Monday, April 8, 2024

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.

Mary Ann Evans (pen name: George Eliot) was an English novelist and poet. She has said: "Blessed is the influence of one true, loving human soul on another."

Unfortunately, influence is not always that positive. Max Weber has said: "Politics means striving to share power or striving to influence the distribution of power, either among states or among groups within a state."

I have just read an excellent report that covers countermeasures and capabilities against *information influence operations (IIO)*.

It includes scenarios and assists in creating a discussion on *what capabilities* are needed and *how* organisations can develop these capabilities based on available resources.

All parts of society can be affected by IIO and should develop capabilities to counter disinformation. The selected workshops can be adapted to work on a *local, regional, or national* level.

To test the workshop method, three workshops at the local, regional, and national level were planned and conducted together with the Swedish Psychological Defence Agency (MPF). Sweden was the example nation, but the method can of

course be applied to other nations. Testing the method at different societal levels contributed to analysing whether the selected method was suited to different actors and could be used to find reasonable levels of capability in countering IIO regarding their responsibilities.

The workshops, called PSYCAP 2023, were held in Sweden and run with a Municipal and a County Administration Board, and a Swedish National agency.

All three organisations were faced with the same challenges, just slightly modified to fit their responsibilities.

The first challenge described a cyberattack that involved someone infiltrating the organisation's IT systems and uploading a new copy of the entire digital folder structure, as well as deleting and adding a large number of documents.

Meanwhile, an investigation into the situation was under way, news starts to spread in the traditional media about leaked documents revealing that a manager within the organisation had misused large sums of money or had otherwise been acting corruptly.

Hacking and leaking documents often carry symbolic value as they can expose injustices that are otherwise concealed from the public. The narrative for the challenge was that all levels of society are corrupt, and public institutions cannot be trusted.

The second challenge continued with the same narrative of distrust in public institutions and corruption. This time a deep fake of the prime minister of Sweden was circulated on social media, announcing in a press conference that the organisation was part of a corruption scandal.

Subsequently, there was a surge of hatred and threats towards the organisation and its staff, leading to sabotage against some of the organisation's facilities.

Forgeries

Fabricating official documents is an effective way of making disinformation appear authentic. For example, fake letterheads, stamps, and signatures can be used to produce forged documentation.

Leaks

Leaking can consists of releasing information that has been obtained by illegitimate means. This carries symbolic weight as leakers traditionally reveal injustices and cover-ups unknown to the public. However, when used as an information influence activity, leaked information is taken out of context and is used to discredit actors and distort the information environment. Leaked information is sometimes obtained through hacking or theft.

Challenge three described an international nuclear incident that could potentially spread some radioactivity to northern Europe, but with smaller particles that would not cause significant impact.

False experts disseminated misinformation claiming that the authorities were lying to the public to avoid causing panic.

This created a substantial information demand among the population, who were trying to find factual recommendations and advice, which is challenging when truth is mixed with lies and disinformation.

The report has the title "Enhancing Organisational Capability: A Tailored Approach with Red Team vs Blue Team Adapted Workshops", a workshop methodology for developing increased capability against information influence operations, prepared and published by the NATO Strategic Communications centre of Excellence (StratCom COE).

Read more at number 8 below. Welcome to the Top 10 list.

Best regards,

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

Number 1 (Page 6)

Commission sends request for information to LinkedIn on potentially targeted advertising based on sensitive data under Digital Services Act

European Commission

Number 2 (Page 8)

Stronger Fraud Risk Management Could Improve the Integrity of the Trademark System

United States Government Accountability Office
GAO
Report to Congressional Committees

Number 3 (Page 11)

Digital finance - does it change the trade-off between risk and resilience?
Prof Claudia Buch, Chair of the Supervisory Board of the European Central Bank, at "The Future of Digitalization and Finance" symposium, organised by the Deutsche Bundesbank, Frankfurt am Main.

Number 4 (Page 17)

FCC Proposes Cybersecurity Labeling Program for Smart Devices

Federal Communications Commission

Number 5 (Page 19)

Department of Commerce, Department of the Treasury, and Department of Justice Tri-Seal Compliance Note
Obligations of foreign-based persons to comply with U.S. sanctions and export control laws

Number 6 (Page 21)

Commission Delegated Regulation establishing a network code on sector-specific rules for cybersecurity aspects of cross-border electricity flows

EUROPEAN COMMISSION

Number 7 (Page 24)

SXSW Panel Replay: Real or Not, Defending Authenticity in a Digital World

Experts from DARPA, Google, Graphika, and LinkedIn speak with CNN at SXSW 2024 about how to address the growing threat posed by deepfakes

DARPA DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

Number 8 (Page 26)

Enhancing Organisational Capability: A Tailored Approach with Red Team vs Blue Team Adapted Workshops

A workshop methodology for developing increased capability against information influence operations

Number 9 (Page 30)

Browse safely with real-time protection on Chrome

Google

Number 10 (Page 32)

World War II Slogan is Crucial to Preventing Unauthorized Disclosure in 2024 - DITMAC Team Working to Reduce Unauthorized Disclosures, Training DOD Workforce

Story by John Joyce, Defense Counterintelligence and Security Agency

dvids DEFENSE VISUAL INFORMATION DISTRIBUTION SERVICE

Number 1

Commission sends request for information to LinkedIn on potentially targeted advertising based on sensitive data under Digital Services Act

The European Commission has formally sent LinkedIn a request for information under the Digital Services Act (DSA), asking for more details on how their service complies with the prohibition of presenting advertisements based on profiling using special categories of personal data.

LinkedIn must provide the requested information by 5 April 2024. Based on the assessment of LinkedIn's reply, the Commission will assess next steps.

A request for information is an investigatory act that does not prejudge potential further steps the Commission may or may not decide to take. However, pursuant to Article 74 (2) of the DSA, the Commission can impose fines for incorrect, incomplete, or misleading information in response to a request for information.

