



Monday, March 16, 2026

Top 10 risk and compliance related news stories and world events that (for better or for worse) shaped the week's agenda, and what is next.

When the [World Economic Forum](#) warns that the defining risks of our era are systemic, cascading, and structurally interconnected, it places a quiet but profound responsibility upon boards, regulators, and executives, to recognize that the architecture of governance itself must evolve.



The Global Risks Report describes a world in which geopolitical fragmentation, technological acceleration, climate stress, financial instability, and regulatory divergence intersect in complex and unpredictable ways.

The new [systemic risk thinking](#) is a significant intellectual advancement. It forced institutions to acknowledge that a cyber incident could become a liquidity event, that a climate event could become a credit event, and that a geopolitical conflict could become a regulatory shock. It compelled boards to see [interdependence](#) where previously they saw discrete exposures.

But systemic risk thinking, as currently practiced, remains incomplete. The report explains why crises cascade. It [does not fully explain](#) how fragility itself can be leveraged, amplified, or strategically exploited. This is where [hybrid risk management](#) emerges, as a conceptual and operational evolution.

Hybrid risk management recognizes that interdependence can be transformed into an instrument of strategic pressure. Supply chains may become vehicles of geopolitical leverage. Sanctions may operate as instruments of economic statecraft. Cyber operations may intersect with legal enforcement, market confidence, and public perception in ways that are neither linear nor incidental.

In such an environment, risk can no longer be assessed solely through the [traditional lens of probability and impact](#). It must also be evaluated in terms of how different vulnerabilities interact across systems, and whether those vulnerabilities may be deliberately exploited by state or non-state actors.

Hybrid risk management requires the [integration](#) of geopolitical intelligence, regulatory foresight, technological oversight, and operational resilience into a single governance architecture.

The World Economic Forum has made a [significant institutional contribution](#) by explaining the structural dimensions of systemic vulnerability that increasingly characterize global governance and markets. The next step is architectural. Institutions must evolve from understanding interconnectedness to governing within it. They must transition from mapping risk convergence to engineering resilience against strategic exploitation of convergence.

[Systemic risk thinking](#) taught us that no institution operates in isolation. Hybrid risk management reminds us that no institution operates in a neutral environment.

I remember the Global Risks Report 2023 (the 18th edition), where the Forum used the term “[polycrisis](#)” (and repeated it 21 times in 98 pages). It described how multiple global risks interact and amplify one another, creating a cluster of interconnected threats whose combined effect is greater than the sum of their parts.

If the term polycrisis feels [linguistically excessive](#), it is only because reality has outpaced our vocabulary.

Best regards,



George Lekatis
President of the IARCP

Introducing an Advanced Specialization in Hybrid Risk and Resilience management, exclusively for CRCMPs.

We are thrilled to announce the launch of the Certified Risk and Compliance Management Professional in Hybrid Risk and Resilience Management - CRCMP(HR²M), online training and certification program.

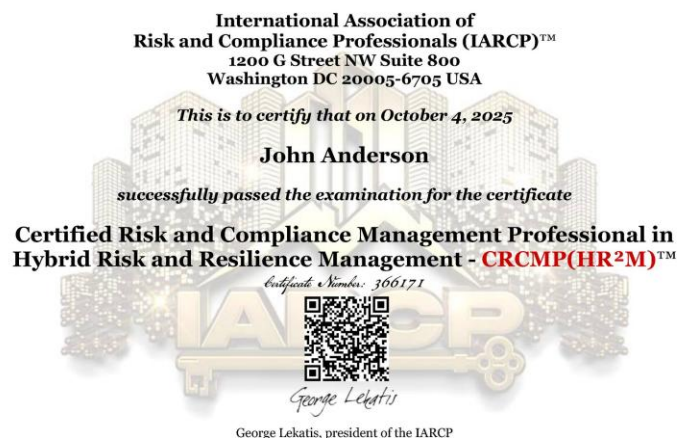
It builds on the solid foundation of the CRCMP designation and equips participants with cutting-edge knowledge to understand, identify, assess, and effectively manage complex hybrid risks.

The program prepares CRCMPs to strengthen organizational resilience across interconnected domains, including geopolitical and regulatory risk, counterintelligence, and supply chain resilience, while advancing capabilities in hybrid threat psychology, hybrid stress testing, and crisis management, ensuring readiness for an increasingly complex risk landscape.

Enrollment in the CRCMP(HR²M) program is restricted to professionals who have already passed the CRCMP exam. To preserve the credibility and value of this credential, the association does not allow substitutions, equivalency credits, or waivers of any kind. The curriculum assumes mastery of the CRCMP body of knowledge.

Learn more and view the full course synopsis:

https://www.risk-compliance-association.com/CRCMP_HR2M.htm



Number 1 (Page 6)

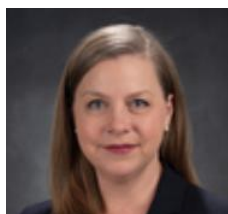
[Basel Committee issues a consolidated version of its guidelines](#)



Number 2 (Page 8)

[Supervision and Regulation](#)

Michelle W. Bowman, Vice Chair for Supervision, Board of Governors of the Federal Reserve System, before the Committee on Banking, Housing, and Urban Affairs, U.S. Senate, Washington, D.C.



Number 3 (Page 14)

[Directive \(EU\) 2024/927 \(AIFMD II\)](#)

[Member State transposition deadline: 16 April 2026.](#)



European
Union

Number 4 (Page 16)

[President Trump's CYBER STRATEGY for America, March 2026](#)

THE WHITE HOUSE
WASHINGTON

Number 5 (Page 21)

[Turning size into scale - Europe's new growth model](#)

Acceptance speech by Ms Christine Lagarde, President of the European Central Bank, for the 2026 Paul A Volcker Lifetime Achievement Award at the 42nd Annual NABE Economic Policy Conference, Washington DC



Number 6 (Page 29)

[SEC Adopts Final Rules for the Holding Foreign Insiders Accountable Act](#)



U.S. Securities and
Exchange Commission

Number 7 (Page 31)

[BIOSAFETY AND BIOSECURITY
Comparing the U.S. and Selected G20 Members](#)



United States Government Accountability Office
Report to Congressional Addressees

Number 8 (Page 33)

[Codex Security: now in research preview](#)



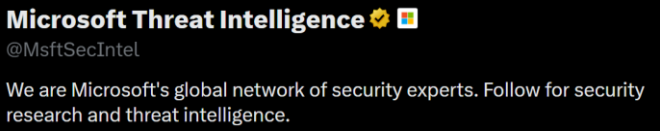
Number 9 (Page 36)

[Meta Takes Legal Action Against Scam Advertisers](#)



Number 10 (Page 39)

[Luring users into running trojanized gaming utilities](#)



Number 1

Basel Committee issues a consolidated version of its guidelines



- The Basel Committee has published a consultation on a consolidated version of its guidelines and sound practices.
- The consolidated version aims to improve accessibility and substantially streamline guidance materials.
- Comments on the consultation are requested by [26 June 2026](#).

The Basel Committee on Banking Supervision launched a [new section of its website](#) that sets out a consolidated version of its guidelines and sound practices for banks and supervisors.

You may visit: https://www.bis.org/basel_consolidated_guidelines/index.htm

You are viewing a draft version of the Consolidated Guidelines that is under [consultation](#).

The Basel Consolidated Guidelines

This page sets out the guidelines and sound practices issued by the Basel Committee on Banking Supervision (BCBS). The [application page](#) outlines the implementation expectations for guidelines and sound practices, and their scope of application. The consolidated guidelines and sound practices comprise the 13 modules listed below. Each module is divided into chapters. Each chapter includes links to the original source publications from which the contents of the chapter are based, related standards, related guidelines or sound practices, and other publications that are relevant to a particular topic.

The consolidated guidelines and sound practices aim to improve the accessibility of the Committee's outputs by setting them out in a more user-friendly format. The website has been published, initially in draft form, together with a consultative document to gather feedback from stakeholders.

Guidelines and sound practices are currently published on the Committee's section of the Bank for International Settlements (BIS) website, as a series of pdf documents. The consolidated guidelines reorganise the contents of existing guidelines and sound practices into a modular format. This format replicates the approach used by the Committee in the development of its consolidated set of standards (the Basel Framework), which was launched in December 2019 and was well received by stakeholders.

The publication of the guidelines and sound practices in this new format has focused on reorganising existing materials. There was no intention to introduce new expectations through the current exercise. As part of this process, the Committee has also taken the opportunity to remove content that it considers to be outdated, duplicative, or superseded. Through this exercise, the Committee has substantially reduced the volume of its guidance materials by approximately 75%. The final output reflects a more streamlined and evergreen set of expectations.

The Committee intends to periodically review its guidelines and sound practices as standards, supervisory practices and the financial system evolve.

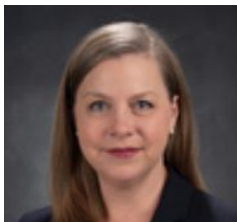
The Committee welcomes comments on the three questions set out in the consultative document. Comments should be uploaded here by Friday 26 June 2026. All comments will be published on the Bank for International Settlements website unless a respondent specifically requests confidential treatment.

To learn more: <https://www.bis.org/press/p260226.htm>



*Number 2***Supervision and Regulation**

Michelle W. Bowman, Vice Chair for Supervision, Board of Governors of the Federal Reserve System, before the Committee on Banking, Housing, and Urban Affairs, U.S. Senate, Washington, D.C.



