International Association of Potential, New and Sitting Members
of the Board of Directors (IAMBD)
1200 G Street NW Suite 800, Washington DC, 20005-6705 USA
Tel: 202-449-9750 Web: www.iambd.org

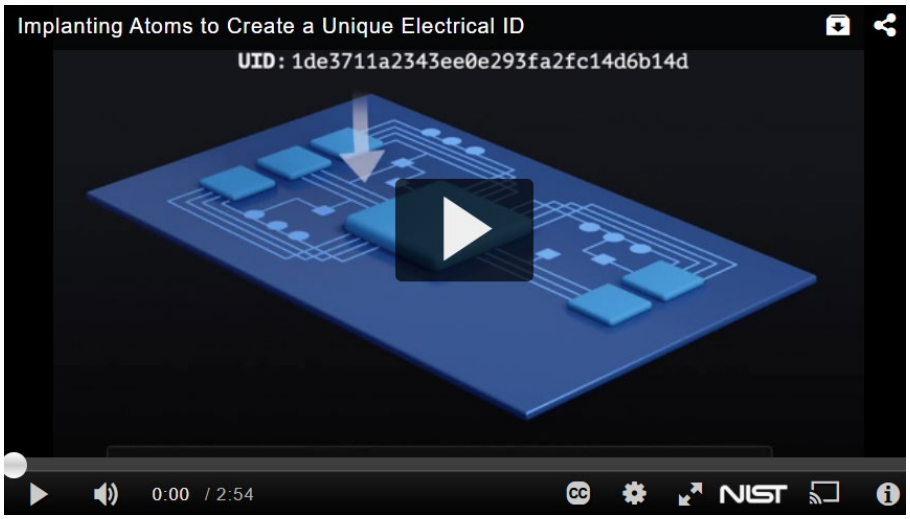
News for the Board of Directors, October 2021

Dear members and friends,

According to the National Institute of Standards and Technology (NIST), if someone sells you a luxury handbag from Paris, France, but it turns out be a forgery from Paris, Texas, the counterfeit item might cost you a thousand bucks and the crook could wind up in jail. But if a counterfeit electronic device gets installed in a car, it could cost passengers or the driver their lives.

Without new security measures, the interconnected wireless technologies, digital electronics and micromechanical electronic systems that make up the Internet of Things are vulnerable to forgeries and tampering that could cause entire telecommunication networks to fail. In 2017, sales of counterfeit products of all sorts — from electronics to pharmaceuticals — amounted to an estimated $1.2 trillion worldwide.

To help prevent counterfeit computer chips and other electronic devices from flooding the market, researchers at the National Institute of Standards and Technology (NIST) have demonstrated a method that could electronically authenticate products before they leave the factory.



The video:
https://cdnapisec.kaltura.com/index.php/extwidget/preview/partner_id/684682/uiconf_id/31013851/entry_id/1_kv68s3z0/embed/dynamic

To detect the presence of forged components in a system, you need a way of uniquely identifying and authenticating these components throughout the supply chain.

To achieve this, NIST researchers have developed a new low-cost process for creating unique and non-duplicable ID tags by altering the electronic structure of silicon.

These tags could be embedded into a device during the manufacturing process and easily authenticated by anyone receiving the device, ensuring a secure supply chain for components in critical systems. Credit: Sean Kelley/NIST.

The scientists employed a well-known technique called doping, in which small clusters of “foreign” atoms of a different element from those in the device to be labeled are implanted just beneath the surface.

The implanted atoms alter the electrical properties of the topmost layer without harming it, creating a unique label that can be read by an electronic scanner.

Using doping to create electronic tags for devices is not a new idea. However, the NIST technique, which uses the sharp tip of an atomic force microscope (AFM) probe to implant atoms, is simpler, less costly and

requires less equipment than other doping techniques using lasers or a beam of ions, said NIST researcher Yaw Obeng. It is also less damaging than other methods.

“We’re putting a sticker on every device, except that the sticker is electronic and no two are identical because in each case the amount and pattern of the dopant atoms is different,” said Obeng.

To create the electronic ID, Obeng and his colleagues first deposited a 10-nanometer (billionth of a meter) film of dopant material — in this case aluminum atoms — about 10-centimeter-square silicon wafers that were then broken into postage-stamp-size fragments so that they could fit in the AFM.

The team then used the needle-like tip of the AFM probe to push aluminum atoms a few nanometers into the silicon fragments. The diameter of the implanted regions was tiny, no larger than 200 nm.

The implanted atoms alter the arrangement of silicon atoms just beneath the surface of the wafer.

These silicon atoms, as well as those that reside throughout the wafer, are arranged in a repeating geometric pattern known as a lattice.
Each silicon lattice acts like an electrical circuit with a certain impedance, the AC (alternating current) equivalent of resistance in a DC (direct current) circuit.

When the implanted aluminum atoms were rapidly heated to about 600 degrees Celsius, a few of them acquired enough energy to replace some of the silicon in lattices just beneath the wafer’s surface. The random substitution altered the impedance of those lattices.

Each dopant-modified lattice has a unique impedance depending on the amount and type of dopant. As a result, the lattice can serve as a distinctive electronic label — a nanometer-scale version of a QR code for the wafer, Obeng said.

When a scanner directs a beam of radio waves at the device, the electrically altered lattices respond by emitting a unique radio frequency corresponding to their impedance. Counterfeit devices could be easily identified because they would not respond to the scanner in the same way.

“This research is key because it offers a means to uniquely identify components by a secure, unalterable and inexpensive means,” said Jon Boyens, a researcher with NIST’s Computer Security Division who was not a co-author of the study.

The study, which Obeng presented on Sept. 16 at the International Conference on IC Design and Technology in Dresden, Germany, builds upon earlier work by the same team (https://aip.scitation.org/doi/abs/10.1063/1.5065385?journalCode=jap).

The new study refines the AFM method for inserting dopant atoms, so that the AFM probe can more precisely place the atoms in the silicon wafer. The higher precision will make it easier to test the electronic ID system under real-life conditions.

Obeng and his collaborators, who include Joseph Kopanski of NIST and Jung-Joon Ahn of NIST and George Washington University in Washington, D.C., consider their technique a prototype that will need modification before it can be used in mass production.

One possibility is to use the sharp probes of several AFMs working side by side so that the dopant material could be implanted in many devices at once.

Another strategy would employ high-pressure rollers to rapidly push dopant atoms coating a computer chip or other device a few nanometers into the device.

A pattern stenciled onto the rollers would ensure that the dopant atoms were implanted according to a precise blueprint. Rollers are widely used to smooth paper, textiles and plastics.

To read more: https://www.nist.gov/news-events/news/2021/09/smart-use-doping-implanted-atoms-create-unique-electrical-ids-distinguish

PCAOB Solicits Additional Public Comment on Proposed New Requirements for Lead Auditor's Use of Other Auditors

The Public Company Accounting Oversight Board (PCAOB) issued a second supplemental request for comment on its proposal to strengthen requirements that apply to audits involving multiple audit firms. The comment period runs through **November 30, 2021.**

You may visit: https://pcaob-assets.azureedge.net/pcaob-dev/docs/default-source/rulemaking/docket042/2021-005-other-auditors-ssrc.pdf?sfvrsn=6000f093_4

In many audits, the lead auditor issues the auditor's report, but other auditors perform important audit work to assist the lead auditor in obtaining sufficient appropriate audit evidence in support of the lead auditor's opinion(s).

The roles of other auditors have become more significant and have evolved as companies' global operations have grown.

Working with other auditors can differ from working with people in the same audit firm, creating challenges in coordination and communication.

These challenges can lead to misunderstandings about the nature, timing, and extent of the other auditors' work and can detract from the quality of the audit.

To address the challenges of working with other auditors, the PCAOB previously issued a proposal to strengthen requirements regarding a lead auditor's responsibilities for planning, supervising, and evaluating the work of other auditors.

The stated aim of the proposal has been to increase the lead auditor's supervision of the work of other auditors and to enhance the lead auditor's ability to prevent or detect deficiencies in the other auditors' work.

The PCAOB sought additional comment on that proposal in September 2017. Today's request for comment seeks further input on certain revisions to the initial proposal that are designed to improve the approach.

"It is important for investor protection that the lead auditor sufficiently plans, supervises, and evaluates the work of other auditors," said PCAOB Acting Chairperson Duane M. DesParte. "With the supplemental request

for comment we issue today, we look forward to receiving further stakeholder input as we move to strengthen existing requirements."

TABLE OF CONTENTS

Since it last solicited public comment on this proposal in 2017, the PCAOB has continued to review the work performed in audits that involve other auditors and to engage with stakeholders and other auditing standard setters in this area.

Today's proposed amendments are intended to:

(1) adjust certain requirements to better take into account the lead auditor's role in the audit and

(2) improve the readability and usability of the amendments and facilitate their implementation.

The public is encouraged to comment on the revisions proposed in the release or on any other aspect of the proposed amendments. After this round of public comment, the Board intends to consider the comments received and decide whether to adopt final amendments.

Learn more at the Supervision of Audits Involving Other Auditors project page at: https://pcaobus.org/oversight/standards/research-standard-setting-projects/supervision-of-audits-involving-other-auditors

To learn more, you may visit: https://pcaob-assets.azureedge.net/pcaob-dev/docs/default-source/rulemaking/docket042/2021-005-other-auditors-ssrc.pdf?sfvrsn=6000f093_4

ESMA to focus on supervision, sustainability, digitalisation and the Capital Markets Union in 2022

The European Securities and Markets Authority (ESMA), the EU's securities markets regulator, has published its 2022 Annual Work Programme (AWP), setting out its priority work areas for the next 12 months to deliver on its mission to enhance investor protection and promote stable and orderly financial markets.