Main establishment of the provider in the EU	**LinkedIn Ireland Unlimited Company**
Designated service	**LinkedIn**
Type of service under DSA	Very large online platform
Average monthly active users in millions*	Logged-in active users: 45.2 Logged-out site visits: 132.5
Digital Services Coordinator as of 17 February 2024	Ireland
DSA enforcement actions	• 25.04.2023: designation (Commission decision .pdf; press release) • 18.01.2024: request for information (press release) • 14.03.2024: request for information (press release)

Following the designation as a very large online platform in April 2023, LinkedIn is required to comply with the full set of provisions introduced by the DSA, including the obligation to enable users to identify basic information about the nature and origins of an advertisement and the ban on presenting advertisements based on profiling using special categories of personal data, such as sexual orientation, political opinions, or race.

This enforcement action is based on a complaint submitted to the Commission by civil society organisations:
https://edri.org/our-work/civil-society-complaint-raises-concern-that-linkedin-is-violating-dsa-ad-targeting-restrictions/

To read more:
https://digital-strategy.ec.europa.eu/en/news/commission-sends-request-information-linkedin-potentially-targeted-advertising-based-sensitive-data#:~:text=The%20European%20Commission%20has%20formally,special%20categories%20of%20personal%20data.

Number 2

Stronger Fraud Risk Management Could Improve the Integrity of the Trademark System

United States Government Accountability Office

Report to Congressional Committees

What GAO Found

The Trademark Modernization Act of 2020 (TMA) established two new procedures—expungement and reexamination—that allow individuals and businesses to challenge a registered trademark on the basis that it was not used in commerce, as is normally required. A successful challenge results in the trademark being removed from the register, thus making it available for potential use for the challenger or other applicants.

GAO found that from December 2021 through June 2023 the U.S. Patent and Trademark Office (USPTO) and attorneys representing trademark owners filed nearly 500 petitions under the new procedures.

Fraudulent Images of the Same Flashlight with Different Logos Included in Trademark Applications Submitted to USPTO

Source: GAO adaptation of U.S. Patent and Trademark Office images. | GAO-24-106533

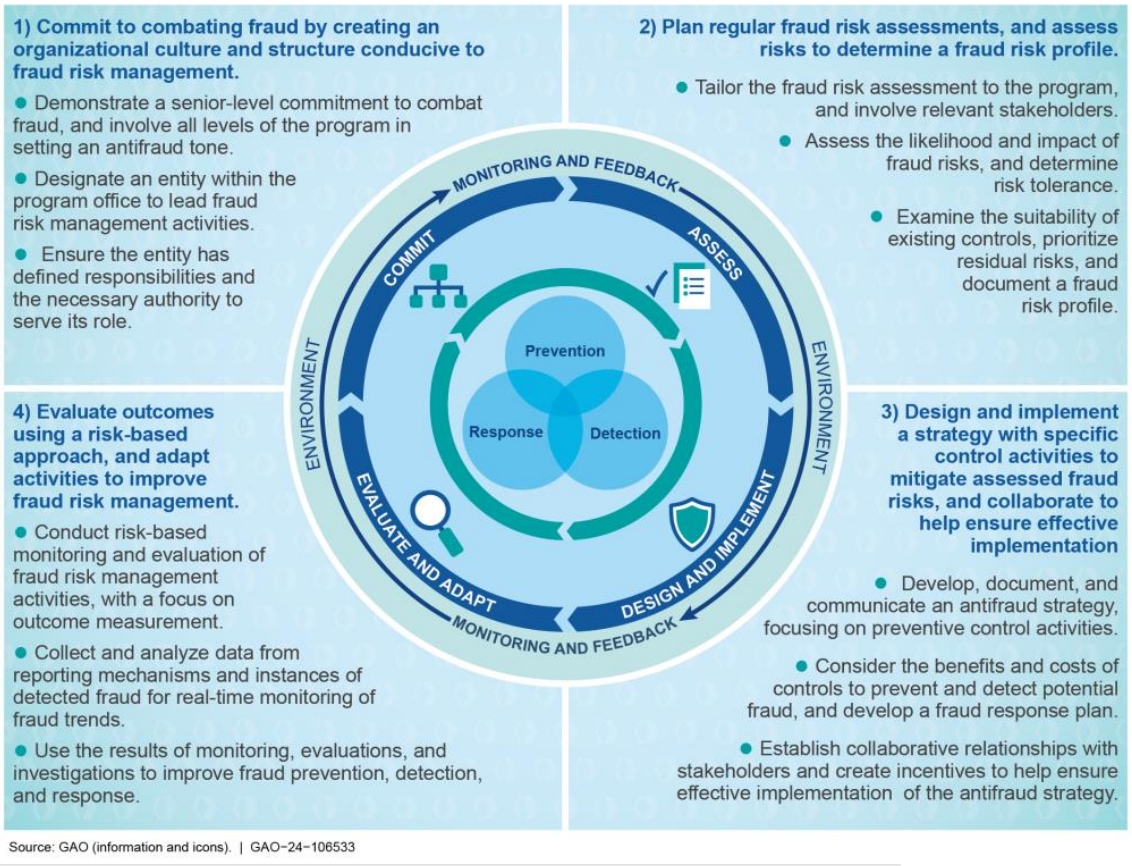
Collectively, these petitions resulted in the removal of more than 2,500 falsely claimed goods and services from the trademark register. Trademark attorneys told GAO that the new procedures can be cost-effective and low-risk.

Existing USPTO programs have also addressed inaccurate or false trademark applications and registrations. The agency's post registration audit program removed trademarked goods and services in about half of its randomly selected audits each year from the start of the program in 2017. This suggests that there may be more than 1 million false and inaccurate registrations out of about 2.8 million overall due to an influx of applications, among other factors.