Chairman Scott, Ranking Member Warren, and Members of the Committee, thank you for the opportunity to testify on the Federal Reserve's supervisory and regulatory activities.

My testimony today will focus on two areas. First, the current state of the banking sector. Second, progress on my priorities as Vice Chair for Supervision since my confirmation last year.

My priorities relate to the effectiveness, safety and soundness, and stability of our financial system, and the effectiveness and accountability of our regulation and supervision of that system.

Our supervision and regulation must support a safe and sound banking system that fosters economic growth while also safeguarding financial stability.

Banking Conditions

I will begin by providing an update on banking conditions. The banking system remains sound and resilient. Banks continue to report strong capital ratios and significant liquidity buffers, which position them well to support economic growth. The overall health of the banking sector is demonstrated by continued growth in lending, a decline in non-performing loans across most categories, and strong profitability.

Notably though, non-bank financial institutions continue to increase their share of the total lending market, creating strong competition for regulated banks without facing the same capital, liquidity, and other prudential standards. This competition from nonbanks includes payments and lending.

Regulated banks must have the tools and flexibility to innovate and compete effectively while maintaining the safety and soundness that defines our banking system. To that end, the Federal Reserve is encouraging banks to innovate to improve the products and services they provide.

We have rescinded several policies that were intended to hinder innovation. We are also working with the other banking regulators to develop regulations that include capital and liquidity for stablecoin issuers as required by the GENIUS Act.

Additionally, we will provide clarity regarding the treatment of digital assets to ensure that the banking system is well placed to support digital asset activities. This includes clarity on the permissibility of activities and willingness to provide regulatory feedback on proposed new use cases.

As a regulator, it is my role to encourage innovation in a responsible manner, and we must continuously improve our ability to supervise the risks that innovation may present to safety and soundness.

Prioritizing Community Banking Issues

One of the Federal Reserve's goals is to tailor our regulatory and supervisory framework so that it accurately reflects the risk that different bank business models pose to the financial system. Community banks are and should be subject to less stringent standards than large banks, and there is significant opportunity to tailor regulations and supervision to the unique needs and circumstances of these banks. We cannot continue to push policies and supervisory expectations designed for the largest banks down to smaller, less risky, and less complex banks.

Therefore, I support efforts by Congress to reduce burden on community banks. I support increasing static and outdated statutory thresholds, including asset thresholds, that have not been updated for many years.

Asset growth due, in part, to inflation and economic growth over time has resulted in small banks becoming subject to laws and regulations that were intended for much larger banks. I also support improvements to the Bank Secrecy Act and anti-money laundering framework that will assist law enforcement while minimizing the unnecessary regulatory burden that disproportionately falls on community banks.

As an example, the thresholds for Currency Transaction Reports and Suspicious Activity Reports have not been adjusted since they were established, despite decades of significant growth in the economy and financial system. These thresholds should be updated to more effectively focus resources on those transactions and activities that truly are suspicious.

Where possible, the Federal Reserve is taking actions to further tailor regulatory and supervisory measures to support community banks in more effectively serving their customers and communities.

We are carefully considering comments on our proposed changes to the community bank leverage ratio. These changes would provide community banks greater flexibility and optionality in their capital framework while preserving safety and soundness and enabling these banks to focus on their core mission: to support economic growth and activity through lending to households and businesses.

We also recently released new capital options for mutual banks, including capital instruments that could qualify as tier 1 common equity or as additional tier 1

equity. We are open to further refinement of these options and look forward to feedback.

It is also time to tailor the merger and acquisition and de novo chartering application processes for community banks. We are exploring streamlining those processes and updating the Federal Reserve Board's (Board's) merger analysis to accurately reflect and consider competition among small banks.

Now is the time to build a framework for community banks that recognizes their unique strengths and supports their critical role in providing financial services to businesses and families throughout the United States.

Effective regulatory frameworks are an essential operational foundation for our ability to appropriately supervise financial institutions. We are currently conducting our third Economic Growth and Regulatory Paperwork Reduction Act (EGRPRA) review to eliminate outdated, unnecessary, or overly burdensome rules.

My expectation is that, unlike previous EGRPRA reviews, this review will create substantive change. This type of regular assessment should be an ongoing aspect of our work. A proactive approach will ensure that regulations are responsive and adaptable to the evolving needs of, and conditions in, the banking sector.

Regulatory Agenda for Large Banks

We are also modernizing and simplifying the Federal Reserve's regulation of large banks. The Board is considering modifications to each of the four pillars of our regulatory capital framework for large banks: stress testing, the supplementary leverage ratio, the Basel III framework, and the G-SIB surcharge.

Stress Testing

The Board released a proposal in October of last year to enhance public accountability and ensure robust outcomes of our stress testing framework and practices. The proposal includes disclosure of the stress test models, the framework for designing stress test scenarios, and the scenarios for the 2026 stress tests.

The proposed model changes reduce volatility in capital requirements by addressing some shortcomings in our models and by providing full transparency.

The proposal also ensures that any future significant changes to these models will benefit from public input prior to implementation. Earlier this month, after reviewing the comments on the 2026 scenarios, the Board published the final scenarios for the 2026 stress test.

Supplementary Leverage Ratio (SLR)

The banking agencies also finalized changes to the enhanced SLR proposal for U.S. global systemically important banking organizations (G-SIBs). These

changes help ensure that leverage capital requirements serve primarily as a backstop to risk-based capital requirements, as originally intended.

When the leverage ratio generally becomes the binding constraint, it discourages banks and dealers from engaging in low-risk activities, including holding Treasury securities, because the leverage ratio assigns the same capital requirement across both safe and risky assets.

Basel III

The Board, together with our federal banking agency colleagues, has taken steps to advance Basel III in the United States. Finalizing Basel III reduces uncertainty and provides clarity on capital requirements, enabling banks to make better-informed business and investment decisions.

My approach is to calibrate the new framework from the bottom up, rather than reverse engineer changes to achieve predetermined or preconceived outcomes to capital requirements. These changes will modernize capital requirements to support market liquidity, affordable homeownership, and safety and soundness.

In particular, the capital treatment of mortgage loans and mortgage servicing assets under the U.S. standardized approach has resulted in banks reducing their participation in this important lending activity, limiting access to mortgage credit. We are considering approaches to differentiate the riskiness of mortgages in ways that will benefit financial institutions of all sizes, not just the largest banks.

G-SIB Surcharge

In addition, the Federal Reserve is working to refine the G-SIB surcharge framework in coordination with broader capital framework reform efforts. It is essential that our comprehensive framework strikes the right balance between safety and soundness, ensuring financial stability and promoting economic growth.

We must maintain a robust financial system without imposing unnecessary burdens that impede economic growth while carefully calibrating the surcharge to avoid inadvertently inhibiting the ability of the banking sector to support the broader economy.

Supervision

Turning to the Federal Reserve's supervisory program, over the last seven years, I have consistently emphasized the importance of transparency, accountability, and fairness in supervision.

These principles guided my approach as a state banking commissioner, and they continue to guide my approach today and I remain focused on the Board's responsibility to promote the safe and sound operations of banks and the stability of the U.S. financial system.

An effective supervisory framework must focus on the core material risks to banks operations and to the stability of the broader financial system. Let me be clear: those core material risks include non-financial risks where they pose threats to safety and soundness. Strong risk management, whether in credit, liquidity, cybersecurity, or operations, remains essential, and we will continue to examine for these risks

Supervision must also be tailored, matching oversight to each institution's size, complexity, and risk profile. I have consistently supported a risk-focused, tailored approach to supervision and regulation. This approach is consistent with the direction I provided to Federal Reserve examiners in guidance that was also publicly released last fall.

One example of this implementation is our work on new and existing Matters Requiring Attention (MRAs), ensuring they are based on threats to safety and soundness and are aligned with this guidance using clear language and identifying transparent expectations.

This review is an opportunity to recalibrate—to prioritize what truly matters—and it complements the supervision that is ongoing. We will also continue to issue supervisory findings when necessary. It is not a reduction of our supervisory toolkit or approach.

Another step we are taking to address these concerns is through the review of our CAMELS framework, which has been in place since 1979 with minimal modification. The management ('M') component, for example, has been widely criticized as an arbitrary and highly subjective catch-all category.

Establishing clear metrics and parameters for all of the components will ensure transparency and objectivity in our supervisory assessments. Bank ratings should reflect overall safety and soundness, not just isolated deficiencies in a single component.

Prior to the recent modification of the Large Financial Institution (LFI) ratings system, banks have often been labeled as not "well managed" despite strong capital and liquidity positions. To address this shortcoming, the Board recently finalized revisions to the LFI ratings system that address the mismatch between ratings and overall firm condition.

In addition to sharpening the focus on core material risks, updating our ratings frameworks, and refining our supervisory tools, we are also reviewing our supervisory directives, reports, and actions. This includes an independent third-party review of the 2023 bank failures.

This review will objectively examine why our supervision fell short and deliver actionable findings to further strengthen our supervisory practices. Further, the Board has officially ended the practice of using reputational risk in our supervisory program.

This change addressed legitimate concerns that supervision around an ambiguous concept like reputational risk could improperly influence a bank's business decisions.

