and on who paid for the advertisement.
- Ban advertisements that target users based on sensitive data, such as political or religious beliefs, sexual preferences, etc.
- Provide statements of reasons to a user affected by any content moderation decision, e.g., content removal, account suspension, etc. and upload the statement of reasons to the DSA Transparency database.
- Provide users with access to a complaint mechanism to challenge content moderation decisions.
- Publish a report of their content moderation procedures at least once per year.
- Provide the user with clear terms and conditions, and include the main parameters based on which their content recommender systems work.
- Designate a point of contact for authorities, as well as users.

In addition to online platforms, the Digital Services Act also applies to hosting services (e.g. cloud services or domain name systems, background services which connect users to requested website addresses), as well as to online intermediaries (e.g. internet service providers, or domain). Hosting services and online intermediaries are subject to a subset of obligations under the DSA.

Since end of August 2023, the DSA has already applied to the 19 Very Large Online Platforms (VLOPs) and Search Engines (VLOSEs) designated in April 2023 (with more than 45 million monthly users on average). Three other platforms designated as VLOPs in December 2023 have until end of April to comply with the most stringent obligations under the DSA. However, they will have to comply with the general DSA obligations from tomorrow.

Digital Services Coordinators in Member States

Platforms not designated as VLOPs or VLOSEs will be supervised at Member State level by an independent regulator acting as the national Digital Services Coordinator (DSC). It will be the responsibility of the DSCs to ensure that these platforms play by the rules. DSCs will supervise and enforce the DSA for the platforms established on their territory.

In practice, the Digital Services Coordinators will:

- Be the first port of call for complaints by users on infringements against the DSA by any platform, including VLOPs and VLOSEs. The Digital Services Co-ordinator will, when appropriate, transmit the complaint to the Digital Services Co-ordinator of the platform's Member State of establishment, where appropriate, accompanied by an opinion.
- Certify existing out-of-court appeal mechanisms for users to address complaints and challenge content moderation decisions.
- Assess and award the status of trusted flaggers to suitable applicants, or independent entities that have demonstrated expertise in detecting, identifying, and notifying illegal content online.
- Process researchers' requests for access to VLOPs and VLOSEs data for specific research. The DSCs will vet the researchers and request access to data on their behalf.
- Be equipped with strong investigation and enforcement powers, to ensure compliance with the DSA by the providers established in their territory.

They will be able to order inspections following a suspected infringement of the DSA, impose fines on online platforms failing to comply with the DSA, and impose interim measures in case of serious harm to the public sphere.

The European Board for Digital Services

The Digital Services Coordinators and the Commission will form an independent advisory group, the European Board for Digital Services, to ensure that the DSA is applied consistently, and that users across the EU enjoy the same rights, regardless of where the online platforms are established.

The Board will be consulted on the enforcement of the DSA and advise on arising issues related to the DSA and can contribute to guidelines and analysis. It will also assist in the supervision of Very Large Online Platforms and Very Large Online Search Engines and will issue yearly reports on the prominent systemic risks and best practices in mitigating them.

Next Steps

In **March 2024**, the Commission intends to adopt Guidelines on risk mitigation measures for **electoral processes**.

A public consultation on the data access delegated act is expected in April with adoption by July and entry into force in **October 2024**.

In **May**, the Commission plans to adopt an Implementing Act on transparency report templates.

To read more:

https://ec.europa.eu/commission/presscorner/detail/en/ip_24_881

Disrupting malicious uses of AI by state-affiliated threat actors



We terminated accounts associated with state-affiliated threat actors. Our findings show our models offer only limited, incremental capabilities for malicious cybersecurity tasks.

We build AI tools that improve lives and help solve complex challenges, but we know that malicious actors will sometimes try to abuse our tools to harm others, including in furtherance of cyber operations. Among those malicious actors, state-affiliated groups—which may have access to advanced technology, large financial resources, and skilled personnel—can pose unique risks to the digital ecosystem and human welfare.

In partnership with Microsoft Threat Intelligence, we have disrupted five state-affiliated actors that sought to use AI services in support of malicious cyber activities. We also outline our approach to detect and disrupt such actors in order to promote information sharing and transparency regarding their activities.

Disruption of threat actors

Based on collaboration and information sharing with Microsoft, we disrupted five state-affiliated malicious actors: two China-affiliated threat actors known as Charcoal Typhoon and Salmon Typhoon; the Iran-affiliated threat actor known as Crimson Sandstorm; the North Korea-affiliated actor known as Emerald Sleet; and the Russia-affiliated actor known as Forest Blizzard. The identified OpenAI accounts associated with these actors were terminated.

These actors generally sought to use OpenAI services for querying open-source information, translating, finding coding errors, and running basic coding tasks.

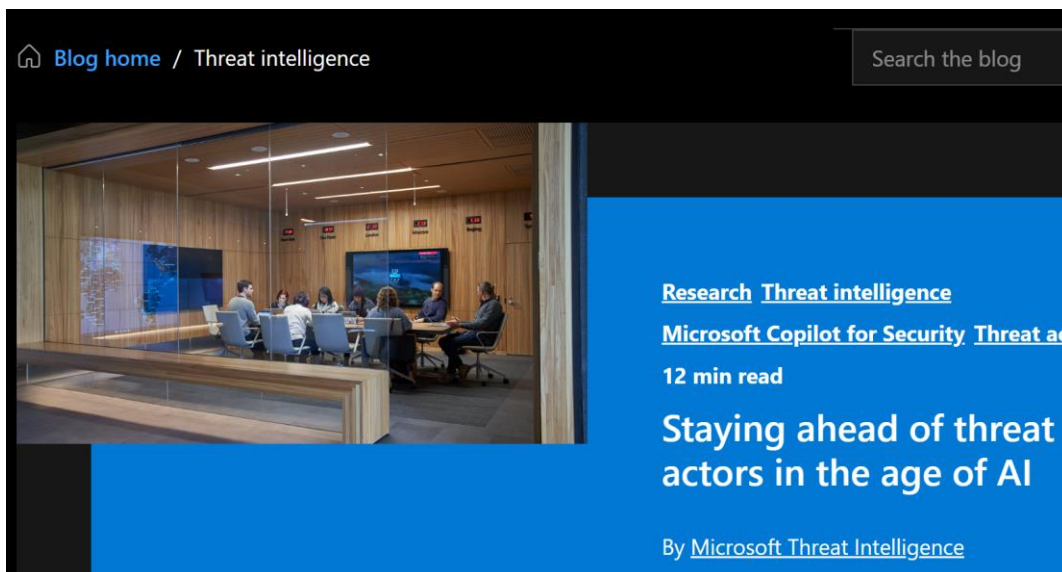
Specifically:

- Charcoal Typhoon used our services to research various companies and cybersecurity tools, debug code and generate scripts, and create content likely for use in phishing campaigns.
- Salmon Typhoon used our services to translate technical papers, retrieve publicly available information on multiple intelligence agencies and regional threat actors, assist with coding, and research common ways processes could be hidden on a system.
- Crimson Sandstorm used our services for scripting support related to app and web development, generating content likely for spear-phishing campaigns, and researching common ways malware could evade detection.
- Emerald Sleet used our services to identify experts and organizations focused on defense issues in the Asia-Pacific region, understand publicly

available vulnerabilities, help with basic scripting tasks, and draft content that could be used in phishing campaigns.

- Forest Blizzard used our services primarily for open-source research into satellite communication protocols and radar imaging technology, as well as for support with scripting tasks.

Additional technical details on the nature of the threat actors and their activities can be found in the Microsoft blog post: <https://www.microsoft.com/en-us/security/blog/2024/02/14/staying-ahead-of-threat-actors-in-the-age-of-ai/>



The activities of these actors are consistent with previous red team assessments we conducted in partnership with external cybersecurity experts, which found that GPT-4 offers only limited, incremental capabilities for malicious cybersecurity tasks beyond what is already achievable with publicly available, non-AI powered tools.

A multi-pronged approach to AI safety

Although the capabilities of our current models for malicious cybersecurity tasks are limited, we believe it's important to stay ahead of significant and evolving threats. To respond to the threat, we are taking a multi-pronged approach to combating malicious state-affiliate actors' use of our platform:

- *Monitoring and disrupting malicious state affiliated actors.* We invest in technology and teams to identify and disrupt sophisticated threat actors' activities. Our Intelligence and Investigations team—working in concert with our Safety, Security, and Integrity teams—investigates malicious actors in a variety of ways, including using our models to pursue leads, analyze how adversaries are interacting with our platform, and assess their broader intentions. Upon detection, OpenAI takes appropriate action to disrupt their activities, such as disabling their accounts, terminating services, or limiting access to resources.