The USPTO has taken steps to limit fraud risks, such as establishing a culture conducive to fraud risk management. However, the USPTO has not conducted a comprehensive fraud risk assessment of the trademark register or designed a fraud risk strategy. Implementing leading practices from GAO's Fraud Risk

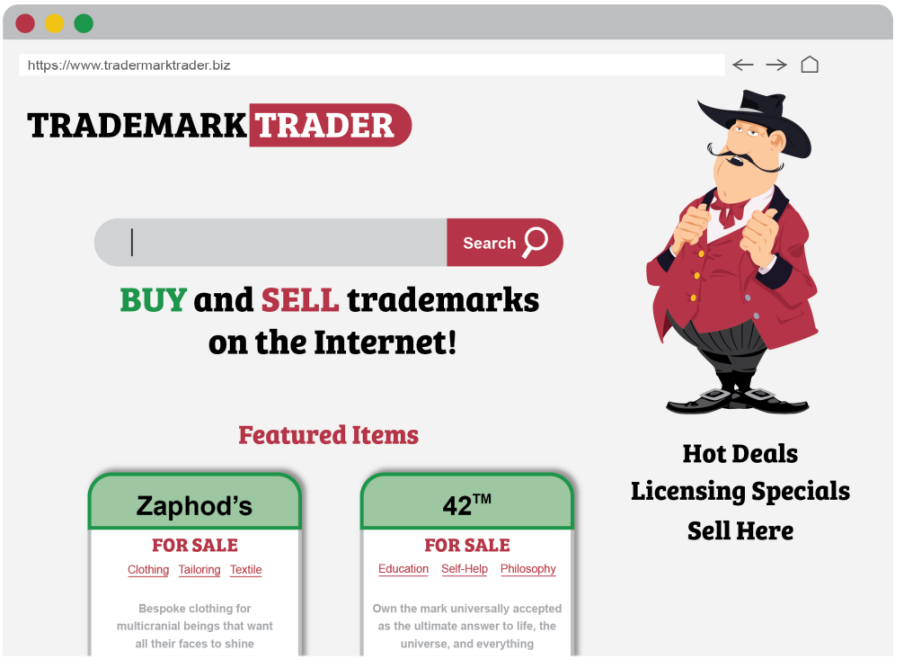
Framework would allow the USPTO to comprehensively consider fraud risks, establish more effective controls, and fully articulate a tolerable level of fraud risk while considering the costs and benefits of potential control activities.

Figure 3: GAO Fraud Risk Management Framework



Source: GAO (information and icons). | GAO-24-106533

Figure 8: Illustrative Example of a Fictitious Trademark Auction Site



Source: GAO (data); Alexandr Sidorov/stock.adobe.com (images). | GAO-24-106533

GAO also found that the USPTO's current data systems do not allow the agency to:

(1) assess the effectiveness of current trademark fraud prevention programs and

(2) implement new technologies for identifying fraud.

Academics told GAO that computational tools such as predictive analytics could help the USPTO identify trademark applications with false or inaccurate information more effectively.

To read more: https://www.gao.gov/assets/d24106533.pdf

Number 3

Digital finance - does it change the trade-off between risk and resilience?

Prof Claudia Buch, Chair of the Supervisory Board of the European Central Bank, at "The Future of Digitalization and Finance" symposium, organised by the Deutsche Bundesbank, Frankfurt am Main.

Thank you very much for organising this symposium on “The Future of Digitalization and Finance”. I am very grateful and honoured that it coincides with the farewell event for Joachim Wuermeling and me. I would like to thank the distinguished panellists for accepting the invitation to speak here today and I would like to thank all of you for coming.

First and foremost, I would like to thank all the dear colleagues here at the Bundesbank with whom I have worked closely over many years. Our work together has shaped my thinking about the banking and financial system, financial stability, the key role of our institutions in Europe and beyond, and the essential role of central banks in contributing to financial stability and the welfare-enhancing integration of financial markets. In today’s uncertain world, this is more important than ever.

I would like to thank you wholeheartedly for the great cooperation, and I am proud of what we have achieved together.

But the almost ten years that I spent at the Bundesbank as its Vice-President were in fact neither the beginning nor the end of our cooperation. Since the early 2000s, I have worked closely with the Bundesbank on many research projects, and in my new role as Chair of the Supervisory Board of the ECB, I will continue to work with all of you.

Dealing with today’s topic – the implications of digitalisation and its impact on the stability of banks – remains our joint responsibility within the Eurosystem.

Today’s banks operate in an environment which looks radically different to how it looked 30 years ago, due in no small part to the transformative impact of digitalisation.

The digital revolution, along with the rise of artificial intelligence, has the potential to fundamentally affect the key functions that banks perform in the economy. Reducing information asymmetries, mitigating moral hazard, and leveraging their unique position to provide deposit-taking and lending services – these functions determine banks' franchise value and their role in the financial system.

This raises three important questions.

First, are we now witnessing a technological breakthrough in the provision of financial services? Remember what Paul Volcker said in 2009, "The most important financial innovation that I have seen the past 20 years is the automatic teller machine".

Second, how does digitalisation affect banks' risk/return trade-off? Does it lead to more competition and compression of margins, which induces a search for yield, which can in turn destabilise the financial system? Or are there counterbalancing forces that allow banks to better manage risks?

Third, what is the correct regulatory response to these trends? In my view, close cooperation across countries and sectors and addressing sources of systemic risk are key elements of the regulatory response.

We certainly won't be able to answer all these questions today, but I am very much looking forward to the panel discussion.

The changing landscape of competition in banking

The banking sector has undergone a significant transformation over the past 30 years. Let me highlight three shifts that have changed the landscape of competition in banking.

First, the internationalisation of banks has proceeded at a rapid pace. Let me give a European example. Today, international banks have a significant presence in central and eastern Europe, a development that was driven by deregulation and privatisation. This marks a stark contrast to the early 1990s when central and eastern European countries began opening up.

Historically, foreign banks primarily expanded overseas to follow their corporate customers. Outside of financial centres, their market shares were largely confined to trade-related business. But now, the landscape has transformed significantly; both international trade and international finance have seen considerable growth, facilitating the entry of foreign banks into new markets.

Second, banks are facing increased competition, particularly since the global financial crisis. This competition has come from non-bank financial institutions (NBFIs) such as investment funds, insurance companies and peer-to-peer lenders, but also from bigtech firms and fintech start-ups.

Several factors have driven this trend, including stricter regulation of banks and a growing demand for different or more innovative financial services. While bigtech firms have leveraged their massive user bases, technological expertise and data analytics capabilities to offer services, fintech start-ups have often been at the forefront of financial innovation.

Third, the digitalisation of financial services does indeed mark a pivotal point in the banking sector's development. The digital transformation is not just changing

the types of services offered but it is also redefining how these services are delivered and consumed. Digitalisation is changing the way in which financial services can be bundled together.

The key complementary services of the future may not be deposit taking and lending, but financial institutions may obtain a comparative advantage in terms of the information available from online commercial activity and social media. Digitalisation also reduces the cost of providing cross-border financial services, reducing the need for a physical presence in foreign markets, which may in fact benefit integration.