We have also proposed a regulation to prevent Board personnel from encouraging, influencing, or compelling banks to debank or refuse to bank a customer due to their constitutionally protected political or religious beliefs, associations, speech, or conduct.

Let me be clear: banking supervisors should never, and will not under my watch, dictate which individuals and lawful businesses a bank is permitted to serve. Banks must remain free to make their own risk-based decisions to serve individuals and lawful businesses.

Finally, I am also increasing supervisory transparency. We have begun publishing internal supervisory manuals, which started with our manuals for G-SIBs.

Thank you again for the opportunity to appear before you this morning. I look forward to answering your questions.

To learn more:

<https://www.federalreserve.gov/newsevents/testimony/bowman20260226a.htm>



Number 3

Directive (EU) 2024/927 (AIFMD II)

Member State transposition deadline: 16 April 2026.



European
Union

Directive (EU) 2024/927 (AIFMD II) was adopted 13 March 2024, published in the Official Journal 26 March 2024, and entered into force 15 April 2024.

Member State transposition deadline: **16 April 2026.**

Article 3

Transposition

1. Member States shall adopt and publish, by 16 April 2026, the laws, regulations and administrative provisions necessary to comply with this Directive. They shall immediately communicate the text of those measures to the Commission.

They shall apply those measures from 16 April 2026, with the exception of the measures transposing Article 1(12), and those transposing Article 2(7) with regard to Article 20a of Directive 2009/65/EC, which they shall apply from 16 April 2027.

When Member States adopt those measures, they shall contain a reference to this Directive or be accompanied by such a reference on the occasion of their official publication. Member States shall determine how such reference is to be made.

2. Member States shall communicate to the Commission the text of the main measures of national law which they adopt in the field covered by this Directive.

ANNEX II

**ANNEX V - LIQUIDITY MANAGEMENT TOOLS AVAILABLE TO AIFMs
MANAGING OPEN-ENDED AIFs**

1. **Suspension of subscriptions, repurchases and redemptions:** suspension of subscriptions, repurchases and redemptions means temporarily disallowing the subscription, repurchase and redemption of the fund's units or shares.
2. **Redemption gate:** a redemption gate means a temporary and partial restriction of the right of unit-holders or shareholders to redeem their units or shares, so that investors can only redeem a certain portion of their units or shares.
3. **Extension of notice periods:** the extension of notice periods means extending the period of notice that unit-holders or shareholders must give to fund managers, beyond a minimum period which is appropriate to the fund, when redeeming their units or shares.
4. **Redemption fee:** redemption fee means a fee, within a predetermined range that takes account of the cost of liquidity, that is paid to the fund by unit-holders or shareholders when redeeming units or shares, and that ensures that unit-holders or shareholders who remain in the fund are not unfairly disadvantaged.
5. **Swing pricing:** swing pricing means a pre-determined mechanism by which the net asset value of the units or shares of an investment fund is adjusted by the application of a factor ("swing factor") that reflects the cost of liquidity.

6. **Dual pricing:** dual pricing means a pre-determined mechanism by which the subscription, repurchase and redemption prices of the units or shares of an investment fund are set by adjusting the net asset value per unit or share by a factor that reflects the cost of liquidity.
7. **Anti-dilution levy:** anti-dilution levy means a fee that is paid to the fund by a unit-holder or shareholder at the time of a subscription, repurchase or redemption of units or shares, that compensates the fund for the cost of liquidity incurred because of the size of that transaction, and that ensures that other unit-holders or shareholders are not unfairly disadvantaged.
8. **Redemption in kind:** redemption in kind means transferring assets held by the fund, instead of cash, to meet redemption requests of unit-holders or shareholders.
9. **Side pockets:** side pockets means separating certain assets, whose economic or legal features have changed significantly or become uncertain due to exceptional circumstances, from the other assets of the fund.

(30) To enable AIFMs of open-ended AIFs established in any Member State to deal with redemption pressures under stressed market conditions, AIFMs should be required to select and include in the AIF rules or instruments of incorporation **at least two liquidity management tools from the harmonised list set out in Annex V, points 2 to 8, to Directive 2011/61/EU**. By way of derogation, where an AIFM manages an AIF that is authorised as a money market fund in accordance with Regulation (EU) 2017/1131 of the European Parliament and of the Council ⁽²⁰⁾, the AIFM should be able to decide to select only one liquidity management tool from that list. Those liquidity management tools should be appropriate to the investment strategy, the liquidity profile and the redemption policy of the AIF. AIFMs should activate such liquidity management tools where necessary to safeguard the interests of the AIF's investors. In addition, AIFMs of open-ended AIFs should always have the possibility of temporarily suspending subscriptions, repurchases and redemptions or of activating side pockets, in exceptional circumstances and where justified having regard to the interests of the AIF's investors. Where an AIFM takes a decision to suspend subscriptions, repurchases and redemptions, it should without undue delay notify the competent authorities of its home Member State. Where an AIFM decides to activate or deactivate side pockets, it should notify the competent authorities of its home Member State within a reasonable timeframe prior to the activation or deactivation of that liquidity management tool. An AIFM should also notify the competent authorities of its home Member State where it activates or deactivates any other liquidity management tool in a manner that is not in the ordinary course of business as envisaged in the AIF rules or instruments of incorporation. That would allow supervisory authorities to better handle potential spill-overs of liquidity tensions into the wider market.

To learn more: <https://eur-lex.europa.eu/eli/dir/2024/927/oj/eng>



Number 4

President Trump's CYBER STRATEGY for America, March 2026

THE WHITE HOUSE
WASHINGTON

Cyberspace was born in America. American talent, innovation, research, and powerful government capabilities combined to create a dynamic, thriving, digital world that every American relies on for information, economic opportunity, and our basic way of life. Indeed, the cyber domain is key to President Trump's actions to ensure America leads the world in finance, innovation and emerging technology, military power, and manufacturing.

Freedom and safety in cyberspace, however, cannot be taken for granted. Adversaries and cybercriminals exploit cyberspace to advance authoritarianism, suppress democracy, and undermine our national and economic security.

Unlike other Administrations, the Trump Administration will not tinker at the edges and apply partial measures and ambiguous strategies that neglect the growing number and severity of cyber threats. President Trump will continue to address threats in cyberspace directly.

America enjoys unrivalled technological and economic innovation, unmatched military power, and a society devoted to free and open expression. Every American should take practical steps to protect themselves and their families in cyberspace, but America's citizens do not stand alone. President Trump has demonstrated time and again that he is determined to make Americans secure and prosperous by harnessing all of our comparative advantages. This strategy is a continuation of President Trump's actions, and directly supports the National Security Strategy by putting America first in cyberspace.

Our adversaries and cyber criminals target our families, neighbors, small businesses, farmers, first responders, patients, and senior citizens in cyberspace. They disrupt critical services like healthcare, banking, food supply, and water treatment. They impose tremendous costs on our economy and make everyday goods less affordable.

President Trump's actions, however, send a clear message: we will act to defend our interests in cyberspace. Whether destroying online scammers' networks and seizing \$15 billion of their stolen money, supporting a globe-spanning operation to obliterate Iran's nuclear infrastructure, or leaving our adversaries blind and uncomprehending during a flawless military operation to bring international narco-terrorist Nicolas Maduro to justice, adversaries are on notice that America's cyber operators and tools are the best in the world and can be swiftly and effectively deployed to defend America's interests.

Americans re-elected President Trump to put America first. This strategy communicates the Trump Administration's cyber vision and approach to the American people, to Congress, to our partners in industry and allies across the globe—and also to adversaries. It explains the Administration's priorities,

summarized in six policy pillars, which will guide action and resourcing through the follow-on policy vehicles. This strategy builds on President Trump's actions to date, and requires a level of coordination, commitment, and political will never before marshalled against cyber threats. President Trump's leadership has created a new era in cyberspace.

Moving Forward

Our resolve is absolute. We will act swiftly, deliberately, and proactively to disable cyber threats to America. We will not confine our responses to the "cyber" realm. We will undertake an unprecedented effort, operating in a coordinated and sustained fashion across the U.S. government. Working with allies across the globe, we will promote U.S. interests and security. We will fight the curtailment of free speech. We will outcompete adversaries who sell "low cost" AI and digital technologies that carry embedded censorship, surveillance, and ideological bias. We will partner closely with industry and academia, at the speed and scale commensurate with the threats we face, and in accordance with our values.

President Trump has made targeting Americans a hazardous business. Our adversaries have and will increasingly feel the consequences of their actions; we will dismantle networks, pursue hackers and spies, and sanction lawless foreign hacking companies. We will unveil and embarrass online espionage, destructive propaganda and influence operations, and cultural subversion.

By disrupting adversaries' cyber campaigns, and making our networks more defensible and resilient, we will unleash innovation, accelerate economic growth, and secure American technology dominance. We will remove burdensome, ineffective regulations so that our industry partners innovate quickly in emerging technologies. Partners in the private sector must be able to respond and recover quickly to ensure continuity of the American economy. We will defend our federal systems, critical infrastructure, and supply chains by putting security at the foundation of innovation. We will modernize our information systems so that old infrastructure does not choke innovation. We will engage internationally through diplomacy, commerce, and operations to ensure norms and standards reflect our values. We will leverage the immense talents and ingenuity of our private sector research base. We will establish a new level of relationship between the public and private sectors to defend America in peace and war.

Pillars of Action

Six Policy Pillars underpin this strategy and will guide implementation and measures for success.