The 2022 AWP has been developed at a time of significant change for ESMA with its new powers and responsibilities, growth in staff numbers and senior management changes.

The key areas of focus for 2022 include: the exercise of new, and existing, supervisory powers for benchmarks and data service providers (DRSPs) as well as central counterparties (CCPs); its contribution to the European Union (EU) priorities on the development of the Capital Markets Union (CMU), sustainable finance and innovation; and the convergence of supervisory and regulatory practices across the EU.

In addition, it will continue to monitor the impact of the United Kingdom's withdrawal from the EU on the evolution of EU and global capital markets.

Natasha Cazenave, Executive Director, said:

"ESMA faces another year of change and challenge in 2022, with new supervisory powers for benchmarks and data service providers, significant contributions expected to support the EU's priorities through single rulebook and supervisory convergence work and further enhancements to our role as an EU capital markets data hub.

"This is an ambitious work schedule that aims to respond to the challenges faced by the EU, its capital markets, and its citizens.

This includes developing the retail investor base to support the Capital Markets Union, promoting sustainable finance and long-term oriented markets, and dealing with the opportunities and risks posed by digitalisation and innovation in the financial sector."

2.4.1 Risk Monitoring and Analysis

Key objectives	Identify and assess financial market risks, report on these risks to the relevant institutions, and inform the public. Provide data, statistical and analytical basis for ESMA and NCA supervision, regulation, and convergence activities. Cooperate with EU and international bodies, including the ESRB, IOSCO and the FSB, to identify and assess financial stability and systemic risks. Identify opportunities and risks related to financial innovation, with particular attention to crypto asset market developments and risks. Systematically monitor trends and risks related to retail investor and ESG developments.

To read more:
https://www.esma.europa.eu/sites/default/files/library/esma20-95-1430_2022_annual_work_programme.pdf

SEC Highlights Investor Protection for World Investor Week 2021

The Securities and Exchange Commission has announced that it will highlight investor education and protection resources during World Investor Week 2021 (WIW). You may visit: https://www.investor.gov/additional-resources/spotlight/world-investor-week

This marks the fifth year of WIW, a global effort promoted by the International Organization of Securities Commissions (IOSCO) that brings together regulators on six continents to raise awareness about the importance of investor education and protection.

The SEC is once again serving as the national coordinator in the U.S. working with the U.S. Commodity Futures Trading Commission, Financial Industry Regulatory Authority, National Futures Association, and North American Securities Administrators Association.

Together with these organizations, the SEC's Office of Investor Education and Advocacy (OIEA) issued a joint Investor Bulletin today to promote WIW's key messages. You may visit: https://www.investor.gov/introduction-investing/general-resources/news-alerts/alerts-bulletins/investor-bulletins/key-topics

Investor education and protection resources are available at Investor.gov.

During WIW, SEC staff will host outreach events on the benefits of investing early, making informed investment decisions, creating an investment plan, and understanding the risks and fees associated with investments; conducting a background check on an investment professional; recognizing the power of compounding interest; and learning how to avoid fraud.

"Investor protection is at the core of the SEC's mission, and we are proud to serve as the national coordinator in the U.S. for World Investor Week," said SEC Chair Gary Gensler. "We especially hope to reach younger investors, first-time investors, and investors in underserved communities. As markets and technology evolve, more investors than ever are able to access our capital markets. I encourage investors at every stage to take advantage of resources available at Investor.gov and ongoing outreach events in communities across the country."

For the first time ever, Chair Gensler issued a WIW kick-off video underscoring the importance of this global initiative, and created a new "Office Hours with Chair Gensler" video about the basics of investing that will be published on his Twitter page on Wednesday.

Through his new "Office Hours" videos, Chair Gensler speaks directly and plainly to America's investors on timely topics, such as digital engagement, cryptocurrencies, climate risk disclosure, and risks involving investing in China and off-shore shell companies.

The SEC's World Investor Week page highlights a "Term of the Day" along with corresponding video clip with definitions about microcap stocks, day trading, ESG (environmental, social, governance) investing, fractional shares, margin accounts, special purpose acquisition companies (SPACs), and index funds.

On the same webpage, investors can access an investing quiz to test their knowledge of the "Term of the Day" and other key messages and themes from WIW. In addition, staff will highlight the importance of thoroughly researching and understanding the risks of online investing and investing in digital assets.

"Knowledge is power, and the best way to protect yourself is to learn investing basics, understand the risks involved with every investment opportunity, and create a long-term plan that best meets your financial goals," said Lori Schock, Director of the SEC's Office of Investor Education and Advocacy. "It's especially important for first-time investors to take advantage of the online resources on Investor.gov. It's a great first step toward protecting your money and learning how to build a smart saving and investing plan for your financial future."

For WIW, Ms. Schock posted a new Director's Take article, "Taking Stock in Teen Trading." that speaks directly to parents and teens about the importance of forming a parent/teen investment partnership early on. In the article, she discusses topics such as teen trading accounts, social media influence, and apps.

Through her Director's Take articles, Ms. Schock provides investors with helpful information on timely topics.

SEC staff WIW outreach events include:

- Saving and investing presentations and webinars for diverse communities nationwide, libraries, students, teachers, seniors, and military service members;

- Presentations to college students, including an event with students from Historically Black Colleges and Universities (HBCUs) in which students will be able to ask questions of Chair Gensler;

- A Facebook Live event with AARP;

- Radio interview with Lori Schock on topics important to seniors; and

- Thrift Savings Plan (TSP) program for federal employees.

To see a list of other SEC outreach activities or learn more about WIW, please visit the SEC's World Investor Week page at: https://www.investor.gov/additional-resources/spotlight/world-investor-week

Investor.gov
U.S. SECURITIES AND EXCHANGE COMMISSION

Deputy Attorney General Lisa O. Monaco Announces New Civil Cyber-Fraud Initiative

Deputy Attorney General Lisa O. Monaco announced the launch of the department's *Civil Cyber-Fraud Initiative*, which will combine the department's expertise in civil fraud enforcement, government procurement and cybersecurity to combat new and emerging cyber threats to the security of sensitive information and critical systems.

"For too long, companies have chosen silence under the mistaken belief that it is less risky to hide a breach than to bring it forward and to report it," said Deputy Attorney General Monaco.

"Well that changes today. We are announcing today that we will use our civil enforcement tools to pursue companies, those who are government contractors who receive federal funds, when they fail to follow required cybersecurity standards — because we know that puts all of us at risk. This is a tool that we have to ensure that taxpayer dollars are used appropriately and guard the public fisc and public trust."

The creation of the Initiative, which will be led by the Civil Division's Commercial Litigation Branch, Fraud Section, is a direct result of the department's ongoing comprehensive cyber review, ordered by Deputy Attorney General Monaco this past May.

The review is aimed at developing actionable recommendations to enhance and expand the Justice Department's efforts against cyber threats.

Civil Cyber-Fraud Initiative Details

The Civil Cyber-Fraud Initiative will utilize the False Claims Act to pursue cybersecurity related fraud by government contractors and grant recipients.

The False Claims Act is the government's primary civil tool to redress false claims for federal funds and property involving government programs and operations.

The act includes a unique *whistleblower* provision, which allows private parties to assist the government in identifying and pursing fraudulent conduct and to share in any recovery and protects whistleblowers who bring these violations and failures from retaliation.

The initiative will hold accountable entities or individuals that put U.S. information or systems at risk by knowingly providing deficient

cybersecurity products or services, knowingly misrepresenting their cybersecurity practices or protocols, or knowingly violating obligations to monitor and report cybersecurity incidents and breaches.

The benefits of the initiative will include:

- Building broad resiliency against cybersecurity intrusions across the government, the public sector and key industry partners.

- Holding contractors and grantees to their commitments to protect government information and infrastructure.

- Supporting government experts' efforts to timely identify, create and publicize patches for vulnerabilities in commonly-used information technology products and services.

- Ensuring that companies that follow the rules and invest in meeting cybersecurity requirements are not at a competitive disadvantage.

- Reimbursing the government and the taxpayers for the losses incurred when companies fail to satisfy their cybersecurity obligations.

- Improving overall cybersecurity practices that will benefit the government, private users and the American public.

The department will work closely on the Initiative with other federal agencies, subject matter experts and its law enforcement partners throughout the government.

Report Cyber-Fraud

Tips and complaints from all sources about potential cyber-related fraud, waste, abuse and mismanagement can be reported by accessing the webpage of the Civil Division's Fraud Section, which can be found at: https://www.justice.gov/civil/report-fraud

Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements

Progress Report on the implementation of the FSB High-Level Recommendations

FSB FINANCIAL STABILITY BOARD

Executive summary

This report provides a status update on progress made on the implementation of the FSB high-level recommendations for Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements.

It discusses key market and regulatory developments since the publication of the FSB high-level recommendations in October 2020; takes stock of the implementation of the FSB high-level recommendations across jurisdictions; describes the status of the review of the existing standard-setting body (SSB) frameworks, standards, guidelines and principles in light of the FSB high-level recommendations; and identifies areas for consideration of potential further international work.

While the current generation so-called stablecoins are not being used for mainstream payments on a significant scale, vulnerabilities in this space have continued to grow over the course of 2020-21.

At present, stablecoins are being used primarily as bridge between traditional fiat currencies and other crypto-assets, which in turn are primarily held and traded for speculative purposes.

Increased participation by retail investors could give rise to broader financial stability issues through an erosion of trust in the financial system.