How does digitalisation affect the stability of banks?

What does the digitalisation of financial services imply for supervisors and regulators? Not only is the jury still out on whether digitalisation increases or decreases the degree of competition in the provision of financial services. There is also no clear answer as to how competition affects stability and how it affects the risk/return trade-off in the banking system.

On the one hand, forces that restrict competition may increase stability. Weak competition generates monopoly rents, which banks may want to protect by investing in safer assets. On the other hand, instabilities may increase in less competitive markets, as banks with greater market power can set higher interest rates, which may lead to borrowers opting for riskier projects, thus resulting in banks becoming riskier. Empirical studies actually show that the risk/return trade-off in banking depends on the types of risk (portfolio risk, insolvency risk, liquidity risk, systemic risk) and the business model being considered (retail versus wholesale banks).

How do the trends that we have seen over the past 30 years change the risk/return trade-off?

Let's take internationalisation first. The internationalisation of banking facilitates a more efficient diversification of risk. By operating across different countries, banks can spread their exposures over a wider array of economic environments and sectors.

International banking operations can achieve a more stable return on investments by leveraging this lack of perfect correlation between different markets. On the flip side though, the internationalisation of banking creates avenues for easier spillover of financial shocks from one country to another.

In a highly interconnected global banking network, stress in one country's banking sector can quickly affect financial institutions and markets in other countries. Shocks can ripple through the international banking system, affecting banks with exposure to that market through losses on investments or reduced confidence among depositors and investors.

The banking union that was established ten years ago is a response to the potentially adverse effects of integration and, at the same time, a channel through

which sustainable integration can be enhanced. The global financial crisis and the euro area sovereign debt crisis exposed significant vulnerabilities within the European banking sectors as well as the inadequacy of national supervisory frameworks to manage cross-border banking risks.

With the start of the Single Supervisory Mechanism (SSM) in 2014, whereby the ECB assumed direct supervision of significant banks in participating countries, common supervisory standards were established and enforced.

This ensures consistent supervision and a more holistic monitoring of the cross-border activities and exposures of banks within the SSM, supporting the integration of the European banking market. The ECB's Annual Report on Supervisory Activities 2023 provides insights into the measures taken to enhance the resilience of the European banking sector.

Changes in competition through the growth of NBFIs likewise affect the stability of banks, with both beneficial diversification of risks and the introduction of new channels of contagion. On the positive side, increased competition from NBFIs can lead to a more diversified financial system.

Diversification can spread risks across a wider array of institutions with different abilities to bear these risks. The system as a whole can become more resilient to shocks. However, competition from NBFIs introduces new vulnerabilities, particularly related to liquidity risk and high leverage, and it may increase incentives to take risk.

Reliance on short-term funding makes NBFIs susceptible to liquidity squeezes, whereby they may be forced to sell assets at depressed prices and potentially triggering a downward spiral in asset prices.

Furthermore, the interconnectedness between banks and NBFIs means that distress in the non-bank sector can quickly transmit to banks through direct exposures, common asset holdings, and market sentiment. An important way in which banks can mitigate this risk is by investing more in the assessment and management of the risks of their non-bank counterparties.

Finally, digitalisation affects risks and return in banking. On the one hand, digitalisation may expose banks to new risks such as cyberattacks and a high dependency on third-party providers.

Cyber threats can compromise data integrity, privacy and the overall operational continuity of banks. The ECB is currently conducting a cyber resilience stress test on 109 directly supervised banks to assess how banks respond to and recover from a cyberattack.

Similarly, dependency on a limited number of technology providers for critical services can introduce significant systemic risks if any of these providers fail or experience disruptions. The Digital Operational Resilience Act (DORA) thus provides supervisory authorities with more competences for the oversight and supervision of banks' outsourcing activities.

On the other hand, a higher concentration within the financial sector, often a consequence of digital transformation, may imply higher profitability and the ability to build larger buffers against risks. Moreover, by cooperating with fintech firms and integrating innovative solutions, banks may also benefit from a more efficient provision of their financial services.

Regulatory responses to the digitalisation of financial services

The current prudential framework for the regulation of banks is designed to be technologically neutral, recognising that regulators and supervisors do not have superior knowledge to market participants regarding the most effective technological solutions. But this certainly does not imply that we should ignore technology. Instead, we need to understand the impact of digitalisation on risks in the financial system and respond to potentially destabilising forces.

Digitalisation certainly reinforces the need for policy and supervisory coordination, both across countries and sectors. Bank risks never stopped at borders, but the digitalisation of financial services certainly affects the speed and nature of shock transmission.

The Financial Stability Board (FSB), reinvigorated since the global financial crisis, thus plays a crucial role in coordinating international efforts to monitor and address the financial stability risks posed by digitalisation. Similarly, the Basel Committee on Banking Supervision (BCBS) has been instrumental in setting global standards for the prudential regulation of banks, adapting these standards to account for the digitalisation of financial services.

Both the FSB and the BCBS have established frameworks for the evaluation of regulatory policies, which are crucial for the accountability and transparency of supervisors and regulators. In Europe, the push for better coordination has led to significant progress towards a banking union as well as to the call for a capital markets union. Both a banking union and a capital markets union are essential steps in creating a more integrated and resilient financial system.

In this cooperation, systemic risks arising from digitalisation and from changes in the provision of financial services need to be addressed. After the global financial crisis, stricter regulations were imposed on banks to reduce the likelihood and impact of future crises.

The reforms aimed to bolster the resilience of banks by enhancing their capitalisation, thus enabling them to better absorb losses and reduce systemic risk. Reforms also tackled the "too-big-to-fail" issue by imposing higher capital requirements on large, systemically important banks and enhancing mechanisms for their recovery and resolution, lessening the financial burden on taxpayers in case of bank failures.

We similarly need to address systemic risks arising from non-banks. NBFIs, much like banks, play a crucial role in the global financial ecosystem, engaging in activities that affect liquidity flows and market functioning both domestically and internationally.

Like banks, non-banks need sufficient resilience to reduce the likelihood of distress and to mitigate the amplification of shocks, taking a systemic perspective rather than focusing solely on individual institutions.

While crypto-assets are not systemically relevant at present due to their small market capitalisation, history teaches us to be vigilant. The task at hand for regulators involves a comprehensive assessment of potential future systemic risks, requiring preventive regulation to address these risks before they materialise.