1. Shape Adversary Behavior

American citizens, companies, and our allies should not have to fend off sophisticated military, intelligence, and criminal adversaries in cyberspace alone. We will deploy the full suite of U.S. government defensive and offensive cyber operations.

We will unleash the private sector by creating incentives to identify and disrupt adversary networks and scale our national capabilities. We must detect, confront, and defeat cyber adversaries before they breach our networks and systems.

We will erode their capacity and capabilities, and use all instruments of national power to raise the costs for their aggression. We will counter the spread of the surveillance state and authoritarian technologies that monitor and repress citizens.

Cybercrime and intellectual property theft are some of the greatest threats to global economies. We will uproot criminal infrastructure and deny financial exit and safe haven.

Defending cyberspace and safeguarding freedom is a collective effort—the distribution of cost and responsibility must be fair across the U.S. and allies who share our democratic values. We will work together to create real risk for adversaries who seek to harm us, and impose consequences on those who do act against us.

2. Promote Common Sense Regulation

Cyber defense should not be reduced to a costly checklist that delays preparedness, action, and response. We will streamline cyber regulations to reduce compliance burdens, address liability, and better align regulators and industry globally.

We will streamline data and cybersecurity regulations to ensure that the private sector has the agility necessary to keep pace with rapidly evolving threats. We will emphasize the right to privacy for Americans and American data.

3. Modernize and Secure Federal Government Networks

We will accelerate the modernization, defensibility, and resilience of federal information systems by implementing cybersecurity best practices, post-quantum cryptography, zero-trust architecture, and cloud transition.

We will work to elevate the importance of cyber in government leadership and in the board room. We will use the best technologies and teams to constantly test and hunt for malicious actors on federal networks.

We will prioritize the security and resilience of the National Security Systems that underpin our military, intelligence, and civilian enterprises.

We will work to adopt AI-powered cybersecurity solutions to defend federal networks and deter intrusions at scale.

Working across the government to modernize and create competitive procurement processes, we will remove barriers to entry so that the government can buy and use the best technology.

4. Secure Critical Infrastructure

We will identify, prioritize, and harden America's critical infrastructure and secure its supply chains, including defense critical infrastructure and adjacent vendors, private companies, networks, and services—such as the energy grid, financial and telecommunication systems, data centers, water utilities, and hospitals—securing information and operational technology supply chains.

We must move away from adversary vendors and products, promoting and employing U.S. technologies. We will deny our adversaries initial access, and in the event of an incident, we must be able to recover quickly. We will galvanize the role of state, local, Tribal, and territorial authorities as a complement to—not a substitute for—our national cybersecurity efforts.

5. Sustain Superiority in Critical and Emerging Technologies

Securing American innovation and protecting our national intellectual advantage will be paramount. We will build secure technologies and supply chains that protect user privacy from design to deployment, including supporting the security of cryptocurrencies and blockchain technologies.

We will promote the adoption of post-quantum cryptography and secure quantum computing. And we will secure the AI technology stack—including our data centers—and promote innovation in AI security. We will swiftly implement AI-enabled cyber tools to detect, divert, and deceive threat actors. We will rapidly adopt and promote agentic AI in ways that securely scale network defense and disruption.

Through cyber diplomacy, we will ensure that AI—particularly generative AI and agentic AI—advances innovation and global stability. We will secure the data, infrastructure, and models that underpin U.S. leadership in AI and we will call out and frustrate the spread of foreign AI platforms that censor, surveil, and mislead their users.

6. Build Talent and Capacity

President Trump has called America's cyber workforce a strategic asset that “protects the American people, the homeland, and the American way of life.” It is an asset worthy of great investment and essential to our nation's economic prosperity and security. We need a pipeline that develops and shares talent.

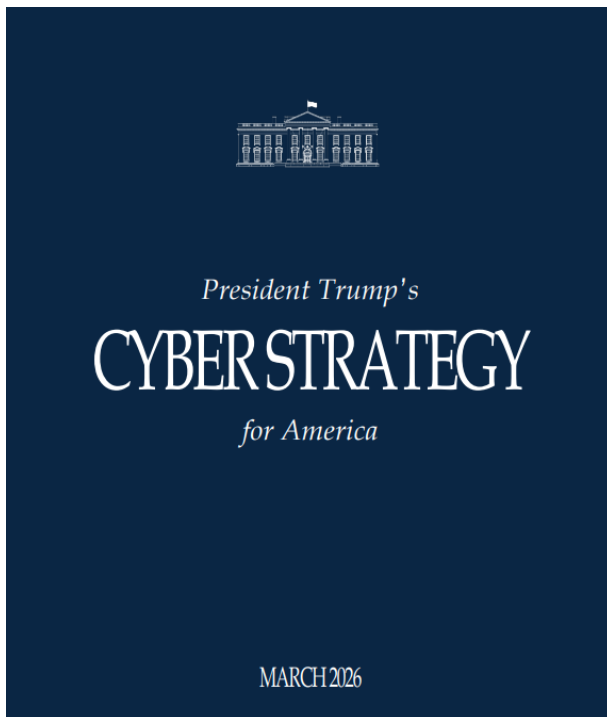
It must be pragmatic and accessible—reconciling and taking advantage of existing avenues within academia, vocational and technical schools, corporations, and venture capital opportunities—to educate and train our existing cyber workforce across industries and occupations, and to recruit the next generation to design and deploy exquisite cyber technologies and solutions.

We will eliminate roadblocks that prevent industry, academia, government, and the military from aligning incentives and building a highly skilled cyber

workforce. We will harness the existing resources, authorities, talents, and ingenuity that make America great.

Conclusion

This strategy makes clear the course President Trump has pursued in cyberspace, and the direction the U.S. government will pursue with increasing impact. President Trump has acted to ensure that Americans—especially future generations—will have a strong country where they are secure and defended, and a future defined by individual freedom, economic prosperity, and opportunity. President Trump will continue showing those who harm our interests and attack our values in cyberspace place themselves at risk.



To learn more:

<https://www.whitehouse.gov/wp-content/uploads/2026/03/President-Trump-Cyber-Strategy-for-America.pdf>



Number 5[Turning size into scale - Europe's new growth model](#)

Acceptance speech by Ms Christine Lagarde, President of the European Central Bank, for the 2026 Paul A Volcker Lifetime Achievement Award at the 42nd Annual NABE Economic Policy Conference, Washington DC



There is perhaps no greater question in political philosophy than whether history is shaped by individuals or by the forces that carry them. Tolstoy devoted the philosophical heart of *War and Peace* to this question.

His answer was uncompromising: the so-called great men of history were not its authors but its instruments.

This is a powerful thesis. But in the history of economic institutions, the evidence points both ways. Institutions are shaped by the laws they are built upon and the mandates they are given. But they are also shaped, sometimes decisively, by the people who serve them.

Perhaps nowhere is this clearer than in the story of Paul Volcker, whom this lecture honours.

What Volcker did in the early 1980s went beyond taming inflation. He transformed the character of the Federal Reserve System. Before he came along, the Fed's independence had been established in principle by the US Treasury Federal Reserve Accord in 1951, but it had not always been defended with equal vigour.

Arthur Burns had given a lecture on what he called “the anguish of central banking” – an argument, in essence, on why central banks could not be expected to control inflation against the weight of political pressure.

Volcker offered no such apology. He raised rates to levels that induced the deepest recession since the 1930s and came under sustained political attack.

His act of personal conviction changed the trajectory of central banking not only in the United States, but worldwide. It is the same tradition that Jay Powell has upheld with such resolve.

Their efforts serve as an important reminder that, while we need legal frameworks to ensure central bank independence, frameworks alone are never enough.

Laws can be rewritten, mandates reinterpreted, institutional norms hollowed out. Independence ultimately has to live in the culture and conviction of the people who serve these institutions – because sooner or later, the legal limits will be tested.

European models of decision-making

Europe, of course, has been accused of lacking precisely this kind of decisiveness. US Treasury Secretary Bessent captured the sentiment recently with his quip about “the dreaded European working group”. It is a familiar charge, and not always an unfair one.

Too often, Europe has allowed itself to become entangled in its own procedures. Progress has been blocked by the need for unanimity, slowed by the impulse to harmonise every detail across 27 countries, and frustrated by an instinct to regulate before we innovate. These are real problems, and Europeans know it.

Some of this is the inevitable result of how the EU has been built. It was conceived to require compromise, diffuse authority and ensure that no single country could impose its will on the others. That was a deliberate choice, born of a continent where the unchecked power of individual states had too often led to catastrophe.

But the idea that this structure condemns us to inaction is wrong. And the clearest evidence of this is the institution I represent.

With 27 members, the ECB’s Governing Council is by far the largest monetary policy committee among the major central banks. The Federal Reserve has 12 voting members. The Bank of England and the Bank of Japan each have nine.

One might expect a structure of this size to result in inertia. In practice, it gives us distinctive strengths.

First, it makes us harder to influence.

A decision forged on the basis of 27 informed perspectives is harder to reach, but it is also far more difficult for any single government to influence or reverse under pressure. In that sense, our very structure reinforces our independence.

Second, our diversity is an asset in times of high uncertainty.

Each member of the Governing Council brings a different assessment of how the economy is evolving, how monetary policy is transmitting and where the risks lie. Taken together, these perspectives form a natural distribution around the central forecast, mapping the uncertainty in a way no single decision-maker can.