In the event that a stablecoin does enter the mainstream of the financial system as a means of payment and/or a store of value in multiple jurisdictions, with the potential to achieve substantial volume, it could become a global stablecoin (GSC).

The emergence of GSCs would pose greater risks to financial stability than existing stablecoins and may challenge the comprehensiveness and effectiveness of existing regulatory, supervisory and oversight approaches.

Ensuring appropriate regulation, supervision and oversight across sectors and jurisdictions will therefore be necessary to prevent any potential gaps and avoid regulatory arbitrage.
Overall, the implementation of the FSB high-level recommendations across jurisdictions is still at an early stage.

In the first half of 2021, the FSB conducted a comprehensive stock-take of the implementation of the FSB high-level recommendations on the regulation, supervision, and oversight of so-called “global stablecoin” arrangements of October 2020.

48 jurisdictions in the FSB and its Regional Consultative Groups (RCGs) participated in the stock-take covering 21 advanced economies and 27 emerging markets and developing economies.

Several jurisdictions have been reviewing and updating their legal and regulatory regimes to address specific risks arising from the emergence of stablecoins.

Jurisdictions have taken or are considering different approaches towards implementing the high-level recommendations.

As the stablecoin landscape is evolving rapidly and as regulatory and supervisory policies are being developed, the differences among regulatory approaches and classifications could be increasing.

For example, certain jurisdictions are seeking to implement the recommendations through the adoption of new rules and regulations, while others have amended or plan to amend existing rules and regulations in such a way that these are applicable to stablecoins.

Other jurisdictions have relied largely on existing regulatory, supervisory and oversight regimes to address the risks associated with stablecoins or with entities that are part of the stablecoin arrangement.

Differing regulatory classifications and approaches to stablecoins at jurisdictional level could give rise to the risk of regulatory arbitrage and harmful market fragmentation.

Standard-setting bodies are continuing to assess whether and how existing international standards may apply to stablecoin arrangements and, where appropriate, adjust their standards in light of the FSB high-level recommendations.

However, a number of issues may not be fully covered by ongoing work.

Authorities should rely on existing standards and principles relevant to the supervision and oversight of GSC arrangements, where they perform the same economic function as existing regulated activities covered by these standards. Any gaps in existing standards and principles should be addressed holistically and in a manner that is coordinated across sectors.

The FSB high-level recommendations complement the international standards and principles and should inform any potential updates to international sectoral standards and principles.

As jurisdictions are using the FSB high-level recommendations in developing their own domestic regulatory approaches, authorities have identified several issues relating to the implementation of the recommendations that may warrant further consideration and where further work at international level could be useful.

Areas for further consideration that respondents to the stock-take identified as most useful include conditions for qualifying a stablecoin as a GSC; prudential, investor protection, and other requirements for issuers, custodians, and providers of other GSC functions (e.g., wallet providers); redemption rights; cross-border and cross-sectoral cooperation and coordination; and mutual recognition and deference.

Further work on these issues at international level may help to support the effective implementation of the FSB high-level recommendations at the jurisdictional level, to mitigate the risk of regulatory fragmentation and arbitrage, and to address risks to financial stability arising from GSCs.

Efforts by standard-setting bodies to review, and where appropriate adjust their standards can further promote international consistency and reduce the risk of arbitrage or regulatory underlaps. The work on fostering the soundness of GSCs is an integral part of the Roadmap for enhancing cross-border payments endorsed by the G20 in October 2020.

The Roadmap, which the FSB has developed in coordination with relevant international organisations and SSBs, calls for a review by the FSB, to be undertaken in consultation with other relevant SSBs and international organisations, of the FSB high-level recommendations.

This progress report and the underlying stock-takes, as well as ongoing and planned work from SSBs, will inform that review.

The FSB will continue to support the effective implementation of the FSB high-level recommendations and facilitate coordination among SSBs. Starting in January 2022, with an expected completion date of July 2023, the FSB will review, in consultation with other relevant SSBs and international organisations, the recommendations in the FSB report and how any gaps identified could be addressed by existing frameworks.

The FSB will update its recommendations, if needed.

To read more: https://www.fsb.org/wp-content/uploads/P071021.pdf

PLI Broker/Dealer Regulation and Enforcement 2021

Gurbir Grewal, Director, Division of Enforcement, Washington D.C.

Thank you for that introduction and for having me here today. At the Division of Enforcement, ensuring that broker-dealers and associated individuals follow our laws and regulations is critical to our mission, so it's only fitting that my first speech as Director is at this event.

While I just referred to it as "our mission" at the Division of Enforcement, what I'd like to talk to you about today is how we all share the responsibility to maintain market integrity and enhance public confidence in our securities markets. But first I must provide the disclaimer that my remarks today express my views, and do not necessarily reflect those of the Commission, the Commissioners, or other members of staff.

- SEC Charges Broker Who Defrauded Seniors Out of Almost $1 Million

- SEC Charges Ernst & Young, Three Audit Partners, and Former Public Company CAO with Audit Independence Misconduct

- SEC Charges Disbarred New York Attorney and Florida Attorney with Scheme to Create False Opinion Letters

- Merrill Lynch Admits to Misleading Customers about Trading Venues

- SEC Charges U.S. Congressman and Others With Insider Trading

These are not headlines from some bygone era of market participants behaving badly; these are all from cases the Commission has brought since 2018. In fact, here's one from just last week: "SEC Charges Investment Bank Compliance Analyst with Insider Trading in Parents' Accounts."

Nearly a dozen years ago, one of my predecessors held a press conference to announce charges against more than twenty defendants, including "Wall Street professionals, corporate insiders, analysts and lawyers," in a pair of alleged insider trading schemes.

In explaining the importance of the cases, Director Khuzami said: "There is a basic principle that governs our capital markets, and that is that there is one set of rules, and everyone is expected to play by that one set of rules. That principle gives investors confidence that the markets are fair."
He was right then, and his words remain true today: Enforcement is, in significant part, animated by the idea that we will pursue potential violations by any market participant, and, in so doing, attempt to shape the behavior of all participants going forward.

But I believe more is required. Because despite all of the strong enforcement actions the SEC has brought over the years and despite all the speeches that SEC Chairs, Commissioners, Enforcement Directors, and others have given at events like this one, the types of behavior described in the headlines I read to you persist, and as a result, a significant part of the public continues to feel that our markets are essentially a game that is rigged against them.

So rather than issue warnings about how aggressively we will pursue you or your clients if you misbehave—which we, of course, will—I want to invite each of you—the lawyers, counselors, and gatekeepers who have such influence over market behavior—to join me.

By working together, we can dispel the notion that the deck is stacked in favor of the few and powerful, promote better conduct among market participants, and ensure that the markets work fairly for all. This, after all, should be our shared mission.

I see three key steps towards achieving this mission, and the first starts with each of you. In a speech he gave in May, Chair Gensler said: "[I]f you're asking a lawyer, accountant, or adviser if something is over the line, maybe it is time to step back from the line. Remember that going right up to the edge of a rule or searching for some ambiguity in the text or a footnote may not be consistent with the law and its purpose." This is a critical point and let me explain why.

This morning you heard discussions on a number of topics, including SPACs, ESG investments, and Regulation Best Interest, or "Reg BI". I defer to your able presenters as to the best substantive takeaways from each of those sessions.

But what you should not take away from them is that, if regulators are particularly focused on issues "X" or "Y" in a given area, that means you or your clients may be able to push the envelope on issue "Z" – or the grey areas around X or Y. That approach is a surefire way to foster misconduct and, potentially, lead to an enforcement action.

You should be thinking, instead, about modeling excellence in your compliance efforts, as you do in your performance. This means that firms need to think rigorously about how their specific business models and products interact with both emerging risks and Enforcement priorities, and tailor their compliance practices and policies accordingly.

For example, with respect to Reg BI, firms should recognize that the new regime draws upon key fiduciary principles, and is intended to enhance previous broker-dealer standards of conduct significantly beyond the suitability obligation.

Armed with this recognition, firms should then give their registered representatives the tools and information that will enable them to identify, disclose, and mitigate conflicts prohibited under Reg BI.

Let me be clear here: I am talking about more than putting together a stock policy and giving a check-the-box training. This requires proactive compliance, and this type of approach has never been more important than today— a time of rapid and profound technological change.

This change is exciting; it can help amplify the dynamism of our markets and increase access for investors. But at the same time it also creates new avenues for misconduct, and new responsibilities for compliance.

Recordkeeping violations may not grab the headlines, but the underlying obligations are essential to market integrity and enforcement. Take for example an enforcement action the Commission brought last year against a California broker-dealer for failing to preserve business-related text messages.

The SEC's order found that some of the firm's registered representatives used their personal devices when communicating with each other, with firm customers, and with other third parties concerning, among other things, the size of orders, the timing of trades, and the pricing of certain securities. These messages were potentially responsive to a records request SEC staff made to the firm in an unrelated investigation and the firm's failure to retain and produce them directly impacted that investigation.

Unfortunately, this is not an isolated example. We continue to see in multiple investigations instances where one party or firm that used off-channel communications has preserved and produced them, while the other has not. Not only do these failures delay and obstruct investigations, they raise broader accountability, integrity and spoliation issues.

A proactive compliance approach requires market participants to not wait for an enforcement action to put in place appropriate policies and procedures to preserve these communications and anticipate these emerging challenges.

Listen, many of these are not even new technological advances. After all, my 75 year-old mother has been texting my 13-year-old daughter for years, and I am certain many in this room have sent or received professional communications on personal devices or unofficial communications channels.

You need to be actively thinking about and addressing the many compliance issues raised by the increased use of personal devices, new

communications channels, and other technological developments like ephemeral apps.