- *Working together with the AI ecosystem.* OpenAI collaborates with industry partners and other stakeholders to regularly exchange information about malicious state-affiliated actors' detected use of AI. This collaboration reflects our voluntary commitment to promote the safe, secure and transparent development and use of AI technology, and aims to promote collective responses to ecosystem-wide risks via information sharing.
- *Iterating on safety mitigations.* Learning from real-world use (and misuse) is a key component of creating and releasing increasingly safe AI systems over time. We take lessons learned from these actors' abuse and use them to inform our iterative approach to safety. Understanding how the most sophisticated malicious actors seek to use our systems for harm gives us a signal into practices that may become more widespread in the future, and allows us to continuously evolve our safeguards.
- *Public transparency.* We have long sought to highlight potential misuses of AI and share what we have learned about safety [link 1, link 2] with the industry and the public. As part of our ongoing efforts to advance responsible use of AI, OpenAI will continue to inform the public and stakeholders about the nature and extent of malicious state-affiliated actors' use of AI detected within our systems and the measures taken against them, when warranted. We believe that sharing and transparency foster greater awareness and preparedness among all stakeholders, leading to stronger collective defense against ever-evolving adversaries. You may visit:
<https://openai.com/research/language-model-safety-and-misuse>
<https://openai.com/blog/best-practices-for-deploying-language-models>

The vast majority of people use our systems to help improve their daily lives, from virtual tutors for students to apps that can transcribe the world for people who are seeing impaired. As is the case with many other ecosystems, there are a handful of malicious actors that require sustained attention so that everyone else can continue to enjoy the benefits. Although we work to minimize potential misuse by such actors, we will not be able to stop every instance. But by continuing to innovate, investigate, collaborate, and share, we make it harder for malicious actors to remain undetected across the digital ecosystem and improve the experience for everyone else.

To read more: <https://openai.com/blog/disrupting-malicious-uses-of-ai-by-state-affiliated-threat-actors>

ARTIFICIAL INTELLIGENCE - Fully Implementing Key Practices Could Help DHS Ensure Responsible Use for Cybersecurity



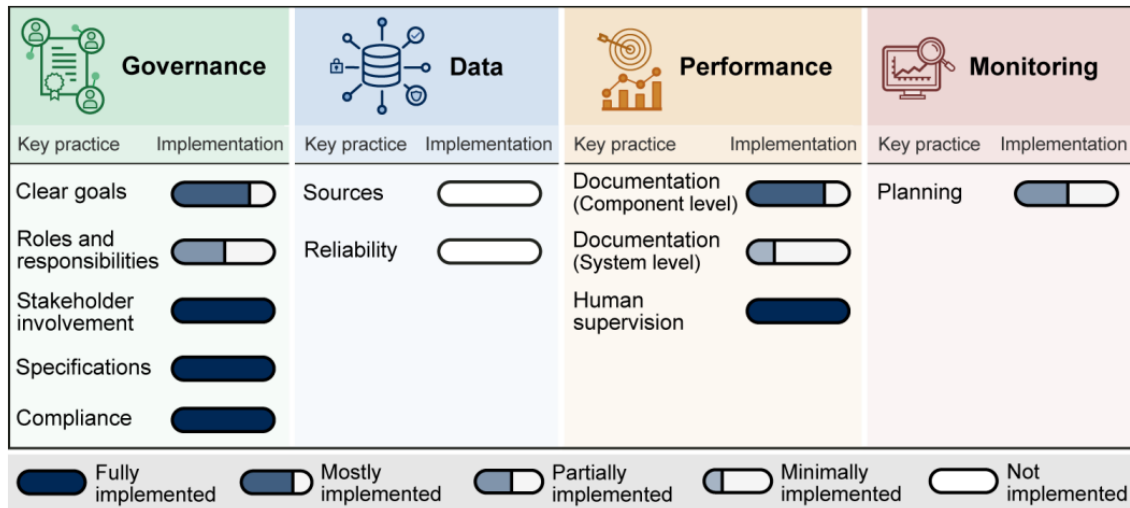
What GAO Found

To promote transparency and inform the public about how artificial intelligence (AI) is being used, federal agencies are required by Executive Order No. 13960 to maintain an inventory of AI use cases. The Department of Homeland Security (DHS) has established such an inventory, which is posted on the Department’s website.

However, DHS's inventory of AI systems for cybersecurity is not accurate. Specifically, the inventory identified two AI cybersecurity use cases, but officials told us one of these two was incorrectly characterized as AI. Although DHS has a process to review use cases before they are added to the AI inventory, the agency acknowledges that it does not confirm whether uses are correctly characterized as AI. Until it expands its process to include such determinations, DHS will be unable to ensure accurate use case reporting.

DHS has implemented some but not all of the key practices from GAO’s AI Accountability Framework for managing and overseeing its use of AI for cybersecurity. GAO assessed the one remaining cybersecurity use case known as Automated Personally Identifiable Information (PII) Detection—against 11 AI practices selected from the Framework (see figure).

Status of the Department of Homeland Security’s Implementation of Selected Key Practices to Manage and Oversee Artificial Intelligence for Cybersecurity







Source: GAO analysis of agency documents and interviews with Department of Homeland Security officials; GAO (icons). | GAO-24-106246

GAO found that DHS fully implemented four of the 11 key practices and implemented five others to varying degrees in the areas of governance, performance, and monitoring. It did not implement two practices: documenting

the sources and origins of data used to develop the PII detection capabilities, and assessing the reliability of data, according to officials.

GAO's AI Framework calls for management to provide reasonable assurance of the quality, reliability, and representativeness of the data used in the application, from its development through operation and maintenance. Addressing data sources and reliability is essential to model accuracy. Fully implementing the key practices can help DHS ensure accountable and responsible use of AI.

Figure 1: Principles, Selected Key Practices, and Questions to Consider for Managing and Overseeing Artificial Intelligence

Principle	Practice	Key considerations
 Governance	Clear goals	What goals and objectives does the entity expect to achieve throughout the AI life cycle? To what extent do stated goals and objectives represent a balanced set of priorities and adequately reflect stated values? How does the AI system help the entity meet its goals and objectives? To what extent does the entity communicate its AI strategic goals and objectives to the community of stakeholders? To what extent does the entity have the necessary resources to achieve the goals and objectives outlined for the AI life cycle? To what extent does the entity consistently measure progress towards stated goals and objectives?
	Roles and responsibilities	What are the roles, responsibilities, and delegation of authorities of personnel involved throughout the AI life cycle? To what extent has the entity clarified the roles, responsibilities, and delegated authorities to relevant stakeholders?
	Stakeholder involvement	What factors were considered when identifying the community of stakeholders involved throughout the life cycle? Which stakeholders did the entity include throughout the life cycle? What specific perspectives did stakeholders share, and how were they integrated throughout the life cycle? To what extent has the entity addressed stakeholder perspectives on the potential negative impacts of the AI system on end users and impacted populations?
	Technical specifications	What challenge/constraint is the AI system intended to solve? To what extent has the entity clearly defined technical specifications and requirements for the AI system? How do the technical specifications and requirements align with the AI system's goals and objectives? What justifications, if any, has the entity provided for the assumptions, boundaries, and limitations of the AI system?
	Compliance	To what extent has the entity identified the relevant laws, regulations, standards, and guidance, applicable to the AI system's use? How does the entity ensure that the AI system complies with relevant laws, regulations, standards, federal guidance, and policies? To what extent is the AI system in compliance with applicable laws, regulations, standards, federal guidance, and entity policies?
 Data	Sources	How has the entity documented the AI system's data provenance, including sources, origins, transformations, augmentations, labels, dependencies, constraints, and metadata?
	Reliability	To what extent are data used to develop the AI system accurate, complete, and valid?
 Performance	Component-level documentation	How is each model component solving a defined problem? How are the operating specifications and parameters of model and non-model components selected, evaluated, and optimized? How suitable are the components to the available data and operating conditions?
	System-level documentation	To what extent has the entity documented the AI system's development, testing methodology, metrics, and performance outcomes? To what extent does the documentation describe test results, limitations, and corrective actions, including efforts to minimize undesired effects in the outcomes?
	Human supervision	How has the entity considered an appropriate degree of human involvement in the automated decision-making processes? What procedures have been established for human supervision of the AI system? To what extent has the entity followed its procedures for human supervision to ensure accountability?
 Monitoring	Planning	What plans has the entity developed to monitor the AI system? To what extent do the plans describe processes and procedures to continuously monitor the AI system? What is the established frequency for monitoring the AI system?