When you are confronted with a pandemic, an energy crisis, a war and a reconfiguration of global trade within the space of a few years, that diversity becomes a form of institutional insurance.

Third, none of this comes at the cost of speed.

When the pandemic struck, we designed and launched a €750 billion emergency asset purchase programme within days. When inflation surged, we raised rates by 450 basis points in a little over a year, the fastest tightening cycle in the ECB's history. We then cut them again by 200 basis points as inflation stabilised at our medium-term target.

Of course, monetary policy is a special domain. We have a clear mandate to guide our decisions, whereas lawmakers face more competing objectives. But the wider EU has also shown it can act when confronted with urgent crises.

Our monetary response during the pandemic, for example, was made far more effective by the decision of EU leaders to create the Next Generation EU programme, a €750 billion common fiscal instrument agreed within months and financed through joint borrowing. This kind of programme would have been unthinkable just a year earlier.

The question today is whether Europe can act not only under the pressure of crisis, but also on the structural issues that determine long-term growth.

The argument that Europe is incapable of this kind of change – that our procedures condemn us to stagnation – is being tested against the evidence. And the evidence is starting to tell a different story in three key areas.

The changing composition of demand

The first area is in the composition of demand.

For much of the past 15 years, the euro area relied heavily on the rest of the world to generate growth. After the global financial crisis, domestic demand as a share of GDP fell to the bottom of the range among advanced economies. At the same time, the current account shifted from being broadly balanced to showing persistent surpluses.

Fiscal policy played an important role. Between 2009 and 2019, the euro area's cyclically adjusted fiscal stance averaged at a surplus of 0.2% of GDP, compared with a deficit of almost 3.7% in the United States. Inadequate domestic demand was identified by our US partners long before relations became more complicated.

Today, Europeans widely recognise that this model has run its course. It presents two fundamental problems.

First, we now operate in a world in which our largest single export market is subject to tariffs, and where our third-largest export market, China, is running a trade surplus of around USD 1.2 trillion. In such an environment, external demand is inevitably less reliable.

Over the next three years, Eurosystem staff expect exports to expand at roughly half their historical average pace.

Second, this model has meant exporting our savings at a time when we face substantial investment needs at home.

US capital markets now account for roughly one-third of euro area residents' holdings of listed equities, a share comparable to that invested domestically.

These investments have generated significant income gains. In 2025 alone, euro area investors earned almost €200 billion from their US equity holdings, or around 1.3% of GDP. But the broader returns, in productivity gains and innovation, accrue where the capital is deployed. That has overwhelmingly been in the United States.

As an illustration, if the euro area were to deploy some of that capital productively at home – enough to close just one-quarter of the productivity gap with the United States – the gains for the economy could be in the order of €500 billion per year. That is more than twice the income earned on those foreign investments.

Yet a shift is now underway.

Last year, euro area growth reached 1.5%, its strongest performance in three years, despite rising trade tensions. This growth was driven entirely by domestic demand, with net exports subtracting half a percentage point.

Europe's geopolitical needs and macroeconomic interests now point in the same direction: the investment required for security and resilience will also strengthen our domestic growth.

Government spending on defence and infrastructure is rising markedly while simultaneously supporting private investment. AI is providing an additional tailwind: private digital investment has risen by almost 20% since 2020, and our survey of large European corporates points to ongoing strong growth in AI-related spending.

This momentum is likely to be sustained. Much of the increase in defence spending still lies ahead, and investment in data centres and energy grids is now moving into the implementation phase.

Overall, between 2026 and 2028 investment is projected to account for almost 40% of euro area growth – well above its historical average of around one-quarter – representing more than €150 billion in additional cumulative investment.

While these investments are being made to promote Europe's own growth and resilience, they also support a more balanced relationship with our trading partners.

The current account surplus fell to 1.6% of GDP in 2025, down from 2.7% in 2024, and our projections indicate that it should remain around that level. A significant share of what remains reflects the savings behaviour of an ageing population.

New possibilities for supply

The key question for Europe, however, is how stronger demand can translate into stronger sustained growth.

There is a link. Eurosystem research shows that aggregate demand conditions play a role in productivity growth. When revenues rise and financing constraints ease, firms are more likely to increase spending on research and development and adopt new technologies.

But that transmission is not automatic. Looking at domestic demand as a share of GDP, Germany has been near the bottom of the range among large economies for extended periods, while France has been near the top. Yet their long-term growth outcomes have not been markedly different.

The reason is that demand can only bring a sustained increase in growth if firms are able to respond. And longstanding supply-side constraints have limited their capacity to expand, innovate and scale across Europe.

This is where the second shift comes in, and it is on the supply side itself. Europe's private sector is showing that it is ready to adopt new technologies at speed, provided we remove the remaining barriers.

Europe is not leading the way in developing frontier AI models. But if history is any guide, the larger economic prize may lie not in producing these tools, but in applying them across the wider economy.

This is already happening. Providers of digital services in Europe are reporting double-digit growth as firms adopt AI tools. And firms that have deployed AI are seeing productivity gains of around 4% on average.

Europe also has strengths that are not yet fully apparent.

Current estimates of AI's impact on growth are larger for the United States, driven mainly by its strength in AI-intensive services – namely technology, finance and business services – and by much higher levels of digital investment.

But the next wave will be about embedding these tools in complex physical systems, particularly in manufacturing and industrial processes.

Here Europe starts from a position of strength. Even throughout the pandemic and the energy crisis, Europe's high-tech manufacturers continued to raise their productivity, while the broader economy faltered.

A recent survey finds that almost half of EU manufacturing firms are already using AI and big data, compared with less than a third in the United States. European manufacturers are also ahead in the deployment of robotics – 55% versus 36%.

Europe's industrial base – sometimes seen as a legacy of the old economy – may turn out to be its most important asset.

This potential is not lost on investors.

If we go back to late 2024, the mood towards Europe was gloomy: 23% of institutional investors surveyed by the ECB expected to reduce their allocation to Europe over the coming year, while just 8% planned to increase it. By the end of last year, those shares had reversed: just 7% planned to reduce allocation to Europe, while 40% planned to increase it.

Investment is also flowing into the most dynamic sectors. Last year, AI-related deals accounted for more than a third of all European venture capital investment.

The pieces, then, are falling into place: a private sector that is adopting new technologies, and investors willing to finance that adoption.

But whether this potential turns into sustained growth will depend on reforms. Above all, it will depend on whether we create the scale, in markets and in finance, to allow these technologies to diffuse across the entire European economy.

Turning Europe's size into scale

This brings me to the third area of change.

Two major reports since 2024 – by Enrico Letta and Mario Draghi – have set out in detail the internal barriers that still hold Europe back and how to remove them.

The message that emerges most clearly is this: Europe is a sleeping giant. Its potential is immense, but the changes needed to unlock it are not.

This starts with the Single Market. On paper, it is the largest consumer market in the advanced world, consisting of 450 million people. In practice, it remains deeply fragmented.

Services now account for three-quarters of Europe's economy. Yet intra-EU trade in services amounts to only around one-sixth of GDP – roughly the same as our trade in services with the rest of the world.

The barriers are highest where they do the most damage: in digital services, which will drive innovation, and in capital markets, which must finance it.

But what stands out is the leverage: small changes in policy can unlock very large gains in growth.

ECB analysis shows that if internal barriers were as low in all Member States as they are in the Netherlands, trade within the Union could increase by almost 15% for services and 4% for goods, with effects on GDP roughly four times larger than the estimated losses from US tariffs.

The same principle applies to capital markets.

European households hold more than €12 trillion in cash and deposits – roughly one-third of their financial assets. In the United States, the figure is closer to one-tenth.

If EU households were to align their deposit-to-financial assets ratio with that of US households, a stock of up to €8 trillion could be redirected into long-term, market-based investments – or a flow of more than €350 billion annually.

But things are moving, with work underway to remove the obstacles I described earlier.

First, new approaches are emerging that offer integration without full harmonisation.

The proposal for a 28th regime is a good example. Rather than aligning 27 sets of national rules, it would create a single European legal framework that companies can choose to use for cross-border operations.

The logic is not unlike what happened with Delaware in the United States: not harmonisation imposed from above, but a single framework attractive enough that firms opt in voluntarily.

The difference is that Europe's version would sit above national law from the outset, offering a common standard without requiring Member States to change their own rules.

Second, our methods of decision-making are evolving so that those who want to move ahead can do so.

Member States used the enhanced cooperation mechanism, which allows willing participants to collaborate, to provide EU budget support for Ukraine. The EU's recent trade agreement with Mercosur was approved by a qualified majority, bypassing what has long been perceived as an effective veto for large Member States on major trade deals.

And last week, EU leaders set June as the deadline for the first phase of the savings and investments union, the long-stalled effort to integrate Europe's capital markets. The message was clear: if it proves impossible to move forward with all 27 Member States, a smaller group will press ahead.

This is not a break with Europe's past. On the projects that have mattered most, Europe has found a way. The euro began with 11 countries. Schengen began with five. In each case, those who moved first created a centre of gravity that then attracted others.

The same dynamic can apply again. And my message today is: it will.

Conclusion

Let me return, in closing, to my opening question: whether history is shaped by institutions or by the individuals who serve them.

Europe has often been portrayed as a system in which neither truly prevails: too bound by rules to allow strong leadership, too diverse to let institutions flourish.