Let me turn to the second part of our shared mission, which I'll call proactive enforcement. While this falls primarily on us, each of you have a role to play here as well.

I'm from Jersey, and I know a thing or two about the Turnpike, and the Garden State Parkway, and about enforcement of my State's laws, having served as a County Prosecutor and as Attorney General.

And one thing I know is that if you post a 65 mile-per-hour speed limit and don't enforce it, people drive 75. Not me, of course, but other people. And they eventually do so with a sense of impunity. And then after a while they will drive 80 or faster, with a growing sense of confidence.

As speeds climb higher and higher, you eventually have situations where accidents increase and heightened enforcement follows. But for all of the victims, it's too late.

It's a stark analogy, but the point is that we are not waiting for accidents to happen. We are trying to address emerging risks before they cause harm to investors. For example, this summer, the Commission brought enforcement actions against a SPAC, its sponsor, its CEO, the proposed merger target, and the target's founder and former CEO.

The SEC's settled order against everyone but the target's CEO found that the target had made misleading claims about its technology and about national security risks associated with its founder and former CEO, and that the SPAC had repeated those misstatements in public filings and failed its due diligence obligations to investors. By bringing this action prior to consummation of the merger, the Commission protected the SPAC's investors from potential harm.

A similarly forward-looking enforcement initiative this past summer involved the new requirement that firms file and deliver Client or Customer Relationship Summaries, known as "Forms CRS." A Form CRS is designed to help retail investors better understand the nature of their relationships with financial firms and individual professionals.

In July, the Commission brought enforcement actions against more than two dozen firms that had failed to timely file or to deliver their Forms CRS to their clients and customers.

As I said when we announced these cases, they "reinforce the importance of meeting [filing and disclosure] obligations and providing retail investors

with information that is intended to help them understand their relationships with their securities industry professionals."

Providing retail investors that essential information is the point of the Form CRS requirement, and we will continue to ensure that firms are satisfying their obligations to do so because that's what's required to prevent future investor harm.

You also have a key role to play in spotting and addressing emerging risks, and that's both by ensuring that your proactive compliance efforts continue even after violative conduct has occurred and by working with us in addressing that conduct. Firms' cooperation with our investigations, including through voluntary self-reporting of potential violations, benefits all market participants.

Over the last several months, I have heard time and again that we are insufficiently clear regarding our views on cooperation. So let me try and offer some clarity. First, let me be clear about what cooperation is not: cooperation is not the mere absence of obstruction.

We do not recommend that parties receive credit for simply living up to their legal and regulatory obligations. Cooperation—at least the sort of cooperation that results in credit—means more than responding to lawful subpoenas.

It means more than making witnesses available for lawfully-compelled testimony. Any defense counsel who advises that credit may be on the table for taking these standard steps is doing their client a disservice.

Cooperation also means more than "self-reporting" to the SEC only when your violation is about to be publicly announced through charges by another regulator or an article in the news media.

And it certainly means more than conducting a purportedly independent investigation and making a presentation to the staff that does not fairly present the facts, but instead is nothing more than an advocacy piece. The behaviors that can earn cooperation credit are no secret: the Seaboard Report turns 20 years old this month; the SEC's Policy Statement Concerning Cooperation by Individuals was issued in 2010; and the Enforcement Manual includes pages of discussion concerning the relevant tools and analytical frameworks.

And in several recent orders, the Commission has described the kinds of behavior that can garner cooperation credit.

For example, last September, the Commission charged BMW for disclosing inaccurate and misleading sales numbers in connection with a bond offering.

The SEC's order detailed the many steps BMW took during the global pandemic to collect, synthesize, translate where necessary, and present significant volumes of relevant materials to staff.

The order highlighted how "BMW also made multiple current and former employees available for interviews by the Staff, and provided presentations and narrative submissions that highlighted critical facts."

In short, BMW's cooperation "substantially advanced the quality and efficiency of the Staff's investigation and conserved Commission resources," and this was reflected in the Commission's decision to impose a reduced penalty against BMW.

But in case it's helpful, let me also tell you how I specifically think about cooperation. I look to whether the would-be cooperator took significant, tangible steps that enhanced the quality of our investigation, allowed us to conserve resources and bring charges more quickly, or helped us to identify additional conduct or other violators that contributed to the wrongdoing. If any or all of these occurred, then credit may be appropriate.

One last thing on cooperation. If you think you deserve credit, and the staff disagrees, I encourage you take a hard, objective look at your conduct during the investigation before trying to convince me the staff is wrong.

As someone who has served as a federal prosecutor, local prosecutor, and state Attorney General, I firmly believe that frontline staff are best-positioned to assess cooperation with the investigations they conduct.

They know the record and they know whether you meaningfully benefited those investigations. I respect their experience and will not only seek their input on decisions, but will also generally defer to their expertise and judgment.

At the same time, I will not look favorably on attempts to make an end run around staff to present the same, undisputed facts about your conduct to me in hopes of a more sympathetic ear.

Similarly, you should understand that we have a close relationship with our colleagues in EXAMS. If a party or its counsel engage in dilatory or obstructive tactics in an examination that gives rise to a referral, I will take a dim view of arguments that you deserve credit for cooperation with the ensuing enforcement investigation. As I said earlier, a key consideration in

weighing cooperation is whether it conserves Commission resources, and this goes for those of our colleagues across the Commission.

Finally, I want to discuss the third step in our shared mission. This one applies when the first two steps have not worked. In that scenario, all of our enforcement tools are on the table, including monetary penalties.

Penalties are among the most important of our tools, in part because of our ability to tailor them to the violation. When Congress granted the SEC penalty authority in the Remedies Act of 1990, one perceived benefit was the SEC's ability to more finely calibrate its enforcement remedies against regulated entities, including broker-dealers.

By granting penalty authority, the Remedies Act empowered the Commission to impose remedies that were substantially more punitive than a censure, but less draconian than revoking a firm's registration or suspending its operations, and thereby potentially harming its customers.

The factors that guide us as we tailor our penalty recommendations are also no secret—we assess the conduct at issue in light of elements including statutory tiers, Commission guidance and judicial opinions, and resolutions in Commission actions involving comparable facts, violations, and parties.

One crucial question we also try to answer is what penalty will appropriately deter future misconduct? After all, penalties calibrated to both the offense and the offender, serve two interlocking purposes: punishment of the wrongdoer and deterrence of future misconduct, both by the penalized party and by others in the market.

And central to deterrence is proportionality. The worse the conduct, the more strongly we want to disincentivize market participants from engaging in it. We must design penalties that actually deter and reduce violations, and are not seen as an acceptable cost of doing business.

What does this mean for our approach to penalties in enforcement actions? As Commissioner Crenshaw put it earlier this year: "[C]orporate penalties should be tied to the egregiousness of the actual misconduct." I agree wholeheartedly. But this does not mean that roughly equivalent misconduct by comparable offenders should be penalized in the same amount the hundredth time it occurs as the first. Rather, to achieve the intended deterrent effect, it may be appropriate to impose more significant penalties for comparable behavior over time. Doing so will make it harder for market participants to simply "price in" the potential costs of a violation.

As we evaluate the relevant penalty factors, we will also be closely assessing whether prior penalties have been sufficient to generally deter the misconduct at issue.

Where they have not been, you can expect to see us seek larger penalties, both in settlement negotiations and, if necessary, in litigation. Even if a firm or individual hasn't offended before, if they violate a law or rule for which the SEC has previously and publicly charged other actors in their industry, it may be appropriate for penalties or other remedies to be increased in response to the lack of deterrence.

So while penalties levied in the past are certainly a relevant data point for our conversations, you should not expect comparable cases to be the beginning and end of our analysis.

Similarly, one factor that has long weighed in our penalty assessments is the recidivism of the specific offender.

When a firm repeatedly violates our laws or rules, they should expect to be penalized more harshly than a first-time offender might be for the same conduct. This is the essence of specific deterrence.

I am confident that by engaging in proactive compliance and meaningful cooperation, and, where necessary, imposing significant, but appropriate penalties, through our enforcement efforts, we will not only reinforce market integrity, but also enhance public confidence in our markets. I look forward to working with all of you in achieving this, our shared mission.

FSI Insights on policy implementation No 36

Big tech regulation: what is going on?

By Juan Carlos Crisanto, Johannes Ehrentraud, Aidan Lawson and Fernando Restoy

BIS

The emergence of large technology firms (big techs) represents a major source of disruption to the financial system and the economy.

Big techs have expanded the available range of financial products and services, often with enhanced customer experience. However, the ease and speed with which these companies can scale up their activities and expand into finance may generate pronounced concentration dynamics.

This could significantly affect the adequate functioning of the financial system and may damage market contestability and eventually increase operational vulnerabilities due to the excessive reliance of market players on the services provided by big techs.

Different jurisdictions have moved to adjust their policy frameworks to cope with the risks presented by big techs.

In particular, a number of policy initiatives have emerged in China, the European Union (EU) and the United States over the last few years in the areas of competition, data protection and data-sharing, operational resilience, conduct of business and financial stability.

These initiatives generally seek to achieve a balance between addressing the different risks posed by big techs and preserving the benefits they bring in terms of market efficiency and financial inclusion.

Thus far, competition has been the policy area where the most initiatives have been conducted and a paradigm shift is emerging.

Given the large potential for big techs to abuse their technological and data superiority to quickly dominate different market segments and adopt anticompetitive practices, preserving market contestability has become a top priority for authorities in China, the EU and the US.

Competition policy proposals include not only the augmentation of traditional ex post enforcement tools but also the creation of new big tech-specific ex ante regulatory regimes.