Source: GAO AI Accountability Framework; GAO (icons). | GAO-24-106246

To read more: <https://www.gao.gov/assets/d24106246.pdf>

Using AI to develop enhanced cybersecurity measures

New research helps identify an unprecedented number of malware families

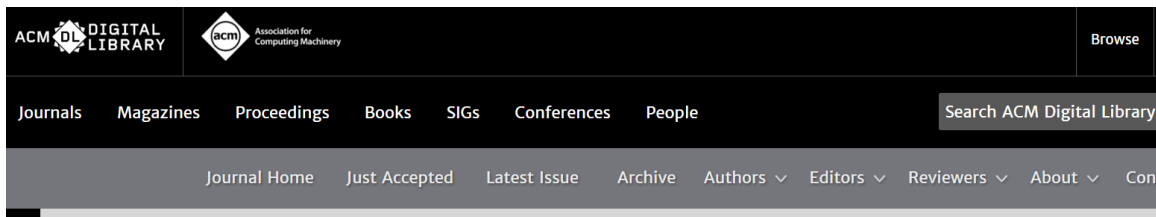


A research team at Los Alamos National Laboratory is using artificial intelligence to address several critical shortcomings in large-scale malware analysis, making significant advancements in the classification of Microsoft Windows malware and paving the way for enhanced cybersecurity measures. Using their approach, the team set a new world record in classifying malware families.

“Artificial intelligence methods developed for cyber-defense systems, including systems for large-scale malware analysis, need to consider real-world challenges,” said Maksim Eren, a scientist in Advanced Research in Cyber Systems at Los Alamos. “Our method addresses several of them.”

The team’s paper was recently published in the Association for Computing Machinery’s journal, Transactions on Privacy and Security. The paper:

<https://dl.acm.org/doi/10.1145/3624567>



Semi-Supervised Classification of Malware Families Under Extreme Class Imbalance via Hierarchical Non-Negative Matrix Factorization with Automatic Model Selection

This research introduces an innovative method using AI that is a significant breakthrough in the field of Windows malware classification. The approach achieves realistic malware family classification by leveraging semi-supervised tensor decomposition methods and selective classification, specifically, the reject option.

“The reject option is the model’s ability to say, ‘I do not know,’ instead of making a wrong decision, giving the model the knowledge discovery capability,” Eren said.

Cyber defense teams need to quickly identify infected machines and malicious programs. These malicious programs can be uniquely crafted for their victims, which makes gathering large numbers of samples for traditional machine learning methods difficult.

This new method can accurately work with samples with both larger and smaller datasets at the same time — called class imbalance — allowing it to detect both

rare and prominent malware families. It can also reject predictions if it is not confident in its answer.

This could give security analysts the confidence to apply these techniques to practical high-stakes situations like cyber defense for detecting novel threats.

Distinguishing between novel threats and known types of malware specimens is an essential capability to develop mitigation strategies. Additionally, this method can maintain its performance even when limited data is used in its training.

Altogether, the use of the reject option and tensor decomposition methods to extract multi-faceted hidden patterns in data, sets a superior capability in characterizing malware. This achievement underscores the groundbreaking nature of the team's approach.

“To the best of our knowledge, our paper sets a new world record by simultaneously classifying an unprecedented number of malware families, surpassing prior work by a factor of 29, in addition to operating under extremely difficult real-world conditions of limited data, extreme class-imbalance and with the presence of novel malware families,” Eren said.

The team's tensor decomposition methods, with high performance computing and graphics processing unit capabilities, are now available as a user-friendly Python library in GitHub.

Paper: “Semi-supervised Classification of Malware Families Under Extreme Class Imbalance via Hierarchical Non-Negative Matrix Factorization with Automatic Model Determination.” Journal Transactions on Privacy and Security. LANL contributors: Eren (A-4), Manish Bhattarai (T-1), Boian Alexandrov (T-1).

To read more: <https://discover.lanl.gov/news/0215-ai-cybersecurity-measures/>

EU Digital Markets Act: the application by Bytedance (TikTok) seeking suspension of the Commission decision designating it as a gatekeeper is dismissed



Bytedance has failed to demonstrate the urgency required for an interim order in order to avoid serious and irreparable damage.

Bytedance Ltd is a non-operating holding company established in China in 2012 which, through local subsidiaries, provides the entertainment platform TikTok.

By decision of 5 September 2023, the Commission designated Bytedance as a gatekeeper under the Digital Markets Act.

In November 2023, Bytedance brought an **action for annulment** of that decision.

By separate document, Bytedance lodged an application for interim measures seeking suspension of that decision.

By today's order, the President of the General Court **dismisses** Bytedance's application for interim measures.

According to the President of the General Court, Bytedance has not shown that it is necessary to suspend the contested decision until the proceedings on the substance of the case are closed in order to avoid serious and irreparable harm to Bytedance.

Bytedance argued, inter alia, that the immediate implementation of the contested decision **risks causing the disclosure** of highly strategic information concerning TikTok's **user profiling** practices, which is not otherwise in the public domain.

That disclosure would enable TikTok's competitors and other third parties to obtain insight into TikTok's business strategies in a way that would significantly harm its business.

According to the President of the General Court, Bytedance has not shown that there is a real risk of disclosure of confidential information or that such a risk would give rise to serious and irreparable harm.

NOTE: The General Court will deliver final judgment on the substance of this case at a later date. An order as to interim measures is without prejudice to the outcome of the main proceedings. An appeal, limited to points of law only, may be brought before the Vice-President of the Court of Justice against the decision of the President of the General Court within two months and ten days of notification of the decision.

NOTE: An action for annulment seeks the annulment of acts of the institutions of the European Union that are contrary to EU law. The Member States, the European institutions and individuals may, under certain conditions, bring an

action for annulment before the Court of Justice or the General Court. If the action is well founded, the act is annulled. The institution concerned must fill any legal vacuum created by the annulment of the act.

To read more: <https://curia.europa.eu/jcms/upload/docs/application/pdf/2024-02/cp240028en.pdf>

Two truths and a myth in banking regulation

Pablo Hernández de Cos, Chair of the Basel Committee on Banking Supervision and Governor of the Bank of Spain, at the Eurofi High Level Seminar, Ghent.



Introduction

Good morning, and thank you for inviting me to speak at this Eurofi High Level Seminar. It's a pleasure to be in Ghent with you today.

Throughout the years, there has been no shortage of discussions at these Eurofi events about the work of the Basel Committee, and prudential regulation and supervision more generally.

Take a cursory look back at previous conferences, and you will stumble upon sessions with titles such as:

- “Impacts of Basel III on EU financial activities”;
- “Implementing Basel III in the EU: remaining challenges and timing”;
- “Basel III implementation in the EU: key political stakes”; and, as part of this week's event,
- “Basel III implementation: global consistency challenges”

You would be forgiven for wondering whether we are in some sort of Basel III implementation Groundhog Day! In fact, Basel Committee member jurisdictions are making good progress with implementing the outstanding Basel III standards.

Around a third of members have implemented all, or the majority of, the standards already, while two thirds plan to implement them by the end of this year. Most of the remaining jurisdictions expect to implement the outstanding standards by next year.

But it is also true that discussions around Basel III – including at these events – are often dominated by somewhat flimsy assertions. Many have been warning about the detrimental impact of Basel III for almost 15 years now. Yet the empirical evidence to date is overwhelmingly clear: the global banking system has become more resilient since the implementation of Basel III, and bank lending has expanded in most jurisdictions during this time period.

So we could all benefit from a reminder about why the Basel III standards are critical to safeguarding the resilience of the global banking system and supporting economic growth and the prosperity of households and businesses.

I will therefore take a step back today to underline two recurring truths and to debunk a recurring myth when it comes to bank regulation and supervision.

Truth number 1: banking crises have a profound impact

The history of banking crises is rich and deep. Since 1920, the average share of countries around the world experiencing a systemic banking crisis in any given year is about 7%.

There have been over 150 systemic banking crises around the globe since 1970. The Committee itself, which celebrates its 50th anniversary this year, was established in the aftermath of a series of banking crises in 1974.

Systemic banking crises have a profound impact on our economies and social welfare. Banking crises have historically led to a persistent loss in output to the tune of 10% of GDP.

Banking crisis-induced recessions permanently depress the level of output, with typically no return to pre-crisis trends.

If this sounds like ancient history, then recall that it was less than a year ago when we witnessed the most significant system-wide banking stress since the Great Financial Crisis in terms of scale and scope.

Over the span of a few days and weeks, five banks with total assets exceeding \$1.1 trillion were shut down, put into receivership or rescued.

The distress of these banks triggered a broader assessment of the resilience of the broader banking system. In response, large-scale public support measures were deployed by some jurisdictions to mitigate the impact of the stress.

A back-of-the-envelope estimate suggests that roughly \$500 billion of direct public support was provided in response to the turmoil. That's a large number!

To read more: <https://www.bde.es/wbe/en/noticias-eventos/actualidad-banco-espana/gob-eurofi2024.html>

CISA and MS-ISAC Release Advisory on Compromised Account Used to Access State Government Organization

CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY



CISA and the Multi-State Information Sharing & Analysis Center (MS-ISAC) released a joint Cybersecurity Advisory (CSA), Threat Actor Leverages Compromised Account of Former Employee to Access State Government Organization to provide network defenders with the tactics, techniques, and procedures (TTPs) utilized by a threat actor and methods to protect against similar exploitation.