But defining Europe in these terms would be underestimating its ability to adapt. Precisely because of our structure, we have often had to innovate in order to move forward.

Today, our institutions are evolving so that decisions can be taken at scale. And when unanimity is not possible, those who are ready to act are increasingly doing so.

Our goal is to act within a solid legal framework, while allowing those who are prepared to lead to move first and show the way.

When I was nominated for the ECB Presidency, the question I was asked most by American colleagues was: can Europe really act?

After a pandemic, an energy crisis and a war on our borders, I no longer hear that question. The question now is whether Europe can act with the same resolve on its longstanding structural weaknesses – even when not under pressure from a crisis.

I believe we will. Not because I am optimistic by nature, but because the cost of not acting has finally become impossible to ignore, and because what is needed is not beyond our capacity. It is within our grasp.

Thank you.

To learn more:

<https://www.ecb.europa.eu/press/key/date/2026/html/ecb.sp260223~4c2aa74452.en.html>



Number 6

SEC Adopts Final Rules for the Holding Foreign Insiders Accountable Act



**U.S. Securities and
Exchange Commission**

The Securities and Exchange Commission today adopted final rule and form amendments to reflect the requirements of the recently enacted Holding Foreign Insiders Accountable Act (HFIA), which will increase transparency into the holdings and transactions of directors and officers of **foreign private issuers (FPIs)**.

SECURITIES AND EXCHANGE COMMISSION

17 CFR Parts 240 and 249

[Release No. 34-104903]

RIN 3235-AN75

Holding Foreign Insiders Accountable Act Disclosure

AGENCY: Securities and Exchange Commission.

ACTION: Final rule.

Directors and officers of FPIs with a class of equity securities registered under Section 12 of the Securities Exchange Act of 1934 (Exchange Act) must begin disclosing their holdings and transactions in the FPI's equity securities on March 18, 2026, the effective date of the HFIA Act.

The HFIA Act, enacted on Dec. 18, 2025, amended Section 16(a) of the Exchange Act to require every person who is a director or an officer of an Exchange Act reporting FPI (but not "10 percent holders" who beneficially own more than 10 percent of any class of equity securities of such FPIs) to file Section 16 reports electronically and in English.

The HFIA Act mandates that the Commission issue final regulations (or amend or rescind existing regulations in whole or in part) to carry out the amendments made by the HFIA Act no later than 90 days after the date of enactment.

The SEC's final rule amendments revise the following rules and forms to reflect the changes made by the HFIA Act:

- Rule 3a12-3(b) to remove the current exemption from Section 16 in its entirety and replace it with exemptions from the Section 16(b) short-swing profit rules and Section 16(c) short selling prohibition only
- Rule 16a-2, which identifies persons and transactions subject to Section 16, to exclude 10 percent holders of FPIs' equity securities from the requirements of Section 16(a) and related rules
- Section 16 reports

The adopting release is published on the SEC website and will be published in the Federal Register.

SUMMARY: The Securities and Exchange Commission (“Commission”) is adopting final amendments to certain of its rules and forms under the Securities Exchange Act of 1934 (“Exchange Act”) to reflect the requirements of the Holding Foreign Insiders Accountable Act (“HFIA Act”). The HFIA Act amended Section 16(a) of the Exchange Act to **require directors and officers of a foreign private issuer** with a class of equity securities registered under Section 12 of the Exchange Act to provide disclosure of their beneficial ownership and transactions involving the issuer’s equity securities. The final amendments revise the Commission’s rules and forms to reflect these statutory requirements.

DATES: *Effective date:* March 18, 2026.

To learn more:

<https://www.sec.gov/newsroom/press-releases/2026-23-sec-adopts-final-rules-holding-foreign-insiders-accountable-act>

<https://www.sec.gov/files/rules/final/2026/34-104903.pdf>



Number 7

BIOSAFETY AND BIOSECURITY
Comparing the U.S. and Selected G20 Members



United States Government Accountability Office
Report to Congressional Addressees

What GAO Found

To understand, prevent, and treat infectious diseases, researchers study biological agents, such as bacteria and viruses. In the U.S., federal agencies have established guidelines to help ensure that U.S. biomedical research labs minimize biosafety and biosecurity risks.

Certain principles or “key components” of biosafety and biosecurity may help reduce risks of all biological agents and research. GAO identified 10 key components that describe key steps a U.S. lab should take to mitigate the risks of biological agent research.

The comparability of the selected Group of Twenty (G20) members’ relevant guidance documents to the 10 U.S. key components varied widely. Nine of the 10 selected G20 members in GAO’s review had documents that were comparable to one or more of the U.S. key components for all biological agents and research.

G20 Member	U.S. key components									
	Risk Assessments	Biosafety Program	Biosecurity Program	Occupational Health Program	Emergency and Incident Response	Institutional Policies	Research Review and Oversight	Personnel Training	Inventory Management	Material Transport
African Union	●	◐	◐	○	○	◐	◐	◐	○	○
Australia	●	●	◐	◐	●	◐	●	◐	◐	◐
Canada	●	●	●	●	●	●	●	●	●	●
China	●	●	◐	●	◐	◐	●	●	●	●
European Union	●	●	◐	●	●	●	●	●	●	●
India	◐	●	◐	●	●	◐	●	●	●	●
Japan	○	○	○	○	○	○	○	○	○	○
Mexico	●	●	◐	●	◐	●	●	●	●	◐
South Africa	●	●	○	●	◐	◐	○	●	○	◐
United Kingdom	●	●	○	●	●	◐	●	●	○	●

● Comparable to the U.S.
 ◐ Somewhat comparable to the U.S.
 ○ Not comparable to the U.S./not present

Source: GAO analysis of G20 members’ relevant publicly-available documents. | GAO-26-107338

The U.S. key components include additional precautions for specified high-risk agents—such as Ebola virus—and research. Guidance documents from Australia, Canada, and China included comparable language to most of the additional precautions GAO identified for U.S. key components of biosafety and biosecurity.

National guidance documents addressing biosafety and biosecurity are important, but other factors might also influence a G20 member's biosafety and biosecurity. For example, Australian officials told GAO that state and territory governments play a role in managing biosecurity, such as responding to animal disease outbreaks.

Table 1: U.S. Biosafety Level Definitions

Biosafety level	Description	Sample precaution: safety equipment and standard practices
1	Containment appropriate for well-characterized biological agents that are not known to consistently cause disease in healthy adults.	Lab coats, gloves, eye protection. Work is performed on a lab bench.
2	Containment appropriate for moderate-risk biological agents that may cause human disease if accidentally inhaled, swallowed, or exposed to the skin.	Uses all precautions above, and any procedures that can cause aerosols or splashes are performed in a biological safety cabinet.
3	Containment appropriate for biological agents that may be transmitted through the air and cause potentially lethal disease.	Uses all precautions above, and researchers may be required to wear respirators. All work is performed in a biological safety cabinet.
4	Containment appropriate for biological agents that pose a high risk of transmission through the air and may cause life-threatening disease for which no vaccines or treatments are available.	Uses all precautions above, but researchers may be required to wear a full body protective suit. Labs are airtight and exhaust air is filtered before being released from the lab.

Source: GAO summary of U.S. Department of Health and Human Services (HHS), Centers for Disease Control and Prevention and National Institutes of Health, Biosafety in Microbiological and Biomedical Laboratories 6th Edition (Bethesda, MD, and Atlanta, GA: revised June 2020) and U.S. HHS, Administration for Strategic Preparedness & Response, Biosafety Level Requirements, <https://aspr.hhs.gov/S3/Pages/Biosafety-Level-Requirements.aspx>. Accessed June 18, 2025. | GAO-26-107338

Table 2: Key Components of U.S. Biosafety and Biosecurity for All Biological Agents and Research

1. Risk Assessments

- Before any research project starts, institutions should conduct a risk assessment to identify the hazardous characteristics of an agent or toxin, activities that may result in human exposure, likelihood that exposure will cause an infection, and probable consequences of an infection.^{a,b}
- Institutions should use risk assessments to select appropriate mitigations, including the application of biosafety levels and good microbiological practices, safety equipment, and facility safeguards that can help prevent laboratory-associated exposures and infections.
- Qualified individuals, such as biosafety professionals or subject matter experts, and institutional review entities, should review risk assessments, and institutions should regularly update risk management strategies to address evolving risks.

2. Biosafety Program

- Institutions should develop and implement a biosafety program that identifies hazards and specifies mitigation strategies to eliminate or reduce the likelihood of exposures and unintentional releases of hazardous materials, including appropriate decontamination methods, good microbiological practices and procedures, and personal protective equipment.
- Institutions should develop the biosafety plan in consultation with the facility director and safety professionals, and the plan should be available, accessible, and periodically reviewed and updated as necessary.
- Biosafety programs should incorporate various control and containment measures, including infrastructure design, access restrictions, personnel training, containment equipment, and safe methods for managing infectious material.

3. Biosecurity Program

- Institutions should conduct a site-specific risk assessment and analyze the probability and consequences of loss, theft, and potential misuse of materials, technology, or information. Institutions should use this risk assessment to inform their biosecurity program and routinely review and revise the risk assessment and program, including following any laboratory biosecurity-related incident.
- Laboratory biosecurity programs should include procedures for personnel vetting, personnel reliability evaluations, violence prevention programs, laboratory biosecurity training, dual use research oversight, cybersecurity standards, material and facility control, and accountability standards.