This involves close monitoring, international cooperation to close regulatory gaps, and a concerted effort to prevent regulatory arbitrage. In this sense, the Markets in Crypto-Assets (MiCa) regulation is a key European response to the provision of crypto-related services.

Finally, an emerging challenge in the digital financial landscape is the blurring of lines between policy areas. Digital financial services often cut across traditional sectoral boundaries, combining elements of banking, investment and insurance services, etc.

Policies aimed at fostering innovation in financial technologies can thus have significant implications for several policy areas. Hence, prudential supervisors not only need to coordinate with each other, but also with competition authorities to understand the dynamic market forces at play.

This coordination is crucial for ensuring that the drive towards digitalisation and the resulting market concentration, not least due to the market power of third-party providers of financial services, do not undermine financial stability.

To read more:
https://www.bankingsupervision.europa.eu/press/speeches/date/2024/html/ssm.sp240322~7bbfe50962.en.html

Number 4

FCC Proposes Cybersecurity Labeling Program for Smart Devices

A voluntary cybersecurity labeling program providing consumers with clear information about the security of their internet-enabled devices, commonly called "Internet of Things" (IoT) or "smart" devices.

Federal Communications Commission **FCC 24-26**

Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Cybersecurity Labeling for Internet of Things	)	PS Docket No. 23-239
	)	

REPORT AND ORDER
AND
FURTHER NOTICE OF PROPOSED RULEMAKING

Adopted: March 14, 2024 **Released: March 15, 2024**

Comment Date: (30 days after date of publication in the Federal Register)
Reply Comment Date: (60 days after date of publication in the Federal Register)

By the Commission: Chairwoman Rosenworcel and Commissioners Starks, Simington, and Gomez issuing separate statements.

Consumers rely heavily on Internet-connected products to help them manage many aspects of day-to-day life, including home safety, health, recreation, and personal convenience.

With this convenience, however, comes risk. Internet of Things (IoT) products are susceptible to a wide range of relatively common security vulnerabilities that are increasingly exploited by cybercriminals who are invading people's privacy and threatening national security.

With this Report and Order (Order), the Commission takes prompt and decisive measures to strengthen the nation's cybersecurity posture by adopting a voluntary cybersecurity labeling program for wireless Internet of Things products.

The Commission's IoT Labeling Program will provide consumers with an easy-to-understand and quickly recognizable FCC IoT Label that includes the U.S. government certification mark (referred to as the Cyber Trust Mark) that provides assurances regarding the baseline cybersecurity of an IoT product, together with a QR code that directs consumers to a registry with specific information about the product.

Consumers who purchase an IoT product that bears the FCC IoT Label can be assured that their product meets the minimum cybersecurity standards of the IoT Labeling Program, which in turn will strengthen the chain of connected IoT products in their own homes and as part of a larger national IoT ecosystem.

Today's Order will help consumers make better purchasing decisions, raise consumer confidence with regard to the cybersecurity of the IoT products they buy to use in their homes and their lives, and encourage manufacturers of IoT products to develop products with security-by-design principles in mind.

In the following Order, we set forth the framework by which the IoT Labeling Program will operate. We focus the IoT Labeling Program initially on IoT "products," which we define to include one or more IoT devices and additional product components necessary to use the IoT device beyond basic operational features.

Recognizing that a successful voluntary IoT Labeling Program will require close partnership and collaboration between industry, the federal government, and other stakeholders, we adopt an administrative framework for the IoT Labeling Program that capitalizes on the existing public, private, and academic sector work in this space, while ensuring the integrity of the IoT Labeling Program through oversight by the Commission.

To read more:
https://www.fcc.gov/document/fcc-proposes-cybersecurity-labeling-program-smart-device

https://docs.fcc.gov/public/attachments/FCC-24-26A1.pdf

Number 5

Department of Commerce, Department of the Treasury, and Department of Justice Tri-Seal Compliance Note

Obligations of foreign-based persons to comply with U.S. sanctions and export control laws

Today's increasingly interconnected global marketplace offers unprecedented opportunities for companies around the world to trade with the United States and one another, contributing to economic growth.

At the same time, malign regimes and other bad actors may attempt to misuse the commercial and financial channels that facilitate foreign trade to acquire goods, technology, and services that risk undermining U.S. national security and foreign policy and that challenge global peace and prosperity.

In response to such risks, the United States has put in place robust sanctions and export controls to restrict the ability of sanctioned actors to misuse the U.S. financial and commercial system in advance of malign activities.

These measures can create legal exposure not only for U.S. persons, but also for non-U.S. companies who continue to engage with sanctioned jurisdictions or persons in violation of applicable laws.

To mitigate the risks of non-compliance, companies outside of the United States should be aware of how their activities may implicate U.S. sanctions and export control laws.

This Note highlights the applicability of U.S. sanctions and export control laws to persons and entities located abroad, as well as the enforcement mechanisms that are available for the U.S. government to hold non-U.S. persons accountable for violations of such laws, including criminal prosecution.

It further provides an overview of compliance considerations for non-U.S. companies and compliance measures to help mitigate their risk.

COMPLIANCE CONSIDERATIONS FOR FOREIGN-BASED PERSONS

As with any company participating in the global marketplace, foreign-based persons must ensure that they have robust compliance measures in place to avoid violating U.S. sanctions or export control laws.

In particular, companies should take care to do the following:

• Employ a risk-based approach to sanctions compliance by developing, implementing, and routinely updating a sanctions compliance program.

• Establish strong internal controls and procedures to govern payments and the movement of goods involving affiliates, subsidiaries, agents, or other counterparties. Such controls can help detect linkages to sanctioned persons or jurisdictions that may otherwise be obscured by complex payment and invoicing arrangements.

• Ensure that know-your-customer information (such as passports, phone numbers, nationalities, countries of residence, incorporation, and operations, and addresses) and geolocation data are appropriately integrated into compliance screening protocols and information is updated on an ongoing basis based on its overall risk assessment and specific customer risk rating.

• Ensure that subsidiaries and affiliates are trained on U.S. sanctions and export controls requirements, can effectively identify red flags, and are empowered to escalate and report prohibited conduct to management.

• Take immediate and effective action when compliance issues are identified, to the extent possible, to identify and implement compensating controls until the root cause of the weakness can be determined and remediated.