**JOINT
CYBERSECURITY
ADVISORY**

Co-Authored by:

TLP: CLEAR Product ID: AA24-046A
February 15, 2024

MS-ISAC®
Multi-State Information
Sharing & Analysis Center®

The banner features a dark blue background with a futuristic cityscape and network lines. The text "JOINT CYBERSECURITY ADVISORY" is prominently displayed in white. Below this, it states "Co-Authored by:" followed by the logos for CISA and MS-ISAC. To the right, it includes the classification "TLP: CLEAR", the product ID "AA24-046A", and the date "February 15, 2024".

Threat Actor Leverages Compromised Account of Former Employee to Access State Government Organization

Following an incident response assessment of a state government organization's network environment, analysis confirmed compromise through network administrator credentials of a former employee. This allowed the threat actor to successfully authenticate to an internal virtual private network (VPN) access point.

CISA and MS-ISAC encourage network defenders and organizations review the TTPs and implement the mitigations provided in the joint CSA. For more information, visit CISA's Cross-Sector Cybersecurity Performance Goals.

To read more: <https://www.cisa.gov/news-events/alerts/2024/02/15/cisa-and-ms-isac-release-advisory-compromised-account-used-access-state-government-organization>

Reward Offers for Information on LockBit Leaders and Designating Affiliates

U.S. DEPARTMENT *of* STATE

The Department of State is announcing reward offers totaling up to \$15 million for information leading to the arrest and/or conviction of any individual participating in a LockBit ransomware variant attack and for information leading to the identification and/or location of any key leaders of the LockBit ransomware group.



Since January 2020, LockBit actors have executed over 2,000 attacks against victims in the United States, and around the world, causing costly disruptions to operations and the destruction or exfiltration of sensitive information. More than \$144 million in ransom payments have been made to recover from LockBit ransomware events.

The reward offer complements announcements by the Department of Justice and the Federal Bureau of Investigation with the United Kingdom's National Crime Agency, along with other international partners, of a coordinated series of law enforcement actions that will disrupt the LockBit ransomware criminal organization.

To further strengthen our fight against malicious cyber actors, the United States also designated two individuals involved in LockBit pursuant to Executive Order 13694 . We will continue to stand with our partners to disrupt ransomware actors that threaten our economies and critical infrastructure. For more information on this designation, please see Treasury's press release .

To read more: <https://www.state.gov/reward-offers-for-information-on-lockbit-leaders-and-designating-affiliates/>

FBI Cyber Deputy Assistant Director Brett Leatherman's Remarks

at Press Conference Announcing the Disruption of the LockBit Ransomware Group I'm pleased to represent the FBI here today, as I oversee the FBI's Cyber Operations Branch.

I am excited to speak about our multi-year disruption campaign against the LockBit ransomware group.

LockBit has hurt thousands of victims across the country and around the world to include in recent years, targeting all sectors, from government and public sector companies, such as hospitals and schools, to high-profile, global companies.

Today, a joint sequenced operation among 10 countries disrupted LockBit's front- and back-end infrastructure in the U.S. and abroad.

The FBI seized four servers in the U.S. as part of this technical disruption, and we are announcing a total of five LockBit affiliates charged by the Department of Justice.

Two of those indictments are being publicly released today.

In addition, the cyber-related sanctions program implemented by the US Office of Foreign Assets Control (OFAC) imposed sanctions on two LockBit threat actors responsible for malicious cyber-enabled activities.

Lastly, we can proudly announce through the U.S. Department of State a reward of up to \$15 million via the Transnational Organized Crime Rewards Program for anyone with information about LockBit associates.

This includes a reward of up to \$10 million for information leading to the identification or location of any individual(s) who hold a leadership position in the LockBit ransomware variant transnational organized crime group and a reward offer of up to \$5 million for information leading to the arrest and/or conviction of any individual conspiring to participate in or attempting to participate in LockBit ransomware activities.

This large operation could not have happened without the contributions of the National Crime Agency, FBI Newark, our international partners, the FBI's Cyber Division—including our field office personnel across the country—and the FBI personnel stationed overseas, who led the collaboration with our foreign law enforcement partners all, standing shoulder to shoulder, pursuing the same goals, seeking to remediate victims and prevent LockBit from continuing its nefarious activities, it was these partnerships that were essential to today's success.

I cannot go on without mentioning some of the other international partners who contributed to this effort including South West Regional Organized Crime Unit in the U.K., Metropolitan Police Service in the U.K., Europol, Gendarmerie-C3N in France, the State Criminal Police Office L-K-A and Federal Criminal Police Office in Germany, Fedpol and Zurich Cantonal Police in Switzerland, the National Police Agency in Japan, the Australian Federal Police in Australia, the Swedish

Police Authority in Sweden, the National Bureau of Investigation in Finland, the Royal Canadian Mounted Police in Canada, and the National Police in the Netherlands.

This coordinated disruption of LockBit's networks illustrates the power of collaboration between the FBI and our international partners.

The FBI's strategy to combat ransomware leverages both our law enforcement and intelligence authorities to go after the whole cybercrime ecosystem by targeting the key services, namely the actors, their finances, their communications, their malware, and their supporting infrastructure.

And since 2021, that's exactly how we've targeted the LockBit ransomware.

Our access to LockBit's infrastructure was no accident.

Now, as we move to the next phase of the investigation, we've worked with our international partners to seize the infrastructure used by these criminal actors including nearly 11,000 domains and servers located all over the globe—hindering LockBit's ability to sting again.

Through this operation, we have access to nearly 1,000 potential decryption capabilities, and the FBI, NCA, and Europol will be conducting victim engagement with over 1,600 known US victims.

I'm here today to ask those US victims and private sector partners who have been a victim of a LockBit ransomware attack to please go to our IC3 website to complete a questionnaire to see if the FBI can provide you with decryption capabilities found during this infrastructure disruption.

One example of our success helping victims occurred in October of 2023.

A Boeing distribution business, Boeing Distribution Inc. (BDI), was the victim of a LockBit ransomware attack.

Boeing immediately engaged the FBI, which provided timely coordination and information sharing that was instrumental to BDI's investigation and recovery.

Today's lesson for businesses large and small, hospitals and police departments, and all the other many victims of ransomware is this:

Reach out to your local FBI field office today and introduce yourselves, so you know who to call if you become the victim of a cyberattack. If you are a victim of LockBit, please reach out to your local FBI office or fill out the form on lockbitvictims.ic3.gov. The FBI is in possession of nearly 1,000 decryption keys, which we intend to provide to victims.

We're ready to help you build a crisis response plan, so when an intruder does come knocking, you'll be prepared.

And, like the LockBit victims here, when you talk to us in advance—as so many others have—you’ll know how we operate: quickly and quietly, giving you the assistance, intelligence, and technical information you want and need.

When victims report attacks to us, we can help them—and others, too.

Today’s announcement is only the beginning.

We’ll continue gathering evidence, building out our map of LockBit developers, administrators, and affiliates, and using that knowledge to drive arrests, seizures, and other operations, whether by the FBI or our partners here and abroad.

While this is, yes, a fight to protect our country, our citizens, and our national security, make no mistake—the fight for cybersecurity spans the globe. But the FBI’s presence and partnerships do, too.

So, a reminder to cybercriminals: No matter where you are, and no matter how much you try to twist and turn to cover your tracks—your infrastructure, your criminal associates, your money, and your liberty are all at risk. And there will be consequences.

To read more: https://www.fbi.gov/news/speeches/fbi-cyber-deputy-assistant-director-brett-leathermans-remarks-at-press-conference-announcing-the-disruption-of-the-lockbit-ransomware-group? gl=1*17cxb48* gel au*Mzg5NDc3NDIxLjE3MDg2NzkoMTC.



Learn More About the Transnational Organized Crime Rewards Program Targets

NIST SP 800-66 Rev. 2 - Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide, February 2024



This publication aims to help educate readers about the security standards included in the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, as amended by the Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act and Other Modifications to the HIPAA Rules.

**NIST Special Publication 800
NIST SP 800-66r2**

Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule

A Cybersecurity Resource Guide

Jeffrey A. Marron

In general, the requirements, standards, and implementation specifications of the Security Rule apply to the following regulated entities:

- **Covered Healthcare Providers** — Any provider of medical or other health services or supplies who transmits any health information in electronic form in connection with a transaction for which the U.S. Department of Health and Human Services (HHS) has adopted a standard.
- **Health Plans** — Any individual or group plan that provides or pays the cost of medical care (e.g., a health insurance issuer and the Medicare and Medicaid programs).
- **Healthcare Clearinghouses** — A public or private entity that processes another entity's healthcare transactions from a standard format to a non-standard format or vice versa.
- **Business Associate** — A person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of or provides services to a covered entity. A business associate is liable for their own HIPAA violations.

The Security Rule is separated into six main sections that each include several standards that a regulated entity must meet.

Many of the standards contain implementation specifications.

An implementation specification is a more detailed description of the method or approach that regulated entities can use to meet a particular standard.