A number of data protection and data-sharing initiatives have been proposed.

Policy initiatives across the three jurisdictions place special emphasis on personal data use and data protection.

Moreover, there are relevant initiatives, particularly in China and the EU, with respect to users' data portability.

This, together with emerging policy and market developments on data-sharing, seems to be paving the way to a generalised use of personal data for the provision of financial services by different types of entities.

Policy initiatives are addressing the operational resilience of big tech firms.

These typically apply to big techs either as providers of financial services2 or as third-party service providers of financial firms.

The operational resilience requirements in both cases intend to capture all sources of operational risk (in particular, information and communication technology risks) and expect adoption of sound risk management practices, swift response in case of disruption and continuity of critical services.

Some jurisdictions have taken meaningful policy efforts to address potential conduct issues and financial stability challenges but they do not follow an homogeneous pattern.

A key development in the conduct of business area is the EU's proposed Digital Services Act (DSA). This establishes extensive requirements for very large online platforms connected with the functioning and use of their services.

As such, the DSA represents a comprehensive effort to deal with how big techs treat their customers and the information they receive.

Regarding financial stability, the main regulatory development is the China financial holding company (FHC) regime.

This requires all entities holding two or more types of financial institutions to be structured and licenced as FHCs (if size thresholds or other conditions are met).

This effectively mandated big techs to reorganise their financial business and represents a novel entity-based regulatory approach that entails a comprehensive oversight of the activities performed by big techs through all their financial subsidiaries.

Additional regulatory responses might be needed to comprehensively address big tech risks and achieve policy consistency at the international level.

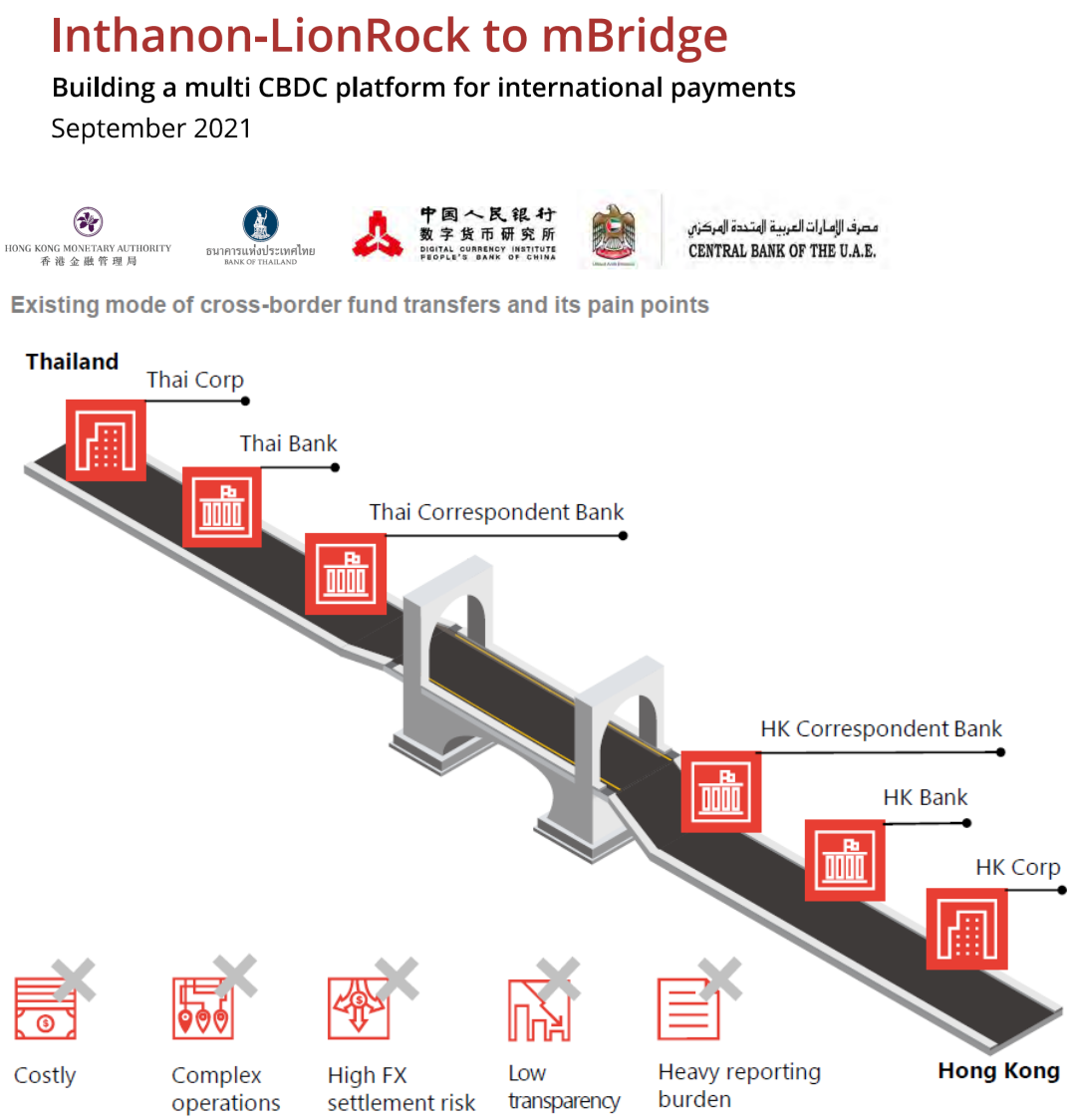
Recent initiatives in China, the EU and the US constitute important steps in addressing risks posed by big techs. However, if big techs continue to gain prominence in the financial system, additional policy responses might be necessary.

It is also very likely that new policy actions will largely need to follow an entity-based approach and require close cooperation between competition, data and financial authorities. Moreover, given the cross-border scope of big tech activities, enhanced international regulatory cooperation is essential.

To read more: https://www.bis.org/fsi/publ/insights36.pdf

Inthanon-LionRock to mBridge: Building a multi CBDC platform for international payments

Joint report by the BIS Innovation Hub Hong Kong Centre, the Hong Kong Monetary Authority, the Bank of Thailand, the Digital Currency Institute of the People's Bank of China, the Central Bank of the United Arab Emirates.



In the absence of multilateral solutions for cross-border payments, correspondent banks currently act as bridges, moving payments from one jurisdiction to another.

To achieve this, they have built extensive correspondent banking networks and arrangements.

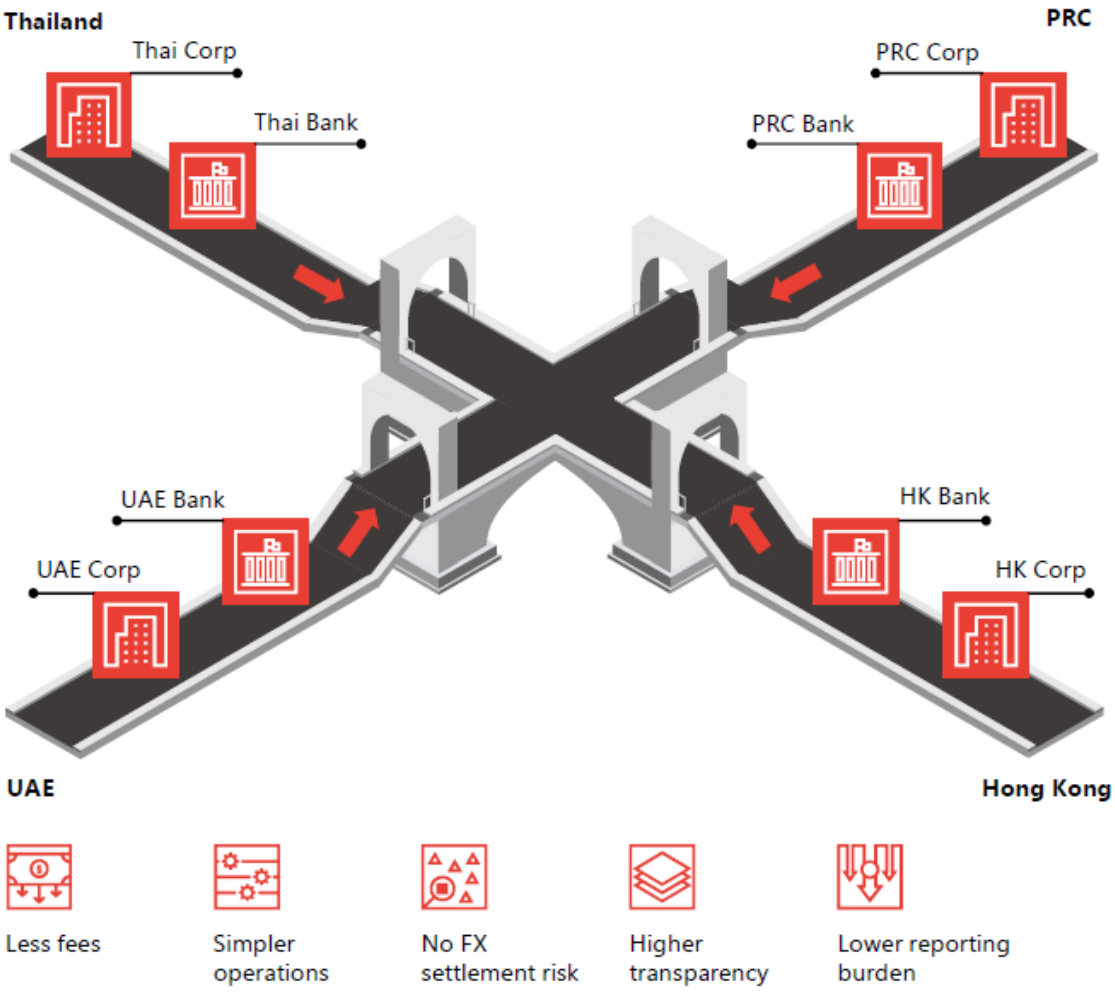
While serving a critical economic role, these networks and arrangements also introduce more intermediary steps in the system, as correspondent banks are spread out across multiple time zones and different operating hours.