• Identify and implement measures to mitigate sanctions and export control risks prior to merging with or acquiring other enterprises, especially where a company is expanding rapidly and/or disparate information technology systems and databases are being integrated across multiple entities.

• Parties who believe that they may have violated sanctions or export control laws should voluntarily self-disclose the conduct to the relevant agency. Please review the Compliance Note: Voluntary Self-Disclosure of Potential Violations.

To read more: https://ofac.treasury.gov/media/932746/download?inline

Department of Commerce, Department of the Treasury, and Department of Justice Tri-Seal Compliance Note:

Obligations of foreign-based persons to comply with U.S. sanctions and export control laws

Number 6

Commission Delegated Regulation establishing a network code on sector-specific rules for cybersecurity aspects of cross-border electricity flows

This initiative was identified as an important measure to improve the resilience of critical energy infrastructure and services in Commission communications on energy system integration, the Security Union Strategy and the Cybersecurity Strategy.

It is based on the powers that the European Parliament and the Council conferred on the Commission in the Regulation (EU) 2019/9434 (Electricity Regulation) to develop sector-specific rules ('network code') that address the cybersecurity aspects of cross-border electricity flows.

This includes rules on common minimum requirements, planning, monitoring, reporting and crisis management.

The network code aims to establish a recurrent process of cybersecurity risk assessments in the electricity sector. The assessments will aim to systematically identify the entities that perform digitalised processes with a critical or high impact in cross-border electricity flows, their cybersecurity risks and the necessary mitigating measures that they need to implement.

Multiple methodologies and standards exist today in the cybersecurity industry. Moreover, it is a fast-evolving knowledge field. With the objective of harmonising and ensuring a common baseline while respecting existing practices and investments as much as possible, the network code therefore establishes a governance model to develop, follow and regularly review the methodologies of different stakeholders.

This governance and stakeholder contribution model takes into account the current mandates of different bodies in both the cybersecurity and electricity regulatory systems.

As technology is constantly evolving and the electricity sector is undergoing rapid digitalisation, the network code therefore strives not to be detrimental to innovation and not to constitute a barrier to new entities accessing the electricity market and the subsequent use of innovative solutions that help make the electricity system more efficient.

As part of this objective, all new systems, processes and procedures must respect cybersecurity requirements. In order to identify new trends and possible future risks in cybersecurity, regular reporting will occur with the comprehensive cross-border electricity cybersecurity risk assessment report, provided for in the network code and carried out at least every 3 years.

The measures envisaged in the network code are important for improving the security of electricity supply in the EU.

This delegated Regulation will lay down harmonised rules applicable to all relevant operators in all Member States. It will aim to reach the objectives, while ensuring a level playing field. It will further help integrate the EU electricity market in a non-discriminatory manner and ensure effective competition.

The objectives of this initiative cannot be achieved at national level as it focuses on crossborder electricity flows and refers to interconnected energy networks across Europe.

This Regulation aims at:

• establishing rules concerning the governance of cybersecurity aspects of cross-border electricity flows to ensure the reliability of the electricity system and the close collaboration with existing governance structures for cybersecurity;

• determining common criteria for performing cybersecurity risk assessments for the operational reliability of the electricity system with regard to cross-border electricity flows;

• promoting a common electricity cybersecurity framework and by that fostering a common minimum electricity cybersecurity level across the Union;

• providing for mechanisms in order to assess the application of the minimum and advanced cybersecurity controls on systems that can affect cross-border electricity flows;

• establishing information flows by establishing rules for the collection and sharing of information in relation to cross-border electricity flows, compatible with other national and EU legislation;

• establishing effective processes to identify, classify and respond to cyber-attacks impacting the cross-border flows of electricity;

• setting up effective processes for the management of cross-border electricity crises related to cyber-attacks;

• defining common principles for electricity cybersecurity exercises to increase resilience and improve the risk preparedness of the electricity sector;

• protecting the information exchanged under this Regulation;

• determining a process for monitoring the implementation of this Regulation, to assess the effectiveness of investments in cybersecurity protection and to report on the progress of cybersecurity protection across the Union; and

• ensuring that the recommendations on the cybersecurity procurement specifications with relevance for cross-border electricity flows are not detrimental to innovation, new systems, processes and procedures.

To read more:
https://energy.ec.europa.eu/document/download/c7580561-4ced-4011-b63e-e1482a83c7b1_en?filename=Delegated%20Act%20on%20the%20new%20Network%20Code%20on%20Cybersecurity_draft.pdf

Number 7

SXSW Panel Replay: Real or Not, Defending Authenticity in a Digital World

Experts from DARPA, Google, Graphika, and LinkedIn speak with CNN at SXSW 2024 about how to address the growing threat posed by deepfakes

DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

Have you ever wondered if that video you're watching, the photo you're looking at, or even that person on the other line is the real deal?

Deepfakes aren't just Hollywood magic anymore—they're part of our everyday lives, found in everything from the news we consume to the memes we share.

During this panel, experts dive into the world of deepfakes to break down the impacts of digital deception and what we can do about it.

Industry, government, and academic leaders discussed how new analytical tools — including those developed by DARPA's Semantic Forensics program — can help organizations and individuals protect themselves against manipulated media.

Speakers included:

- Donie O'Sullivan (moderator), Politics and Technology Correspondent, CNN
- Wil Corvey, Semantic Forensics Program Manager, DARPA
- Matt Turek, Deputy Director, Information Innovation Office, DARPA
- Nick Dufour, Misinformation Mitigation Researcher, Google
- Amruta Deshpande, Senior Research Scientist, Graphika
- James Verbus, Senior Staff Machine Learning Engineer, LinkedIn

DARPA recently announced its analytic catalog of open-source resources developed under SemaFor for use by researchers and industry. As capabilities mature and become available, they will be added to this repository.

The agency also launched the AI Forensics Open Research Challenge Evaluation (AI FORCE). This open community research effort invites participants to contribute their expertise in developing innovative and robust machine learning, or deep learning, models that can accurately detect synthetic AI-generated images.

Through a series of mini challenges, AI FORCE asks participants to build models that can discern between authentic images, including ones that may have been

manipulated or edited using non-AI methods, and fully synthetic AI-generated images.