Implementation specifications are either required or addressable. Regulated entities must comply with required implementation specifications. Regulated entities must perform an assessment to determine whether each addressable implementation specification is a reasonable and appropriate safeguard to implement in the regulated entity's environment.

The assessment, analysis, and management of risk to ePHI provide the foundation for a regulated entity's Security Rule compliance efforts and the protection of ePHI. Readers are reminded of the Security Rule's flexibility of approach. The HHS Office for Civil Rights (OCR) does not prescribe any particular risk assessment or risk management methodology.

Section 3 and Sec. 4 provide background information about risk assessment and risk management processes, respectively, as well as approaches that regulated entities may choose to use in assessing and managing risk to ePHI.

Many regulated entities may benefit from more specific guidance concerning how to comply with the standards and implementation specifications of the Security Rule.

To that end, Sec. 5 highlights considerations for a regulated entity when implementing the Security Rule. Key activities, descriptions, and sample questions are provided for each standard. The key activities suggest actions that are often associated with the security functions suggested by that standard.

Many of these key activities are often included in a robust security program and may be useful to regulated entities. The descriptions provide expanded explanations about each of the key activities and the types of activities that a regulated entity may pursue when implementing the standard.

The sample questions are a non-exhaustive list of questions that a regulated entity may ask itself to determine whether the standard has been adequately implemented.

Regulated entities may implement the Security Rule more effectively if they are shown controls catalogs and cybersecurity activities that align with each standard. To assist regulated entities, this publication includes mappings of the Security Rule's standards and implementation specifications to Cybersecurity Framework [NIST CSF] Subcategories and applicable security controls detailed in NIST Special Publication (SP) 800-53r5 (Revision 5), Security and Privacy Controls for Information Systems and Organizations [SP 800-53].

The mapping also lists additional NIST publications relevant to each Security Rule standard. Readers may draw upon these NIST publications and mappings for assistance in implementing the Security Rule.

Additionally, Appendix F links to a wide variety of resources (e.g., guidance, templates, tools) that regulated entities may find useful for complying with the Security Rule and improving the security posture of their organizations.

For ease of use, the resources are organized by topic. Regulated entities could consult these resources when they need additional information or guidance about a particular topic.

To read more:

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-66r2.pdf>

Executive Order on Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern

THE WHITE HOUSE



By the authority vested in me as President by the Constitution and the laws of the United States of America, including the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.) (IEEPA), the National Emergencies Act (50 U.S.C. 1601 et seq.) (NEA), and section 301 of title 3, United States Code,

I, JOSEPH R. BIDEN JR., President of the United States of America, hereby expand the scope of the national emergency declared in Executive Order 13873 of May 15, 2019 (Securing the Information and Communications Technology and Services Supply Chain), and further addressed with additional measures in Executive Order 14034 of June 9, 2021 (Protecting Americans' Sensitive Data from Foreign Adversaries).

The continuing effort of certain countries of concern to access Americans' sensitive personal data and United States Government-related data constitutes an unusual and extraordinary threat, which has its source in whole or substantial part outside the United States, to the national security and foreign policy of the United States.

Access to Americans' bulk sensitive personal data or United States Government-related data increases the ability of countries of concern to engage in a wide range of malicious activities.

Countries of concern can rely on advanced technologies, including artificial intelligence (AI), to analyze and manipulate bulk sensitive personal data to engage in espionage, influence, kinetic, or cyber operations or to identify other potential strategic advantages over the United States.

Countries of concern can also use access to bulk data sets to fuel the creation and refinement of AI and other advanced technologies, thereby improving their ability to exploit the underlying data and exacerbating the national security and foreign policy threats.

In addition, access to some categories of sensitive personal data linked to populations and locations associated with the Federal Government — including the military — regardless of volume, can be used to reveal insights about those populations and locations that threaten national security.

The growing exploitation of Americans' sensitive personal data threatens the development of an international technology ecosystem that protects our security, privacy, and human rights.

Accordingly, to address this threat and to take further steps with respect to the national emergency declared in Executive Order 13873, it is hereby ordered that:

Section 1. Policy. It is the policy of the United States to restrict access by countries of concern to Americans' bulk sensitive personal data and United States Government-related data when such access would pose an unacceptable risk to the national security of the United States.

At the same time, the United States continues to support open, global, interoperable, reliable, and secure flows of data across borders, as well as maintaining vital consumer, economic, scientific, and trade relationships that the United States has with other countries.

The continuing effort by countries of concern to access Americans' bulk sensitive personal data and United States Government-related data threatens the national security and foreign policy of the United States.

Such countries' governments may seek to access and use sensitive personal data in a manner that is not in accordance with democratic values, safeguards for privacy, and other human rights and freedoms.

Such countries' approach stands in sharp contrast to the practices of democracies with respect to sensitive personal data and principles reflected in the Organisation for Economic Co-operation and Development Declaration on Government Access to Personal Data Held by Private Sector Entities.

Unrestricted transfers of Americans' bulk sensitive personal data and United States Government-related data to such countries of concern may therefore enable them to exploit such data for a variety of nefarious purposes, including to engage in malicious cyber-enabled activities.

Countries of concern can use their access to Americans' bulk sensitive personal data and United States Government-related data to track and build profiles on United States individuals, including Federal employees and contractors, for illicit purposes, including blackmail and espionage.

Access to Americans' bulk sensitive personal data and United States Government-related data by countries of concern through data brokerages, third-party vendor agreements, employment agreements, investment agreements, or other such arrangements poses particular and unacceptable risks to our national security given that these arrangements often can provide countries of concern with direct and unfettered access to Americans' bulk sensitive personal data.

Countries of concern can use access to United States persons' bulk sensitive personal data and United States Government-related data to collect information on activists, academics, journalists, dissidents, political figures, or members of non-governmental organizations or marginalized communities in order to intimidate such persons; curb dissent or political opposition; otherwise limit freedoms of expression, peaceful assembly, or association; or enable other forms of suppression of civil liberties.

This risk of access to Americans' bulk sensitive personal data and United States Government-related data is not limited to direct access by countries of concern. Entities owned by, and entities or individuals controlled by or subject to

the jurisdiction or direction of, a country of concern may enable the government of a country of concern to indirectly access such data.

For example, a country of concern may have cyber, national security, or intelligence laws that, without sufficient legal safeguards, obligate such entities and individuals to provide that country's intelligence services access to Americans' bulk sensitive personal data and United States Government-related data.

These risks may be exacerbated when countries of concern use bulk sensitive personal data to develop AI capabilities and algorithms that, in turn, enable the use of large datasets in increasingly sophisticated and effective ways to the detriment of United States national security.

Countries of concern can use AI to target United States persons for espionage or blackmail by, for example, recognizing patterns across multiple unrelated datasets to identify potential individuals whose links to the Federal Government would be otherwise obscured in a single dataset.

While aspects of this threat have been addressed in previous executive actions, such as Executive Order 13694 of April 1, 2015 (Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities), as amended, additional steps need to be taken to address this threat.

At the same time, the United States is committed to promoting an open, global, interoperable, reliable, and secure Internet; protecting human rights online and offline; supporting a vibrant, global economy by promoting cross-border data flows required to enable international commerce and trade; and facilitating open investment.

To ensure that the United States continues to meet these important policy objectives, this order does not authorize the imposition of generalized data localization requirements to store Americans' bulk sensitive personal data or United States Government-related data within the United States or to locate computing facilities used to process Americans' bulk sensitive personal data or United States Government-related data within the United States.

This order also does not broadly prohibit United States persons from conducting commercial transactions, including exchanging financial and other data as part of the sale of commercial goods and services, with entities and individuals located in or subject to the control, direction, or jurisdiction of countries of concern, or impose measures aimed at a broader decoupling of the substantial consumer, economic, scientific, and trade relationships that the United States has with other countries.

In addition, my Administration has made commitments to increase public access to the results of taxpayer-funded scientific research, the sharing and interoperability of electronic health information, and patient access to their data.

The national security restrictions established in this order are specific, carefully calibrated actions to minimize the risks associated with access to bulk sensitive

personal data and United States Government-related data by countries of concern while minimizing disruption to commercial activity.

This order shall be implemented consistent with these policy objectives, including by tailoring any regulations issued and actions taken pursuant to this order to address the national security threat posed by access to Americans' bulk sensitive personal data and United States Government-related data by countries of concern.