To learn more: <https://www.gao.gov/assets/gao-26-107338.pdf>



Number 8

[Codex Security: now in research preview](#)

OpenAI

Today we're introducing Codex Security, our application security agent. It builds deep context about your project to identify complex vulnerabilities that other agentic tools miss, surfacing higher-confidence findings with fixes that meaningfully improve the security of your system while sparing you from the noise of insignificant bugs.

Context is essential when evaluating real security risks, but most AI security tools simply flag low-impact findings and false positives, forcing security teams to spend significant time on triage.

At the same time, agents are accelerating software development, making security review an increasingly critical bottleneck. Codex Security addresses both challenges.

By combining agentic reasoning from our frontier models with automated validation, it delivers high-confidence findings and actionable fixes so teams can focus on the vulnerabilities that matter and ship secure code faster.

Formerly known as Aardvark, Codex Security began last year as a private beta with a small group of customers. In early internal deployments, it surfaced a real SSRF, a critical cross-tenant authentication vulnerability, and many other issues which our security team patched within hours.

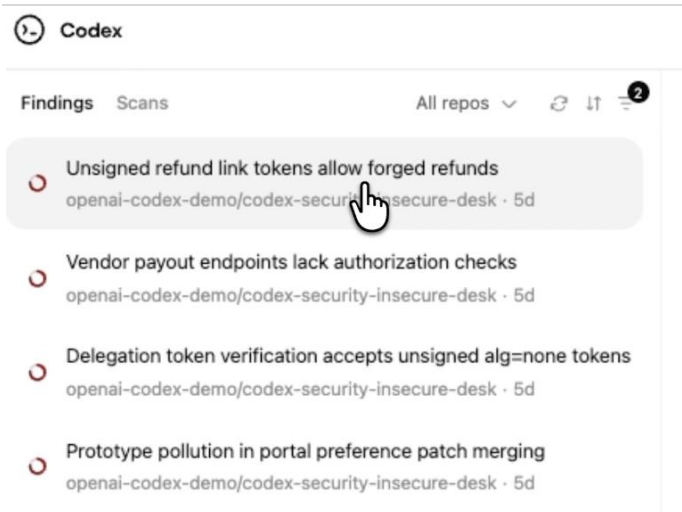
Early deployments with external testers helped us improve how users provide relevant product context and move from onboarding to securing their code.

We also significantly improved the quality of our findings over the course of the beta: scans on the same repositories over time show increasing precision, in one case cutting noise by 84% since initial rollout.

We've reduced the rate of findings with over-reported severity by more than 90%, and false positive rates on detections have fallen by more than 50% across all repositories.

These improvements help Codex Security better align reported severity with real-world risk and reduce unnecessary triage burden for security teams, and we expect the signal-to-noise ratio to continue to improve.

Starting today, Codex Security is rolling out in research preview to ChatGPT Pro, Enterprise, Business, and Edu customers via Codex web with free usage for the next month.



Codex Security leverages OpenAI’s frontier models and the Codex agent. It can reduce noise and accelerate remediation by grounding vulnerability discovery, validation, and patching in system-specific context.

- **Build system context and create an editable threat model:** After configuring a scan, it analyzes your repository to understand the security-relevant structure of the system and generates a project-specific threat model that can capture what the system does, what it trusts, and where it is most exposed. Threat models can be edited to keep the agent aligned with your team.
- **Prioritize and validate issues:** Using the threat model as context, it searches for vulnerabilities and categorizes findings based on expected real-world impact in your system. Where possible, it pressure-tests findings in sandboxed validation environments to distinguish signal from noise. Users can see this analysis in the validated findings.

When Codex Security is configured with an environment tailored to your project, it can validate potential issues directly in the context of the running system. That deeper validation can reduce false positives even further and enable the creation of working proof-of-concepts, giving security teams stronger evidence and a clearer path to remediation.

- **Patch issues with full system context:** Finally, Codex Security proposes fixes to the discovered issues that align with system intent and surrounding behavior. This enables patches that can improve security while minimizing regressions, making them safer to review and land. Users can filter the findings so they stay focused on what matters most to their team and has the highest security impact.

Codex Security can also learn from your feedback over time to improve the quality of its findings. When you adjust the criticality of a finding, it can use that feedback to refine the threat model and improve precision on subsequent runs as it learns what matters in your architecture and risk posture.

It's designed to operate at scale and surface the highest-confidence findings with easy-to-accept patches. Over the last 30 days, Codex Security scanned more than 1.2 million commits across external repositories in our beta cohort, identifying 792 critical findings and 10,561 high-severity findings.

Critical issues appeared in under 0.1% of scanned commits, showing that the system can identify security impacting issues in large volumes of code while minimizing noise to reviewers.

To learn more:

<https://openai.com/index/codex-security-now-in-research-preview/>



Number 9

Meta Takes Legal Action Against Scam Advertisers



Takeaways

- Today, we're taking legal action to combat scams on our platforms, which includes filing multiple lawsuits against deceptive advertisers in Brazil and China that used celeb-bait and a Vietnam-based advertiser who used cloaking and led a subscription fraud scheme.
- We also issued cease and desist letters to eight marketing consultants who advertised the ability to evade our enforcement systems.
- We continue to invest in new AI technology that detects cloaking, a technique that circumvents our review processes and shows content to people that violates our policies.

We work aggressively to find and disrupt scams, on and off our platforms. Recently, we worked closely with law enforcement in the UK and Nigeria to help take down a scam center, which resulted in seven arrests. And today, we filed lawsuits against four scam advertisers who impersonated well-known celebrities and brands to deceive and defraud people.

META

Meta Works With the UK National Crime Agency and the Nigerian Police Force to Disrupt Alleged Online Scams Centre in Nigeria

We've taken technical enforcement actions against these scammers, which includes suspending their methods of payment, disabling related accounts on our platforms, blocking the domain names for websites they used for their scams, and sharing this information with our industry partners so they can block them, too.

Today's lawsuits and our ongoing efforts to combat scams send a clear message: those who seek to exploit others on our platforms will be held accountable.

Fighting Celeb-Bait Scams in Brazil and China

Scammers often misuse the images of public figures, such as celebrities and content creators, to trick people into engaging with ads that lead to scam websites.

These sites commonly ask people to share their personal information or send money.

Of course, celebrities are featured in many legitimate ads. But because scam ads are designed to look real, they're not always easy to detect. This scheme, referred to as 'celeb bait,' undermines people's trust and violates our policies.

To fight celeb-bait scams, we developed protections for celebrities whose images are repeatedly used in these schemes. This program currently protects the images of more than 500,000 celebrities and public figures around the world.

Exposing Subscription Fraud and Cloaking

We're improving our methods for detecting cloaking, a malicious technique that impairs ad review systems by concealing the true nature of a website linked to an ad. In instances like this, a webpage connected to a seemingly legitimate ad displays one version of its content to our ad review system, but shows different content to real users. We block and remove these ads when we detect them, and we share them with our partners so they can take action on their platforms as well.

Our latest tools use AI to help us analyze cloaking and better detect ads that redirect to harmful websites. These tools also help us more quickly reject these ads, and we can more swiftly take action when users report suspected malicious ads.

698M

fake accounts removed from Facebook

135M

pieces of spam content removed from Facebook

Our Ongoing Approach to Stopping Fraud

We continue to improve our detection and enforcement methods and have developed a multi-layered approach to combating fraud, which includes using automated, technical defenses to help protect people on our apps; disrupting criminal scam networks; and strengthening cross-industry partnerships.

For more insights and practical tips to help recognize common scams online, please visit our Scam Prevention Hub.

Tips for staying safe online

- › [Stay safe on our technologies](#)
- › [Secure your account](#)
- › [Protect your personal information](#)
- › [WhatsApp security](#)
- › [Trust and safety on Marketplace](#)
- › [Support for compromised accounts on Facebook](#)
- › [Support for compromised accounts on Instagram](#)
- › [Support for compromised accounts on WhatsApp](#)

How to report scams

- › [Report on Facebook](#)
- › [Report on Facebook Marketplace](#)
- › [Report on Messenger](#)
- › [Report on Instagram](#)
- › [Report on WhatsApp](#)
- › [Scam Relief Resources](#)

To learn more:

<https://about.fb.com/news/2026/02/meta-takes-legal-action-against-scam-advertisers/>

<https://www.meta.com/safety/scam-prevention/>



Number 10

Luring users into running trojanized gaming utilities

Microsoft Threat Intelligence 🇺🇸

@MsftSecIntel

We are Microsoft's global network of security experts. Follow for security research and threat intelligence.

Microsoft Defender researchers uncovered a campaign that lured users into running trojanized gaming utilities distributed through browsers and chat platforms, leading to the deployment of a remote access trojan (RAT).

A malicious downloader staged a portable Java runtime and executed a malicious Java archive (JAR) file named jd-gui.jar. This downloader used PowerShell and living-off-the-land binaries (LOLBins) like cmstp.exe for stealthy execution. It evaded detection by deleting the initial downloader and by adding Microsoft Defender exclusions for the RAT components. It also added persistence using a scheduled task and startup script named world.vbs. Finally, it deployed the final payload, a multi-purpose malware that acted as loader, runner, downloader, and RAT.

The RAT connected to the IP address 79.110.49[.]15 for command and control (C2), enabling threat actors to perform various actions like data theft and additional payload deployment.