To read more: https://www.darpa.mil/news-events/2024-03-26

https://www.youtube.com/watch?v=8zniAjqWI2A

Number 8

Enhancing Organisational Capability: A Tailored Approach with Red Team vs Blue Team Adapted Workshops

A workshop methodology for developing increased capability against information influence operations

The purpose of the report is to present a method for exploring an actor's possibilities for countermeasures and capabilities against information influence operations (IIO).

Using specific scenario conditions, the method assists in creating a discussion on what capabilities are needed and how organisations can develop these capabilities based on available resources.

The method involves conducting workshops using a red team versus blue team exercise which has been adapted to generate a gap analysis for countermeasures in countering IIO.

The report provides guidance on preparing for a workshop aimed at identifying vulnerabilities in an organisation's information environment and developing effective strategies to mitigate the consequences of IIO.

The workshops create a common problem understanding from a scenario and challenges chosen beforehand.

The end result is an analysis that includes existing capabilities in the organisation, a reflection on how to develop capability activities and functions further, and prioritising between these.

The report concludes that the workshop method is a useful tool for risk assessment and preparedness planning, and can be used for decision-making and operational development.

While countering IIO is often a national-level responsibility, we argue that all parts of society can be affected by IIO and should develop capabilities to counter disinformation. Therefore, the selected workshop method can be adapted to work on a local, regional, or national level.

Anticipating disinformation requires proactive capabilities and activities such as risk and threat assessments, forecasting, contingency planning, and policy development to increase preparedness.

Recognising disinformation requires both proactive and reactive functions, including monitoring capabilities and documentation to create indications for recognition.

Reactive functions include impact assessment and investigation into negative impacts on public discourse.

To recognise disinformation campaigns, organisations can monitor social media and set up systems for reporting suspicious activity.

Adapting includes both proactive and reactive functions. Proactively, organisations can prevent and mitigate disinformation by increasing media literacy, creating public awarenes s, and developing partnerships.

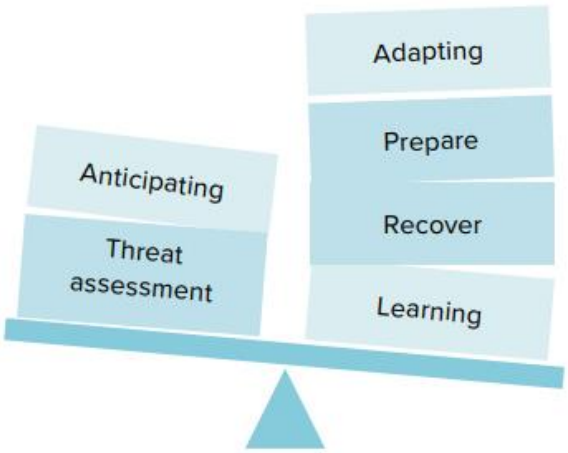
They can also prepare for potential threats by establishing partnerships and publishing relevant analysis.

Reactively, organisations can respond to disinformation by using counter-branding, fact checking, debunking, and counter-messaging.

Recovery may involve publishing analysis, conducting post-incident reviews, and developing strategies to rebuild trust and repair damage to reputation or public trust.

Learning is mainly a reactive function done over time in response to events or specific activities.

To improve continuously, organisations can conduct regular research and analysis, implement training programmes, create evaluation structures, and share best practices with others, feeding back into the cycle, leading back to "Anticipation".