Sec. 2. Prohibited and Restricted Transactions. (a) To assist in addressing the national emergency described in this order, the Attorney General, in coordination with the Secretary of Homeland Security and in consultation with the heads of relevant agencies, shall issue, subject to public notice and comment, regulations that prohibit or otherwise restrict United States persons from engaging in any acquisition, holding, use, transfer, transportation, or exportation of, or dealing in, any property in which a foreign country or national thereof has any interest (transaction), where the transaction:

(i) involves bulk sensitive personal data or United States Government-related data, as further defined by regulations issued by the Attorney General pursuant to this section;

(ii) is a member of a class of transactions that has been determined by the Attorney General, in regulations issued by the Attorney General pursuant to this section, to pose an unacceptable risk to the national security of the United States because the transactions may enable countries of concern or covered persons to access bulk sensitive personal data or United States Government-related data in a manner that contributes to the national emergency described in this order;

(iii) was initiated, is pending, or will be completed after the effective date of the regulations issued by the Attorney General pursuant to this section;

(iv) does not qualify for an exemption provided in, or is not authorized by a license issued pursuant to, the regulations issued by the Attorney General pursuant to this section; and

(v) is not, as defined by regulations issued by the Attorney General pursuant to this section, ordinarily incident to and part of the provision of financial services, including banking, capital markets, and financial insurance services, or required for compliance with any Federal statutory or regulatory requirements, including any regulations, guidance, or orders implementing those requirements.

(b) The Attorney General, in consultation with the heads of relevant agencies, is authorized to take such actions, including the promulgation of rules and regulations, and to employ all other powers granted to the President by IEEPA, as may be necessary or appropriate to carry out the purposes of this order. Executive departments and agencies (agencies) are directed to take all appropriate measures within their authority to implement the provisions of this order.

(c) Within 180 days of the date of this order, the Attorney General, in coordination with the Secretary of Homeland Security, and in consultation with the heads of relevant agencies, shall publish the proposed rule described in subsection (a) of this section for notice and comment. This proposed rule shall:

(i) identify classes of transactions that meet the criteria specified in subsection (a)(ii) of this section that are to be prohibited (prohibited transactions);

(ii) identify classes of transactions that meet the criteria specified in subsection (a)(ii) of this section and for which the Attorney General determines that security requirements established by the Secretary of Homeland Security, through the Director of the Cybersecurity and Infrastructure Security Agency, in accordance with the process described in subsection (d) of this section, adequately mitigate the risk of access by countries of concern or covered persons to bulk sensitive personal data or United States Government-related data (restricted transactions);

(iii) identify, with the concurrence of the Secretary of State and the Secretary of Commerce, countries of concern and, as appropriate, classes of covered persons for the purposes of this order;

(iv) establish, as appropriate, mechanisms to provide additional clarity to persons affected by this order and any regulations implementing this order (including by designations of covered persons and licensing decisions);

(v) establish a process to issue (including to modify or rescind), in concurrence with the Secretary of State, the Secretary of Commerce, and the Secretary of Homeland Security, and in consultation with the heads of other relevant agencies, as appropriate, licenses authorizing transactions that would otherwise be prohibited transactions or restricted transactions;

(vi) further define the terms identified in section 7 of this order and any other terms used in this order or any regulations implementing this order;

(vii) address, as appropriate, coordination with other United States Government entities, such as the Committee on Foreign Investment in the United States, the Office of Foreign Assets Control within the Department of the Treasury, the Bureau of Industry and Security within the Department of Commerce, and other entities implementing relevant programs, including those implementing Executive Order 13873; Executive Order 14034; and Executive Order 13913 of April 4, 2020 (Establishing the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector); and

(viii) address the need for, as appropriate, recordkeeping and reporting of transactions to inform investigative, enforcement, and regulatory efforts.

(d) The Secretary of Homeland Security, acting through the Director of the Cybersecurity and Infrastructure Security Agency, shall, in coordination with the Attorney General and in consultation with the heads of relevant agencies,

propose, seek public comment on, and publish security requirements that address the unacceptable risk posed by restricted transactions, as identified by the Attorney General pursuant to this section. These requirements shall be based on the Cybersecurity and Privacy Frameworks developed by the National Institute of Standards and Technology.

(i) The Secretary of Homeland Security, acting through the Director of the Cybersecurity and Infrastructure Security Agency, shall, in coordination with the Attorney General, issue any interpretive guidance regarding the security requirements.

(ii) The Attorney General shall, in coordination with the Secretary of Homeland Security acting through the Director of the Cybersecurity and Infrastructure Security Agency, issue enforcement guidance regarding the security requirements.

(e) The Secretary of Homeland Security, in coordination with the Attorney General, is hereby authorized to take such actions, including promulgating rules, regulations, standards, and requirements; issuing interpretive guidance; and employing all other powers granted to the President by IEEPA as may be necessary to carry out the purposes described in subsection (d) of this section.

(f) In exercising the authority delegated in subsection (b) of this section, the Attorney General, in coordination with the Secretary of Homeland Security and in consultation with the heads of relevant agencies, may, in addition to the rulemaking directed in subsection (c) of this section, propose one or more regulations to further implement this section, including to identify additional classes of prohibited transactions; to identify additional classes of restricted transactions; with the concurrence of the Secretary of State and the Secretary of Commerce, to identify new or remove existing countries of concern and, as appropriate, classes of covered persons for the purposes of this order; and to establish a mechanism for the Attorney General to monitor whether restricted transactions comply with the security requirements established under subsection (d) of this section.

(g) Any proposed regulations implementing this section:

(i) shall reflect consideration of the nature of the class of transaction involving bulk sensitive personal data or United States Government-related data, the volume of bulk sensitive personal data involved in the transaction, and other factors, as appropriate;

(ii) shall establish thresholds and due diligence requirements for entities to use in assessing whether a transaction is a prohibited transaction or a restricted transaction;

(iii) shall not establish generalized data localization requirements to store bulk sensitive personal data or United States Government-related data within the United States or to locate computing facilities used to process bulk sensitive personal data or United States Government-related data within the United States;

(iv) shall account for any legal obligations applicable to the United States Government relating to public access to the results of taxpayer-funded scientific research, the sharing and interoperability of electronic health information, and patient access to their data; and

(v) shall not address transactions to the extent that they involve types of human 'omic data other than human genomic data before the submission of the report described in section 6 of this order.

(h) The prohibitions promulgated pursuant to this section apply except to the extent provided by law, including by statute or in regulations, orders, directives, or licenses that may be issued pursuant to this order, and notwithstanding any contract entered into or any license or permit granted prior to the effective date of the applicable regulations directed by this order.

(i) Any transaction or other activity that has the purpose of evading or avoiding, causes a violation of, or attempts to violate any of the prohibitions promulgated pursuant to this section is prohibited.

(j) Any conspiracy formed to violate any of the prohibitions promulgated pursuant to this section is prohibited.

(k) In regulations issued by the Attorney General under this section, the Attorney General may prohibit United States persons from knowingly directing transactions if such transactions would be prohibited transactions under regulations issued pursuant to this order if engaged in by a United States person.

(l) The Attorney General may, consistent with applicable law, redelegate any of the authorities conferred on the Attorney General pursuant to this section within the Department of Justice. The Secretary of Homeland Security may, consistent with applicable law, redelegate any of the authorities conferred on the Secretary of Homeland Security pursuant to this section within the Department of Homeland Security.

(m) The Attorney General, in coordination with the Secretary of Homeland Security and in consultation with the heads of relevant agencies, is hereby authorized to submit recurring and final reports to the Congress related to this order, consistent with section 401(c) of the NEA (50 U.S.C. 1641(c)) and section 204(c) of IEEPA (50 U.S.C. 1703(c)).

Sec. 3. Protecting Sensitive Personal Data. (a) Access to bulk sensitive personal data and United States Government-related data by countries of concern can be enabled through the transmission of data via network infrastructure that is subject to the jurisdiction or control of countries of concern.

The risk of access to this data by countries of concern can be, and sometime is, exacerbated where the data transits a submarine cable that is owned or operated by persons owned by, controlled by, or subject to the jurisdiction or direction of a country of concern, or that connects to the United States and terminates in the jurisdiction of a country of concern.

Additionally, the same risk of access by a country of concern is further exacerbated in instances where a submarine cable is designed, built, and operated for the express purpose of transferring data, including bulk sensitive personal data or United States Government-related data, to a specific data center located in a foreign jurisdiction.

To address this threat, the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector (Committee) shall, to the extent consistent with its existing authority and applicable law:

(i) prioritize, for purposes of and in reliance on the process set forth in section 6 of Executive Order 13913, the initiation of reviews of existing licenses for submarine cable systems that are owned or operated by persons owned by, controlled by, or subject to the jurisdiction or direction of a country of concern, or that terminate in the jurisdiction of a country of concern;

(ii) issue policy guidance, in consultation with the Committee's Advisors as defined in section 3(d) of Executive Order 13913, regarding the Committee's reviews of license applications and existing licenses, including the assessment of third-party risks regarding access to data by countries of concern; and

(iii) address, on an ongoing basis, the national security and law enforcement risks related to access by countries of concern to bulk sensitive personal data described in this order that may be presented by any new application or existing license reviewed by the Committee to land or operate a submarine cable system, including by updating the Memorandum of Understanding required under section 11 of Executive Order 13913 and by revising the Committee's standard mitigation measures, with the approval of the Committee's Advisors, which may include, as appropriate, any of the security requirements contemplated by section 2(d) of this order.