To learn more:

<https://x.com/MsftSecIntel/status/2027070355487997998>



Disclaimer

Despite the great care taken to prepare this newsletter, we cannot guarantee that all information is current or accurate. If errors are brought to our attention, we will try to correct them, and we will publish the correct information to the LinkedIn pages of the Association.

Readers will make their own determination of how suitable the information is for their usage and intent. 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 on this newsletter, or our web sites.

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.

This information:

- is of a general nature only and is not intended to address the specific circumstances of any particular individual or entity;
- should not be relied on in the particular context of enforcement or similar regulatory action;
- is not necessarily comprehensive, complete, or up to date;
- is sometimes linked to external sites over which the association has no control and for which the association assumes no responsibility;
- is not professional or legal advice (if you need specific advice, you should always consult a suitably qualified professional);
- is in no way constitutive of interpretative;
- does not prejudice 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 prejudice the interpretation that the Courts might place on the matters at issue.

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

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.

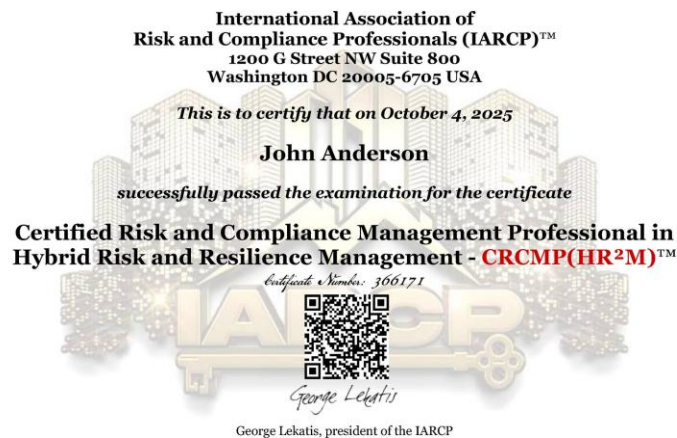
General Terms and Conditions for all visitors:

<https://www.risk-compliance-association.com/Privacy.htm>

2. Advanced Specialization, Certified Risk and Compliance Management Professional in Hybrid Risk and Resilience Management - CRCMP(HR²M), online training and certification program. You may visit: https://www.risk-compliance-association.com/CRCMP_HR2M.htm

The CRCMP(HR²M) program is designed to extend the capabilities of CRCMPs into the advanced domains of hybrid risk and resilience. This advanced specialization:

1. Moves from traditional risk and compliance frameworks into the management of multi-vector, cross-domain, and asymmetric threats that transcend conventional boundaries.
2. Develops expertise in hybrid risk governance.
3. Equips with the skills to design cross-sector resilience strategies, integrate governance across silos, and align risk frameworks with organizational, regulatory, and geopolitical realities.
4. Provides practical methodologies for hybrid stress testing, assisting organizations to withstand hybrid risks.
5. Advances the careers of CRCMPs by adding specialized expertise in hybrid risk and resilience, and offering strategic, cross-sector perspectives that are highly valued by organizations and boards.



Enrollment in the CRCMP(HR²M) program is restricted to professionals who have already passed the Certified Risk and Compliance Management Professional (CRCMP) exam.

To preserve the credibility and value of this credential, the association does not allow substitutions, equivalency credits, or waivers of any kind. The curriculum assumes mastery of the CRCMP body of knowledge.

3. Certified Information Systems Risk and Compliance Professional (CISRPC), distance learning and online certification program.

You may visit:

https://www.risk-compliance-association.com/CISRPC_Distance_Learning_and_Certification.htm

Certified Information Systems Risk and Compliance Professional (CISRPC), distance learning and online certification program

Overview

One of the most common (and costly) mistakes organizations make in the areas of risk management, compliance, IT, information security, and privacy, is relying solely on expert opinions that are **not grounded** in relevant laws and regulations. While professional expertise and technical insight are essential, they must be aligned with the legal and regulatory frameworks that govern these domains.

Without this alignment, organizations risk exposure to significant legal, financial, and reputational damage. For example, implementing information security controls based only on best practices, without accounting for legal requirements, can leave critical compliance gaps. Using risk management frameworks without tailoring them to specific regulatory requirements leaves organizations exposed to risk and compliance challenges.

4. Certified Cyber (Governance Risk and Compliance) Professional CC(GRC)P, distance learning and online certification program. You may visit: https://www.risk-compliance-association.com/CC_GRC_P_Distance_Learning_and_Certification.htm

Certified Cyber (Governance Risk and Compliance) Professional - CC(GRC)P, distance learning and online certification program

Overview

There are still companies and organisations that consider cyber risk a technical risk. But even the most advanced organizations must adapt and build their risk management framework on the foundation that we now operate in a fundamentally different world, one where cyber risk is a core component of hybrid risk. The old mindset is dangerously outdated. Today, cyber operations are embedded in economic warfare, political conflict, supply chain disruption, and military strategy. Cyber risk today is not just about protecting networks, it's about protecting societies from hybrid threats.

A hybrid risk management framework should identify primary cyber threats, map their cascading effects on financial, legal, and business operations, and develop cross-functional response strategies.

5. Certified Risk and Compliance Management Professional in Insurance and Reinsurance CRCMP(Re)I, distance learning and online certification program. You may visit: [https://www.risk-compliance-association.com/CRCMP Re I.htm](https://www.risk-compliance-association.com/CRCMP_Re_I.htm)

Certified Risk and Compliance Management Professional in Insurance and Reinsurance - CRCMP(Re)I, distance learning and online certification program

Overview

In the aftermath of the global financial crisis of 2007–2009, and more recently the COVID-19 pandemic and the macroeconomic shocks triggered by inflation, geopolitical tensions, and climate-related events, the insurance and reinsurance sectors have faced escalating pressure to adapt to increasingly complex, interconnected, and systemic risks that challenge traditional risk models. These crises revealed not only the extraordinary complexity of risk exposures in the industry, but also the gaps in risk comprehension, governance, and compliance preparedness.

Mispriced risk, regulatory blind spots, and insufficient oversight contributed significantly to systemic instability. For insurers and reinsurers, the stakes remain immense. These firms serve as financial shock absorbers across society, and when their risk frameworks falter, the consequences ripple across markets, governments, and policyholders alike.

6. Travel Security Trained Professional (TSecTPro), distance learning and online certification program. You may visit: [https://www.risk-compliance-association.com/TSecTPro Distance Learning and Certification.htm](https://www.risk-compliance-association.com/TSecTPro_Distance_Learning_and_Certification.htm)

Travel Security Trained Professional (TSecTPro), distance learning and online certification program

Overview

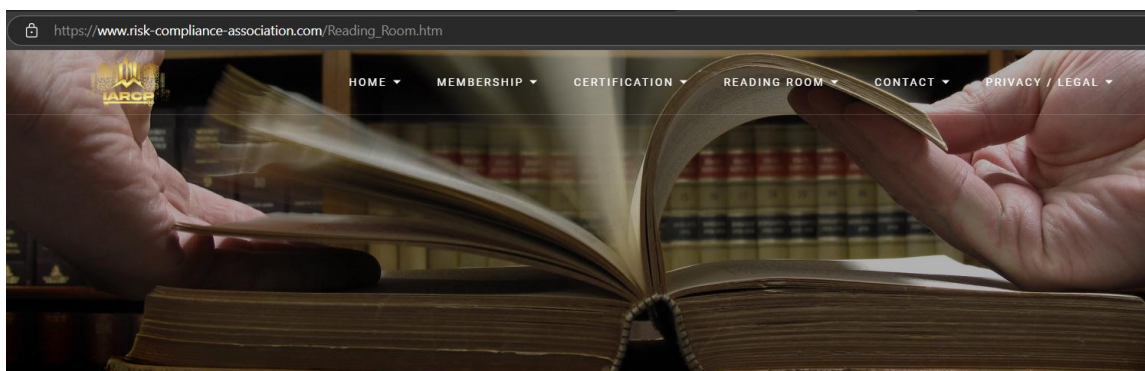
Professionals love international travel. For so many board members, senior executives, managers and employees, business travel taken for work purposes is also an opportunity for pleasure and satisfaction. It is about visiting new places, meeting new people, eating delicious food, having fun. For many, emotional or physical intimate relationships play a central role in the overall travel experience.

Intimacy refers to the closeness and connection – from intellectual intimacy (sharing thoughts, ideas, and professional experience) to emotional and sexual intimacy.

Travelers hate to think that travel also means increased risk, health challenges, legal uncertainty, and new unique threats. They often do not understand (or prefer to ignore) what it means to become subjects to the laws and the legal system of the countries they are visiting.

Our reading room:

https://www.risk-compliance-association.com/Reading_Room.htm



Reading Room, International Association of Risk and Compliance Professionals (IARCP)

Welcome to the Top 10 risk and compliance management news stories and world events that, for better or worse, defined this week's agenda – and a look ahead at what's coming next. This is the newsletter from the International Association of Risk and Compliance Professionals (IARCP).

You may contact:

Lyn Spooner

Email: lyn@risk-compliance-association.com

George Lekatis

President of the IARCP

1200 G Street NW, Suite 800

Washington, DC 20005, USA

Tel: (202) 449-9750

Email: lekatis@risk-compliance-association.com

Web: www.risk-compliance-association.com

HQ: 1220 N. Market Street Suite 804,

Wilmington, DE 19801, USA

Tel: (302) 342-8828