This leads to increased operational complexity, possible bottlenecks and duplication. For example, know-your-customer (KYC) processes are repeated by every bank in the correspondent banking process flow.

As illustrated in the published report of Inthanon-LionRock Phase 1 this in turn leads to higher cost and slower speed of cross-border payments.

This process complexity also is paired with high FX settlement risk, low transparency and a high reporting burden.

Inthanon-LionRock and mBridge Model

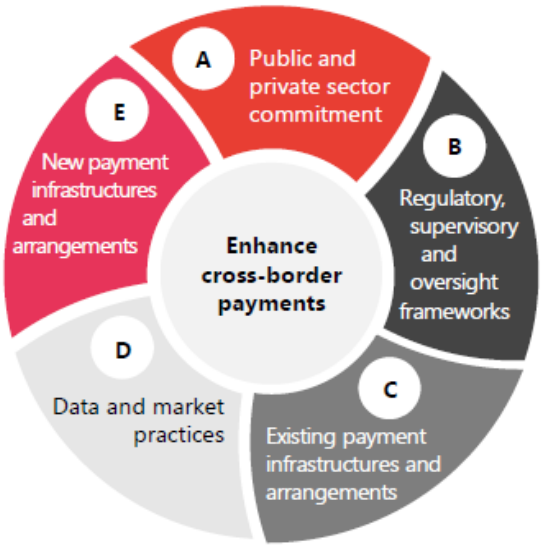


Source: Adapted from Inthanon-LionRock Leveraging Distributed Ledger Technology to Increase Efficiency in Cross-Border Payments, January 2020

Roadmap to enhancing cross-border payments

1. Develop common cross-border payments vision and targets
2. Implement international guidance and principles
3. Define common features of cross-border payment service levels

A



4. Align regulatory, supervisory and oversight frameworks
5. Apply AML/CFT consistently and comprehensively
6. Review interaction between data frameworks and cross-border payments
7. Promote safe payment corridors
8. Foster KYC and identity information-sharing

B

C

9. Facilitate increased adoption of PvP
10. Improve (direct) access to payment systems
11. Explore reciprocal liquidity arrangements
12. Extend and align operating hours
13. Pursue interlinking of payment systems

D

14. Adopt a harmonised version of ISO 20022 for message formats
15. Harmonise API protocols for data exchange
16. Establish unique identifiers with proxy registries

E

17. Consider the feasibility of new multilateral platforms and arrangements for cross-border payments
18. Foster the soundness of global stablecoins arrangements
19. Factor an international dimension into CBDC designs

Source: Enhancing cross-border payments: building blocks of a global roadmap Stage 2 report to the G20, July 2020[18]

To read more: https://www.bis.org/publ/othp40.htm

Moving forward in securing Online Trust via the Digital Wallets

The 2021 Trust Service Forum allows stakeholder communities to engage in open discussions on securing trust services online and on the future of the EU Digital Identity Framework.

Electronic signatures, electronic seals and other online trust services have become a staple in the life of many Europeans.

In light of the COVID-19 pandemic, a key aspect to ensure a viable business model for qualified trust service providers was an increasing usage of online trusted services among European citizens, businesses and public administrations in an online mode.

This new reality across the EU has highlighted the security concerns of remote identification and authentication processes.

The necessity for a new framework for EU digital identity became apparent.

The European Commission presented last June a new framework for the EU digital identity by offering to citizens and businesses the digital wallets that will allow EU citizens to retain their documents such as national digital identities, licences, diplomas and bank credentials securely in their smartphone.

The wallet should also allow them to log in to online services across the EU and to electronically sign their documents.

On September 21st, the European Union Agency for Cybersecurity (ENISA) in collaboration with the European Commission delivered the 7th consecutive ‘’Trust Service Forum’’.

It attracted over to 1000 participants and brought more than forty experts, service providers, conformity assessment, supervisory bodies and national authorities together, to discuss the online trust market and its emerging issues under the European Commission’s Regulation 910/2014, on electronic identification and trusted services for electronic transactions in the internal market (eIDAS Regulation).

On 22nd September, D-TRUST in cooperation with TÜViT and the European School of Management and Technology (ESMT), held the 13th CA-Day.

Both conferences were held in a hybrid format, with physical presence for the panellists at the ESMT premises in Berlin and virtually for the participants.

The forum was jointly opened by the European Commission's Director of Digital Society, Trust and Cybersecurity Ms. Lorena Boix Alonso and ENISA's Head of Policy Development and Implementation Unit Mr. Evangelos Ouzounis and it was consisted of three main distinct blocks.

In the first one, the panellists discussed the new ''EU Digital Identity Framework- bringing opportunity to wider use of online trust solutions across the EU".

The concept of decentralised online identity, that gives back control to users over their personal data and leverages the use of an identity wallet, was additionally discussed.

Second block focused on certification and standardisation efforts and the third one on the trust service market – current state of play, opportunities and outlook.

Panellists had also the opportunity to further elaborate on the upcoming revisions of the eIDAS Regulation that proposes to further extend its application to the private sector and to promote trusted digital identities across the EU.

Background

The Trust Services Forum acts as a platform for participants to share their good practices on the implementation of trust services; review the standards, implementing acts and technical guidelines within the eIDAS; and discuss strategies to promote the adoption of qualified trust services.

The EU Agency for Cybersecurity supports the Commission on the implementation of the eIDAS by providing security recommendations for the implementation of trust services, mapping technical and regulatory requirements, promoting the deployment of qualified trust services in Europe and raising awareness among users on securing their e-transactions.

Under the EU Cybersecurity Act of 2019, the Agency gained an extended mandate to explore the area of electronic identification (eIDs) included in the regulation.

EU's Digital Wallet's proposal

The Commission on the 3rd June 2021 proposed a framework for a European Digital Identity which will be available to all EU citizens, residents, and businesses in the EU. Citizens will be able to prove their identity and share electronic documents from their European Digital Identity wallets with the click of a button on their phone.

They will be able to access online services with their national digital identification, which will be recognised throughout Europe. Large platforms are proposed to accept the use of European Digital Identity wallets upon request of the user, for example to prove their age. Use of the European Digital Identity wallet will always be at the choice of the user.

The new European Digital Identity Wallets will enable all Europeans to access services online without having to use private identification methods or unnecessarily sharing personal data. With this solution they will have full control of the data they share.

Rule governing Board determination under the Holding Foreign Companies Accountable Act

The Public Company Accounting Oversight Board (the "PCAOB" or the "Board") is adopting a new rule, PCAOB Rule 6100, Board Determinations Under the Holding Foreign Companies Accountable Act, to provide a framework for its determinations under the Holding Foreign Companies Accountable Act (the "HFCAA") that the Board is unable to inspect or investigate completely registered public accounting firms located in a foreign jurisdiction because of a position taken by one or more authorities in that jurisdiction.

The rule establishes the manner of the Board's determinations; the factors the Board will evaluate and the documents and information the Board will consider when assessing whether a determination is warranted; the form, public availability, effective date, and duration of such determinations; and the process by which the Board will reaffirm, modify, or vacate any such determinations.

Executive summary

The Sarbanes-Oxley Act of 2002 (the "Act") mandates that the Board inspect registered public accounting firms and investigate possible statutory, rule, and professional standards violations committed by those firms and their associated persons.

That mandate applies with equal force to the Board's oversight of registered firms in the United States and in foreign jurisdictions.

Over the course of more than a decade, the Board has worked effectively with authorities in foreign jurisdictions to fulfill its mandate to oversee registered firms located outside the United States.

With rare exceptions, foreign audit regulators have cooperated with the Board and allowed it to exercise its oversight authority as it relates to registered firms located within their respective jurisdictions.

The norms of international comity have guided those efforts and allowed the Board to work cooperatively across borders, to resolve conflicts of law, and to overcome other potential obstacles.

The Board benefits greatly from cross-border cooperation with its international counterparts and has built constructive relationships that facilitate meaningful oversight.

Authorities in a limited number of foreign jurisdictions, however, have taken positions that deny the Board the access it needs to conduct its mandated oversight activities.

Recognizing the ongoing obstacles to Board inspections and investigations in certain foreign jurisdictions, Congress enacted the HFCAA.

The HFCAA requires that the Board determine whether it is unable to inspect or investigate completely registered public accounting firms located in a foreign jurisdiction because of a position taken by one or more authorities in that jurisdiction.

The HFCAA, among other things, also mandates that, after the Board makes such a determination, the U.S. Securities and Exchange Commission (the "Commission") shall require covered issuers who retain such firms to make certain disclosures in their annual reports and, eventually, if certain conditions persist, shall prohibit trading in those issuers' securities.

Following public comment, the Board is adopting a new rule, PCAOB Rule 6100, Board Determinations Under the Holding Foreign Companies Accountable Act, as proposed with some modifications after consideration of comments, to establish a framework for the Board to make its determinations under the HFCAA.

The final rule establishes the manner of the Board's determinations; the factors the Board will evaluate and the documents and information it will consider when assessing whether a determination is warranted; the form, public availability, effective date, and duration of such determinations; and the process by which the Board will reaffirm, modify, or vacate any such determinations.