(b) Entities in the United States healthcare market can access bulk sensitive personal data, including personal health data and human genomic data, through partnerships and agreements with United States healthcare providers and research institutions. Even if such data is anonymized, pseudonymized, or de-identified, advances in technology, combined with access by countries of concern to large data sets, increasingly enable countries of concern that access this data to re-identify or de-anonymize data, which may reveal the exploitable health information of United States persons. While the United States supports open scientific data and sample sharing to accelerate research and development through international cooperation and collaboration, the following additional steps must be taken to protect United States persons' sensitive personal health data and human genomic data from the threat identified in this order:

(i) The Secretary of Defense, the Secretary of Health and Human Services, the Secretary of Veterans Affairs, and the Director of the National Science Foundation shall consider taking steps, including issuing regulations, guidance, or orders, as appropriate and consistent with the legal authorities authorizing relevant Federal assistance programs, to prohibit the provision of assistance that enables access by countries of concern or covered persons to United States

persons' bulk sensitive personal data, including personal health data and human genomic data, or to impose mitigation measures with respect to such assistance, which may be consistent with the security requirements adopted under section 2(d) of this order, on the recipients of Federal assistance to address this threat.

The Secretary of Defense, the Secretary of Health and Human Services, the Secretary of Veterans Affairs, and the Director of the National Science Foundation shall, in consultation with each other, develop and publish guidance to assist United States research entities in ensuring protection of their bulk sensitive personal data.

(ii) Within 1 year of the date of this order, the Secretary of Defense, the Secretary of Health and Human Services, the Secretary of Veterans Affairs, and the Director of the National Science Foundation shall jointly submit a report to the President through the Assistant to the President for National Security Affairs (APNSA) detailing their progress in implementing this subsection.

(c) Entities in the data brokerage industry enable access to bulk sensitive personal data and United States Government-related data by countries of concern and covered persons. These entities pose a particular risk of contributing to the national emergency described in this order because they routinely engage in the collection, assembly, evaluation, and dissemination of bulk sensitive personal data and of the subset of United States Government-related data regarding United States consumers.

The Director of the Consumer Financial Protection Bureau (CFPB) is encouraged to consider taking steps, consistent with CFPB's existing legal authorities, to address this aspect of the threat and to enhance compliance with Federal consumer protection law, including by continuing to pursue the rulemaking proposals that CFPB identified at the September 2023 Small Business Advisory Panel for Consumer Reporting Rulemaking.

Sec. 4. Assessing the National Security Risks Arising from Prior Transfers of United States Persons' Bulk Sensitive Personal Data. Within 120 days of the effective date of the regulations issued pursuant to section 2(c) of this order, the Attorney General, the Secretary of Homeland Security, and the Director of National Intelligence, in consultation with the heads of relevant agencies, shall recommend to the APNSA appropriate actions to detect, assess, and mitigate national security risks arising from prior transfers of United States persons' bulk sensitive personal data to countries of concern. Within 150 days of the effective date of the regulations issued pursuant to section 2(c) of this order, the APNSA shall review these recommendations and, as appropriate, consult with the Attorney General, the Secretary of Homeland Security, and the heads of relevant agencies on implementing the recommendations consistent with applicable law.

Sec. 5. Report to the President. (a) Within 1 year of the effective date of the regulations issued pursuant to section 2(c) of this order, the Attorney General, in consultation with the Secretary of State, the Secretary of the Treasury, the Secretary of Commerce, and the Secretary of Homeland Security, shall submit a report to the President through the APNSA assessing, to the extent practicable:

(i) the effectiveness of the measures imposed under this order in addressing threats to the national security of the United States described in this order; and

(ii) the economic impact of the implementation of this order, including on the international competitiveness of United States industry.

(b) In preparing the report described in subsection (a) of this section, the Attorney General shall solicit and consider public comments concerning the economic impact of this order.

Sec. 6. Assessing Risks Associated with Human ‘omic Data. Within 120 days of the date of this order, the APNSA, the Assistant to the President and Director of the Domestic Policy Council, the Director of the Office of Science and Technology Policy, and the Director of the Office of Pandemic Preparedness and Response Policy, in consultation with the Secretary of State, the Secretary of Defense, the Secretary of Health and Human Services, the Secretary of Veterans Affairs, the Director of the National Science Foundation, the Director of National Intelligence, and the Director of the Federal Bureau of Investigation, shall submit a report to the President, through the APNSA, assessing the risks and benefits of regulating transactions involving types of human ‘omic data other than human genomic data, such as human proteomic data, human epigenomic data, and human metabolomic data, and recommending the extent to which such transactions should be regulated pursuant to section 2 of this order. This report and recommendation shall consider the risks to United States persons and national security, as well as the economic and scientific costs of regulating transactions that provide countries of concern or covered persons access to these data types.

Sec. 7. Definitions. For purposes of this order:

(a) The term “access” means logical or physical access, including the ability to obtain, read, copy, decrypt, edit, divert, release, affect, alter the state of, or otherwise view or receive, in any form, including through information technology systems, cloud computing platforms, networks, security systems, equipment, or software.

(b) The term “bulk” means an amount of sensitive personal data that meets or exceeds a threshold over a set period of time, as specified in regulations issued by the Attorney General pursuant to section 2 of this order.

(c) The term “country of concern” means any foreign government that, as determined by the Attorney General pursuant to section 2(c)(iii) or 2(f) of this order, has engaged in a long-term pattern or serious instances of conduct significantly adverse to the national security of the United States or the security and safety of United States persons, and poses a significant risk of exploiting bulk sensitive personal data or United States Government-related data to the detriment of the national security of the United States or the security and safety of United States persons, as specified in regulations issued by the Attorney General pursuant to section 2 of this order.

(d) The term “covered person” means an entity owned by, controlled by, or subject to the jurisdiction or direction of a country of concern; a foreign person who is an employee or contractor of such an entity; a foreign person who is an employee or contractor of a country of concern; a foreign person who is primarily resident in the territorial jurisdiction of a country of concern; or any person designated by the Attorney General as being owned or controlled by or subject to the jurisdiction or direction of a country of concern, as acting on behalf of or purporting to act on behalf of a country of concern or other covered person, or as knowingly causing or directing, directly or indirectly, a violation of this order or any regulations implementing this order.

(e) The term “covered personal identifiers” means, as determined by the Attorney General in regulations issued pursuant to section 2 of this order, specifically listed classes of personally identifiable data that are reasonably linked to an individual, and that – whether in combination with each other, with other sensitive personal data, or with other data that is disclosed by a transacting party pursuant to the transaction and that makes the personally identifiable data exploitable by a country of concern – could be used to identify an individual from a data set or link data across multiple data sets to an individual. The term “covered personal identifiers” does not include:

(i) demographic or contact data that is linked only to another piece of demographic or contact data (such as first and last name, birth date, birthplace, zip code, residential street or postal address, phone number, and email address and similar public account identifiers); or

(ii) a network-based identifier, account-authentication data, or call-detail data that is linked only to another network-based identifier, account-authentication data, or call-detail data for the provision of telecommunications, networking, or similar services.

(f) The term “entity” means a partnership, association, trust, joint venture, corporation, group, subgroup, or other organization.

(g) The term “foreign person” means any person that is not a United States person.

(h) The term “human genomic data” refers to data representing the nucleic acid sequences that constitute the entire set or a subset of the genetic instructions found in a cell.

(i) The term “human ‘omic data” means data generated from humans that characterizes or quantifies human biological molecule(s), such as human genomic data, epigenomic data, proteomic data, transcriptomic data, microbiomic data, or metabolomic data, as further defined by regulations issued by the Attorney General pursuant to section 2 of this order, which may be informed by the report described in section 6 of this order.

(j) The term “person” means an individual or entity.

(k) The term “relevant agencies” means the Department of State, the Department of the Treasury, the Department of Defense, the Department of Commerce, the Department of Health and Human Services, the Office of the United States Trade Representative, the Office of the Director of National Intelligence, the Office of the National Cyber Director, the Office of Management and Budget, the Federal Trade Commission, the Federal Communications Commission, and any other agency or office that the Attorney General determines appropriate.

(l) The term “sensitive personal data” means, to the extent consistent with applicable law including sections 203(b)(1) and (b)(3) of IEEPA, covered personal identifiers, geolocation and related sensor data, biometric identifiers, human ‘omic data, personal health data, personal financial data, or any combination thereof, as further defined in regulations issued by the Attorney General pursuant to section 2 of this order, and that could be exploited by a country of concern to harm United States national security if that data is linked or linkable to any identifiable United States individual or to a discrete and identifiable group of United States individuals. The term “sensitive personal data” does not include:

(i) data that is a matter of public record, such as court records or other government records, that is lawfully and generally available to the public;

(ii) personal communications that are within the scope of section 203(b)(1) of IEEPA; or

(iii) information or informational materials within the scope of section 203(b)(3) of IEEPA.

(m) The term “United States Government-related data” means sensitive personal data that, regardless of volume, the Attorney General determines poses a heightened risk of being exploited by a country of concern to harm United States national security and that:

(i) a transacting party identifies as being linked or linkable to categories of current or recent former employees or contractors, or former senior officials, of the Federal Government, including the military, as specified in regulations issued by the Attorney General pursuant to section 2 of this order;

(ii) is linked to categories of data that could be used to identify current or recent former employees or contractors, or former senior officials, of the Federal Government, including the military, as specified in regulations issued by the Attorney General pursuant to section 2 of this order; or

(iii) is linked or linkable to certain sensitive locations, the geographical areas of which will be specified publicly, that are controlled by the Federal Government, including the military.

(n) The term “United States person” means any United States citizen, national, or lawful permanent resident; any individual admitted to the United States as a refugee under 8 U.S.C. 1157 or granted asylum under 8 U.S.C. 1158;

any entity organized solely under the laws of the United States or any jurisdiction within the United States (including foreign branches); or any person in the United States.

Sec. 8. General Provisions. (a) Nothing in this order shall be construed to impair or otherwise affect:

(i) the authority granted by law to an executive department or agency, or the head thereof; or

(ii) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(b) Nothing in this order shall prohibit transactions for the conduct of the official business of the United States Government by employees, grantees, or contractors thereof, or transactions conducted pursuant to a grant, contract, or other agreement entered into with the United States Government.

(c) Any disputes that may arise among agencies during the consultation processes described in this order may be resolved pursuant to the interagency process described in National Security Memorandum 2 of February 4, 2021 (Renewing the National Security Council System), or any successor document.

(d) This order shall be implemented consistent with applicable law and subject to the availability of appropriations.

(e) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

To read more: <https://www.whitehouse.gov/briefing-room/presidential-actions/2024/02/28/executive-order-on-preventing-access-to-americans-bulk-sensitive-personal-data-and-united-states-government-related-data-by-countries-of-concern/>

Disclaimer

The Sarbanes-Oxley Compliance Professionals Association (SOXCPA) (hereinafter “Association”) enhances public access to information. Our goal is to keep this information timely and accurate. If errors are brought to our attention, we will try to correct them.

The Association expressly disclaims all warranties, either expressed or implied, including any implied warranty of fitness for a particular purpose, and neither assumes nor authorizes any other person to assume for it any liability in connection with the information or training programs provided.

The Association and its employees will not be liable for any loss or damages of any nature, either direct or indirect, arising from use of the information provided, as these are general information, not specific guidance for an organization or a firm in a specific country.

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;
- is in no way constitutive of interpretative;
- 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.

We are not responsible for opinions and information posted by others. The inclusion of links to other web sites does not necessarily imply a recommendation or endorsement of the views expressed within them. Links to other web sites are presented as a convenience to users. The Association does not accept any responsibility for the content, accuracy, reliability, or currency found on external web sites.

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.

Readers that are interested in a specific topic covered in the newsletter, must download the official papers, must find more information, and must ask for legal and technical advice before making any business decisions.

Sarbanes-Oxley Compliance Professionals Association (SOXCPA)



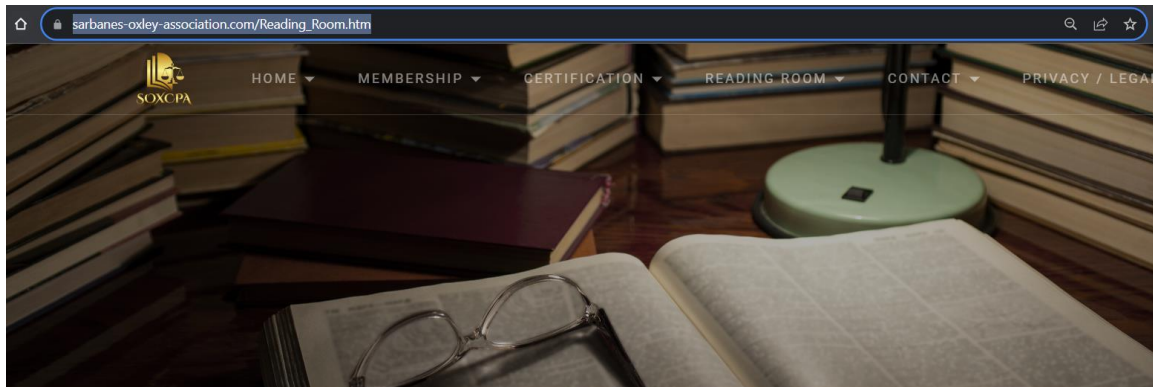
Welcome to the Sarbanes-Oxley Compliance Professionals Association (SOXCPA), the largest Association of Sarbanes-Oxley professionals in the world.

The Sarbanes-Oxley Compliance Professionals Association (SOXCPA) is a business unit of Compliance LLC, incorporated in Wilmington, NC, and offices in Washington, DC, a provider of risk and compliance training in 57 countries.

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.

Our reading room:

https://www.sarbanes-oxley-association.com/Reading_Room.htm



Reading Room, Sarbanes-Oxley Compliance Professionals Association (SOXCPA)

Our monthly newsletter:

Our training and certification programs.

1. Certified Sarbanes-Oxley Expert (CSOE), distance learning and online certification program. You may visit: https://www.sarbanes-oxley-association.com/Distance_Learning_and_Certification.htm
2. Certified Japanese Sarbanes-Oxley Expert (CJSOXE), distance learning and online certification program. You may visit: https://www.sarbanes-oxley-association.com/CJSOXE_Distance_Learning_and_Certification.htm

3. Certified EU Sarbanes-Oxley Expert (CEUSOE), distance learning and online certification program. You may visit: https://www.sarbanes-oxley-association.com/CEUSOE_Distance_Learning_and_Certification.htm

Sarbanes-Oxley is a hot skill that makes a manager or an employee an indispensable asset to a company or organization. There are thousands of new Sarbanes-Oxley jobs advertised in many countries.

Some examples from LinkedIn:

in sarbanes oxley United States

Jobs Date posted Experience level

sarbanes oxley in United States 3,711 results Set alert

RSM Director - Process Risk and Controls Consulting
RSM US LLP
Chicago, IL (Hybrid)
\$140K/yr - \$299K/yr
2 connections work here
Promoted · 2 hours ago

Guidehouse IT Risk & Internal Audit Consultant
Guidehouse
McLean, VA (On-site)
Vision, 401(k)
1 connection works here
Promoted · 3 hours ago

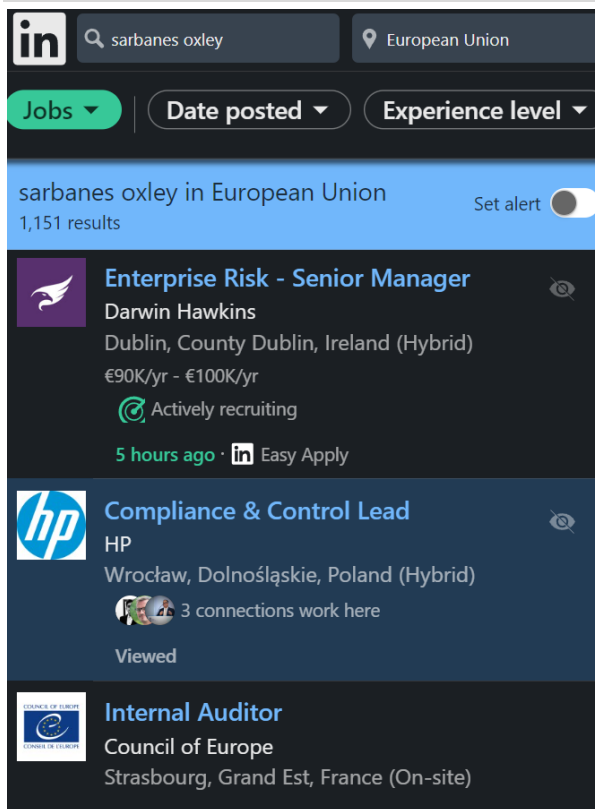
in sarbanes oxley India

Jobs Date posted Experience level

sarbanes oxley in India 977 results Set alert

Goldman Sachs Internal Audit-Bengaluru-Senior Vice President-Business Audit
Goldman Sachs
Bengaluru, Karnataka, India
7 connections work here
Viewed

hp Compliance & Control Lead
HP
Bengaluru, Karnataka, India (Hybrid)
3 connections work here
7 hours ago



Contact Us

Lyn Spooner

Email: lyn@sarbanes-oxley-association.com

George Lekatis

President of the SOXCPA

1200 G Street NW Suite 800,

Washington DC 20005, USA

Email: lekatis@sarbanes-oxley-association.com

Web: www.sarbanes-oxley-association.com

HQ: 1220 N. Market Street Suite 804,

Wilmington DE 19801, USA



Our reading room:

https://www.sarbanes-oxley-association.com/Reading_Room.htm