To read more: https://pcaob-assets.azureedge.net/pcaob-dev/docs/default-source/rulemaking/docket048/2021-004-hfcaa-adopting-release.pdf?sfvrsn=f6dfb7f8_4

Statement in Support of Adoption of PCAOB Rule 6100, Board Determinations Under the Holding Foreign Companies Accountable Act

Duane M. DesParte, Acting Chairperson - PCAOB Open Board Meeting

I fully support adoption of PCAOB Rule 6100, Board Determinations Under the Holding Foreign Companies Accountable Act (HFCAA), as set forth before us today.

Robust inspections and investigations of registered public accounting firms auditing U.S. public companies are core to the PCAOB's mandate under the Sarbanes-Oxley Act. This is true whether such firms are located inside or outside of the United States.

Through the passage of the HFCAA, Congress reaffirmed the importance of our oversight activities in providing protection for investors in all U.S. public companies, regardless of where the companies' audit firms are located or their audits are performed.

Rule 6100 establishes a framework for the determinations we are required to make under the HFCAA. This framework will help to promote consistency in our determinations and to provide transparency to investors, firms, issuers, foreign authorities, and other market participants as to the factors the Board will consider and the processes it will use in making and publicly reporting its determinations.

Furthermore, the framework includes a mechanism whereby the Board will reassess its determinations every year, which will provide increased clarity and certainty to market participants over time.

Transparency of the Board's framework is particularly important given the potential consequences that might follow Board determinations under the HFCAA for issuers, investors, and the broader capital markets.

In addition to setting forth the key factors the Board will assess in making determinations, the rule promotes transparency by requiring the Board to describe in a public report its assessment and the basis for its conclusion for any determination it makes.

The rule also requires the Board to reassess and publicly report on its determinations at least annually, which will help ensure market participants remain timely informed of the status of our ability to inspect or investigate completely audit firms in the covered foreign jurisdictions. In this way, the final rule provides more certainty to market participants

than was provided by the two-step reassessment approach set forth in the proposal.

I therefore support the rule before us. It provides the Board a clear and consistent approach for making its determinations and for keeping all interested market participants well informed through timely public reporting.

In closing, I want to thank all those at the PCAOB who have contributed to developing today's final rule; including our staff in the Offices of International Affairs, General Counsel, and Economic and Risk Analysis and with special recognition for Liza McAndrew Moberg, Beth Hilliard Colleye, Ken Lench, Drew Dropkin, and Damon Andrews. I also want to thank the Commission's staff for their support and assistance.

Conti Ransomware Attacks Impact Healthcare and First Responder Networks

The FBI identified at least 16 Conti ransomware attacks targeting US healthcare and first responder networks, including law enforcement agencies, emergency medical services, 9-1-1 dispatch centers, and municipalities within the last year.

These healthcare and first responder networks are among the more than 400 organizations worldwide victimized by Conti, over 290 of which are located in the U.S. Like most ransomware variants, Conti typically steals victims' files and encrypts the servers and workstations in an effort to force a ransom payment from the victim.

The ransom letter instructs victims to contact the actors through an online portal to complete the transaction. If the ransom is not paid, the stolen data is sold or published to a public site controlled by the Conti actors.

Ransom amounts vary widely and we assess are tailored to the victim. Recent ransom demands have been as high as $25 million.

Cyber attacks targeting networks used by emergency services personnel can delay access to real-time digital information, increasing safety risks to first responders and could endanger the public who rely on calls for service to not be delayed.

Loss of access to law enforcement networks may impede investigative capabilities and create prosecution challenges.

Targeting healthcare networks can delay access to vital information, potentially affecting care and treatment of patients including cancellation of procedures, rerouting to unaffected facilities, and compromise of Protected Health Information.

Technical Details

Conti actors gain unauthorized access to victim networks through weaponized malicious email links, attachments, or stolen Remote Desktop Protocol (RDP) credentials. Conti weaponizes Word documents with embedded Powershell scripts, initially staging Cobalt Strike via the Word documents and then dropping Emotet onto the network, giving the actor access to deploy ransomware.

Actors are observed inside the victim network between four days and three weeks on average before deploying Conti ransomware, primarily using dynamic-link libraries (DLLs) for delivery.

The actors first use tools already available on the network, and then add tools as needed, such as Windows Sysinternals and Mimikatz to escalate privileges and move laterally through the network before exfiltrating and encrypting data.

In some cases where additional resources are needed, the actors also use Trickbot. Once Conti actors deploy the ransomware, they may stay in the network and beacon out using Anchor DNS.

If the victim does not respond to the ransom demands two to eight days after the ransomware deployment, Conti actors often call the victim using single-use Voice Over Internet Protocol (VOIP) numbers. The actors may also communicate with the victim using ProtonMail, and in some instances victims have negotiated a reduced ransom.

To read more: https://www.aha.org/system/files/media/file/2021/05/fbi-tlp-white-report-conti-ransomware-attacks-impact-healthcare-and-first-responder-networks-5-20-21.pdf

Simulating wartime decisions helps prepare for the real thing

Los Alamos NATIONAL LABORATORY

On August 17, Alaskan officials reported 81 cases of an unidentified hemorrhagic fever, similar to but more contagious than the Ebola or Marburg viruses, on the Alaskan island of St. Paul in the Bering Strait.

Within a day, 24 infected people had died. The outbreak occurred two weeks after the United States was accused of sinking the Russian ship Ulana.

Americans had attempted to search Ulana because they suspected it of carrying biological warfare materials to Russia's recently solidified ally North Korea.

Four U.S. Marines died in the skirmish, as well as almost all of the Russian ship's crew.

In addition, a group of South Korean tourists—one of whom had North Korean ties—visited St. Paul three days before the first infection was discovered.

These combined events have led to an increasingly volatile situation between the United States, Russia, and multiple countries in the Asian-Pacific.

If you're thinking you missed some major breaking news, you can breathe a sigh of relief. This all takes place in a *fictional version of 2039*; it's a scenario that was played out in a tabletop exercise (TTX)—a mini-wargame— titled St. Paul Syndrome II, in March of 2021.

Pieces on a board

A wargame, according to deceased wargaming expert Francis J. McHugh of the United States Naval War College, "is a simulation, in accordance with predetermined rules, data, and procedures, of selected aspects of a conflict situation." It's essentially a pretend war.

Wargaming has been around for hundreds of years. "John Clerk, a landsman with no actual experience in the ways of the sea, revolutionized British 18th-century naval tactics by using a tabletop for an ocean and wooden blocks to represent ships," McHugh explained in Fundamentals of War Gaming, which was published in 1960.

The United States has used similar techniques for a long time. According to a 2015 article by then Deputy Secretary of Defense Bob Work and Vice Chairman of the Joint Chiefs of Staff General Paul Selva, during the 1920s and 1930s, "militaries the world over struggled to adapt to new inventions such as radar and sonar, as well as rapid improvements in wireless communications, mechanization, aviation, aircraft carriers, submarines, and a host of other militarily relevant technologies."

During this time, the United States military began to lean heavily on wargaming to play out the possibilities of these new developments and their impact on warfare.

"Wargaming is strategic analysis," says Rich Castro, the retired director of the Strategic Analyses and Assessments Office at Los Alamos National Laboratory. "The Lab's participation is important because wargaming is an analytical tool that brings together many different thoughts, combining the expertise of the Department of Defense, Department of Energy, and the national laboratories."

Wargames help leaders consider different scenarios and think about how they might play out so they can prepare to make quick decisions in the event that a similar scenario actually takes place. "Things are moving so fast, technology moves so fast, you have to think faster," Castro says.

"We don't have the luxury of thinking about these problems in the long-term. There are a lot of changes in our adversaries—cyber, space, nuclear, conventional—that didn't exist during the Cold War. They all come together now in an escalation ladder. You have to play this out or you're caught completely off guard."

Full-scale wargames are played at different locations in the United States, often at the Naval War College in Rhode Island, with hundreds of participants present from all across the country.

The basic structure is that a group of analysts from the organization running the game write a scenario— usually focused on a particular region, technology, or situation that is pertinent to current concerns—to be played out over the course of one or two weeks. Preparation for the game usually takes several months.

Players are assigned to teams that represent countries; a control group determines the outcome of team decisions, actions, and interactions with other country teams. The control group also represents countries that do not have assigned teams. More than 30 large-scale wargames are held annually across the nation, and players from Los Alamos are invited for a particularly important reason—their nuclear expertise.

The nuclear niche

According to Tim Goorley, Los Alamos' lead wargaming consultant for nuclear effects, Los Alamos provides expertise on what happens to people, aircraft, sea vessels, and satellites, for example, in the event of a nuclear detonation. That information is then fed into the game to help the players on both sides understand what possible actions they could take next.

Laboratory personnel provide expertise in person at wargames, and they're consulted ahead of the games during the long, complicated process of scenario creation. For example, one game incorporated whether it was possible to have a new weapon, and, if such a weapon existed, how many the United States might own. Goorley called some Los Alamos engineers to see whether such a weapon could be produced in the timeframe required by the game and whether it could be deployed and used in the way the game planners wanted.

The Los Alamos scrimmage

Another way in which wargames are useful is that they help debunk commonly believed myths about nuclear weapons.

Many wargames end with the detonation of a nuclear weapon, assuming that's a game-over event.

But, according to Goorley, that's not true at all; things are just getting started.

"People don't realize how much you can still do just a few miles or days out from ground zero," he says. "You need to keep going through the game for about a week or two after the detonation to fully understand the effects."

Although many films show city blocks being instantly vaporized by a nuclear weapon, or show an electromagnetic pulse sending a huge part of the country back to the dark ages, those scenarios are not realistic, and realism is vital to productive wargames.

As Goorley puts it, the Laboratory "takes the falling sky and puts it back up."

Experts from Los Alamos are also able to give particular insight into adversaries' policy and technical capabilities. "It takes a nuclear weapons designer to catch a nuclear weapons designer," Goorley explains.

Although full-scale wargames are the longest and most detailed versions, smaller versions referred to as tabletop exercises exist, in which fewer people play out a scenario in a shorter timeframe.

Los Alamos has been conducting tabletop exercises for several years, the most recent being the St. Paul Syndrome II scenario.

St. Paul Syndrome II was a collaboration between the Laboratory's Office of National Security and International Studies (NSIS) and the Center for Strategies and International Studies (CSIS), a Washington, D.C., think tank with whom the Lab has partnered. In fact, the most recent TTX was a replay of a scenario (St. Paul Syndrome I) that different participants played out in the summer of 2020.

By keeping that scenario secret, Los Alamos and CSIS were able to use it again with new players who, through their different decisions, revealed entirely new options and pathways for the unfolding events. "I have learned never to expect particular outcomes," says Ian Williams, an International Security Program fellow and deputy director for the CSIS Missile Defense Project. "Even when running the same scenario with participants of similar professional backgrounds, we see teams take a wide variety of strategies and actions."

St. Paul Syndrome I and II were developed "to explore how decision makers respond to a multi-domain national security conflict," says Paula Knepper, an NSIS program manager. "In this case, we have nuclear and bioweapons as well as an issue related to the Arctic."

The scenario was "the most complex one that we have done so far," Williams says. "Rather than have one major crisis that all the teams were focused on, the scenario had each team facing a different issue that overlapped with the vital interests of the other country teams. This dramatically increased the potential friction points between countries."

NSIS is in charge of choosing Laboratory participants and filling each team roster. An invitation is quite desirable at Los Alamos; for St. Paul Syndrome II, the rosters were filled in less than 24 hours. "One of our objectives is staff development," Knepper says.

"We keep in mind creating opportunities for Laboratory staff to extend their professional networks. We also look for team diversity—experiences, organizations, technical backgrounds, etc. We find that diverse teams have the most insightful and creative outcomes."

Wargames are as realistic as possible and are based on current intelligence, so most are conducted at top secret levels so real intelligence agents can attend and contribute what they know.

The recent TTX between Los Alamos and CSIS, however, was not classified, so the lessons learned from it can be put to broader use. TTXs can be

unclassified because they focus on scenarios that take place years in the future, in a world that is only a possibility.

Los Alamos is a particularly useful ecosystem for wargames and small-scale exercises alike because of the close proximity and working relationships of people from many areas of expertise, including engineers, infrastructure experts, policy experts, and scientists from myriad fields.

“The Laboratory is a unique place,” Castro says, “in that it can pull together a team to quickly address multi-domain issues, and everyone can be sequestered in an area just to concentrate on one problem. I don’t know other places that you can do that.”

The coronavirus pandemic threw a wrench into that unique capability in that teams were not able to sequester in person for the past two TTXs, but CSIS and NSIS quickly adapted to build a virtual game space.

Personnel from CSIS ran the game and were assigned to help the country teams, but all of the players were Lab employees.

Some were scientists from fields including nuclear engineering, astrophysics, geophysics, and biosecurity and public health. Others were from intelligence systems, international studies, and international threat reduction.

Most Los Alamos players had never participated in a wargame before. “It was really neat hearing how people with different academic and professional backgrounds approached problems,” says Caleb Schelle, a shock and vibration testing engineer. “I was one of the younger members on the team, and I appreciated learning how more experienced scientists and engineers chose their words and actions thoughtfully.”

Amanda Evans, a scientist in chemical and biological threats, also valued the insight of her colleagues during the TTX. “Building our team’s interactions was a very positive experience,” she says, “as was learning from more experienced colleagues.”

Kickoff

Before the TTX began, participants were divided into teams, each team representing a country—the United States, Russia, China, and Japan. Team members prepared by reading historical background information that was available to all teams plus some country-specific information provided by their countries’ intelligence services.

Teams also received information about their own countries’ military capabilities and strategic positions, along with information about that of other countries—to the best of their intelligence agencies’ knowledge. They

then began to make decisions to play out the scenario, all over the course of just four days.

On the first day of the TTX, after meeting all together, the country teams broke into separate groups and got to work examining the current state of the scenario and determining their main objectives.

At the end of each day, each team must submit its "turn," which includes its objectives and actions—both public and covert.

The time spent in groups is used to discuss how to make those decisions, to read and discuss new information as it comes in throughout the day from the control group, and, at times, to communicate with other countries.

Early in the day, the United States team learned from the Centers for Disease Control and Prevention that the St. Paul virus was a form of Marburg virus that had been developed in a Soviet laboratory in the 1980s, meaning that the outbreak was a bio-attack made by either Russia or Russian-aided North Korea.

The American team's response to this news was much more peaceful than many might have guessed. "It was interesting to see how the U.S. team did not really view it as an attack," observes NSIS Director John Scott. "They appeared to be most concerned about containing the outbreak on the island."

Meanwhile, the Russian team began to launch misinformation campaigns to place blame on the United States for the Ulana sinking, China worked to disrupt American power in the Pacific, and Japan, faced with growing anti-American sentiment among its citizens, strategized the best ways to restore peace to both the region and its own people.

Over the next four days, teams worked to destabilize relationships between other countries, solidify their allies, secure military positions, avoid war, gather and decipher intelligence, get their political parties re-elected, and stop an outbreak of a disease with a 99 percent fatality rate. They moved their military ships around, demanded that each other remove ships from certain areas, and communicated with each other via confidential channels. They issued public statements to each other and to their own citizens.

Teams also received a great deal of information that threw them for loops. For example, uncovered intelligence determined that the Russians had scuttled the Ulana (sunk their own ship) and blamed it on the Americans. Information was also revealed that the Ulana was carrying equipment for bioweapons, yet it seemed that Russia was not directly involved in releasing Marburg on St. Paul Island.

To read more: https://discover.lanl.gov/publications/national-security-science/2021-summer/wargames

Selecting and Hardening Remote Access VPN Solutions

National Security Agency | Cybersecurity and Infrastructure Security Agency | Cybersecurity Information Sheet

Virtual Private Networks (VPNs) allow users to remotely connect to a corporate network via a secure tunnel.

Through this tunnel, users can take advantage of the internal services and protections normally offered to on-site users, such as email/collaboration tools, sensitive document repositories, and perimeter firewalls and gateways.

Because remote access VPN servers are entry points into protected networks, they are targets for adversaries.

This joint NSA-CISA information sheet provides guidance on:

- Selecting standards-based VPNs from reputable vendors that have a proven track record of quickly remediating known vulnerabilities and following best practices for using strong authentication credentials.

- Hardening the VPN against compromise by reducing the VPN server's attack surface through:

Configuring strong cryptography and authentication

Running only strictly necessary features

Protecting and monitoring access to and from the VPN

Active Exploitation

Multiple nation-state Advanced Persistent Threat (APT) actors have exploited public Common Vulnerabilities and Exposures (CVEs) to compromise vulnerable VPN devices.

In some cases, exploit code is freely available online. Exploitation of these public CVEs can enable a malicious actor to perform:
- Credential harvesting
- Remote code execution of arbitrary code on the VPN device
- Cryptographic weakening of encrypted traffic sessions

- Hijacking of encrypted traffic sessions
- Arbitrary reads of sensitive data (e.g., configurations, credentials, keys) from the device

These effects usually lead to further malicious access through the VPN, resulting in large-scale compromise of the corporate network or identity infrastructure and sometimes of separate services as well.

To read more: https://media.defense.gov/2021/Sep/28/2002863184/-1/-1/0/CSI_SELECTING-HARDENING-REMOTE-ACCESS-VPNS-20210928.PDF

Disclaimer

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

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

This information:

- is of a general nature only and is not intended to address the specific circumstances of any particular individual or entity;

- should not be relied on in the particular context of enforcement or similar regulatory action;

- is not necessarily comprehensive, complete, or up to date;

- is sometimes linked to external sites over which the Association has no control and for which the Association assumes no responsibility;

- is not professional or legal advice (if you need specific advice, you should always consult a suitably qualified professional);

- is in no way constitutive of an interpretative document;

- does not prejudge the position that the relevant authorities might decide to take on the same matters if developments, including Court rulings, were to lead it to revise some of the views expressed here;

- does not prejudge the interpretation that the Courts might place on the matters at issue.

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

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

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

International Association of Potential, New and Sitting Members of the Board of Directors (IAMBD)

The IAMBD offers standard, premium and lifetime membership, networking, training, certification programs, a monthly newsletter with alerts and updates, and services we can use.

The association develops and maintains three certification programs and many specialized tailor-made training programs for directors.

Join us. Read our monthly newsletter with news, alerts, challenges and opportunities. Get certified. Provide independent evidence that you are an expert.

You can explore what we offer to our members:

1. Membership - Become a standard, premium or lifetime member.
You may visit:
https://www.iambd.org/HowToBecomeMember.html

2. Monthly Updates – Visit the Reading Room of the association at:
https://www.iambd.org/Reading_Room.htm

3. Training and Certification - Become a Certified Member of the Board of Directors (CMBD), Certified Member of the Risk Committee of the Board of Directors (CMRBD) or Certified Member of the Corporate Sustainability Committee of the Board of Directors (CMCSCBD).

You may visit:
https://www.iambd.org/Distance_Learning_and_Certification.htm

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