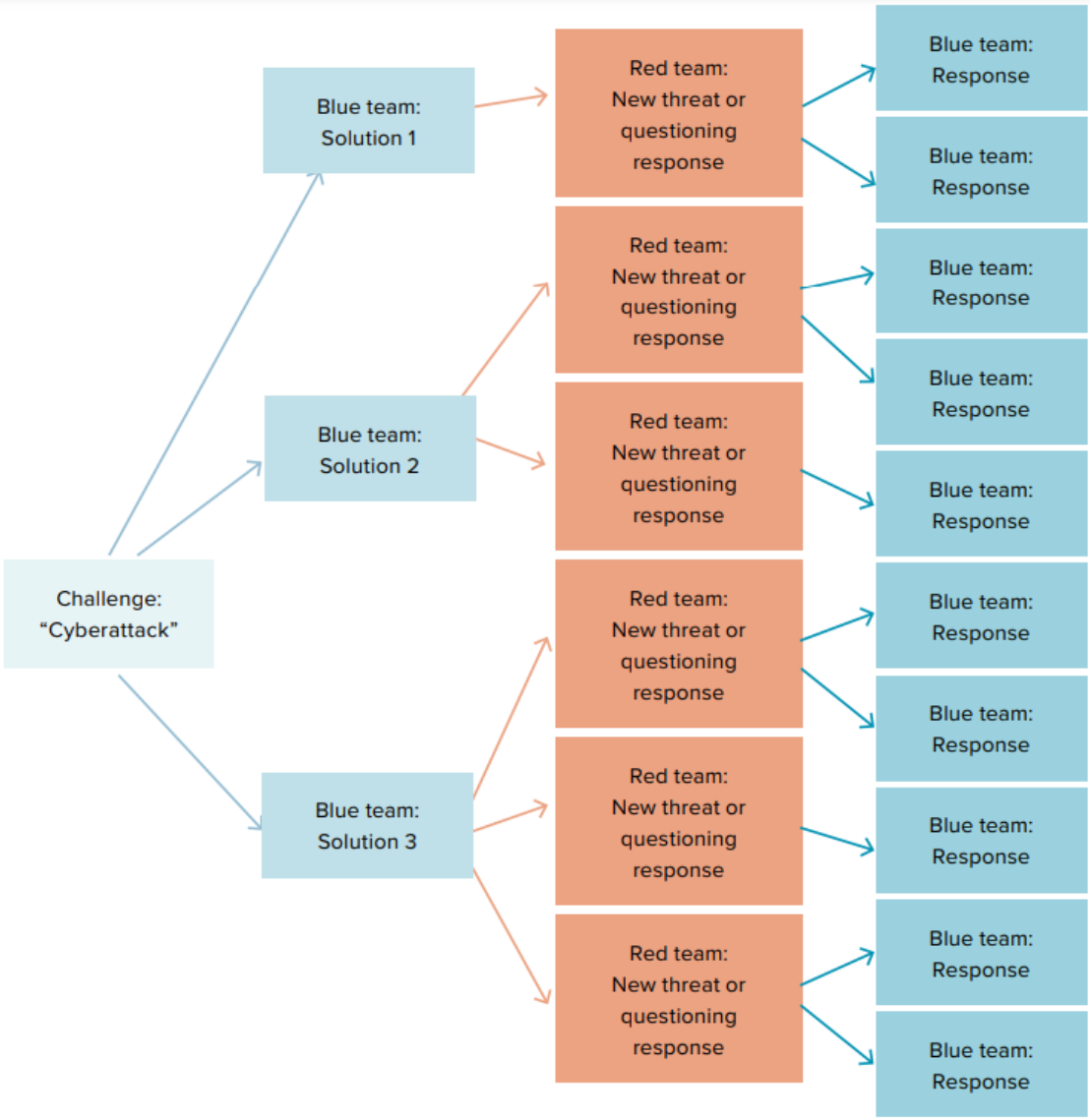


Figure 3. This flowchart demonstrates the team discussions and how they typically progress. Additionally, it serves as a method for organising discussions on a whiteboard to facilitate documentation and analysis.

To read more:
https://stratcomcoe.org/publications/enhancing-organisational-capability-a-tailored-approach-with-red-team-vs-blue-team-adapted-workshops/299

Number 9

Browse safely with real-time protection on Chrome

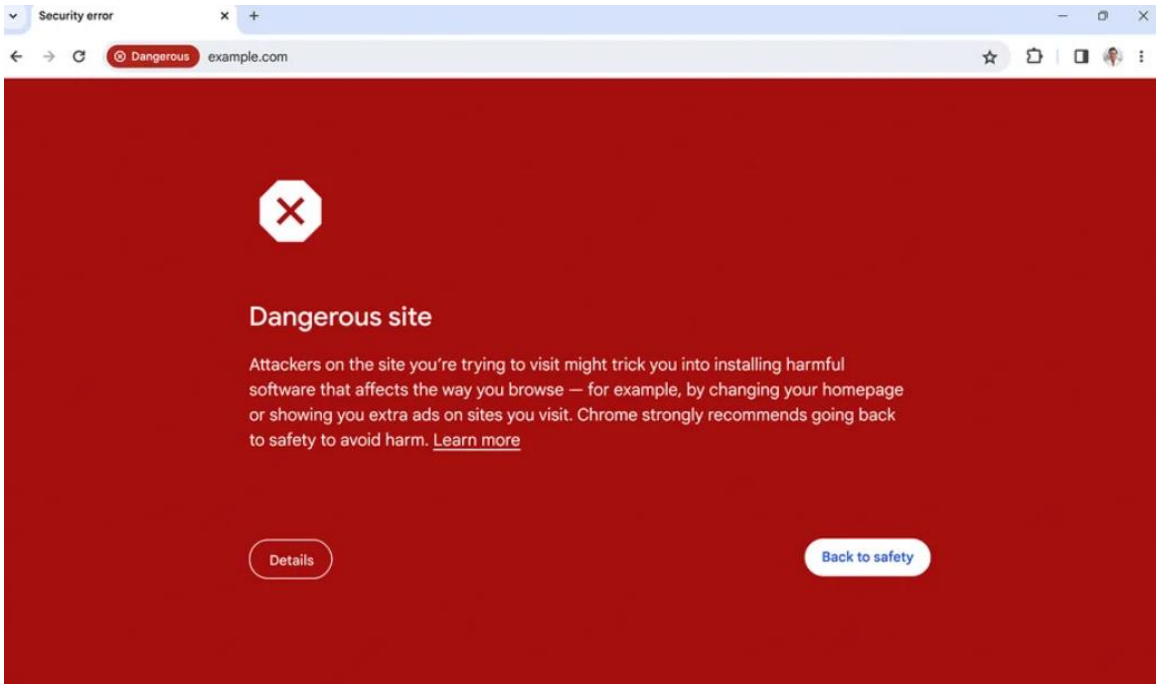
Google

Cybersecurity attacks are constantly evolving, and sometimes the difference between successfully detecting a threat or not is a matter of minutes. To keep up with the increasing pace of hackers, we're bringing real-time, privacy-preserving URL protection to Google Safe Browsing for anyone using Chrome on desktop or iOS. Plus we're introducing new password protections on Chrome for iOS as another way to help you safely navigate the web.

Real-time protection through Safe Browsing

Safe Browsing already protects more than 5 billion devices worldwide, defending against phishing, malware, unwanted software and more. In fact, Safe Browsing assesses more than 10 billion URLs and files every day, showing more than 3 million user warnings for potential threats.

Previously, the Standard protection mode of Safe Browsing used a list stored on your device to check if a site or file was known to be potentially dangerous. That list is updated every 30 to 60 minutes — but we've found that the average malicious site actually exists for less than 10 minutes.



So now, the Standard protection mode for Chrome on desktop and iOS will check sites against Google's server-side list of known bad sites in real time. If we suspect a site poses a risk to you or your device, you'll see a warning with more

information. By checking sites in real time, we expect to block 25% more phishing attempts.

The new capability — also rolling out to Android later this month — uses encryption and other privacy-enhancing techniques to ensure that no one, including Google, knows what website you're visiting. While this does require some additional horsepower from the browser, we've worked to make sure your experience remains smooth and speedy.

If you want even more protection, you can always turn on Safe Browsing's Enhanced Protection mode, which uses AI to block attacks, provides deep file scans and offers extra protection from malicious Chrome extensions.

To read more:
https://blog.google/products/chrome/google-chrome-safe-browsing-real-time/

Number 10

World War II Slogan is Crucial to Preventing Unauthorized Disclosure in 2024 - DITMAC Team Working to Reduce Unauthorized Disclosures, Training DOD Workforce

Story by John Joyce, Defense Counterintelligence and Security Agency

dvids
DEFENSE VISUAL INFORMATION DISTRIBUTION SERVICE

It was World War II and the "loose lips sink ships" slogan sprang up throughout the United States from billboards and posters to Hollywood productions advising Americans in the military, government, industry and the public to prevent inadvertent disclosure of important information to the enemy.

"It's just as true and crucial today as it was throughout World War II," said Andy Rovnak, DOD Unauthorized Disclosure Program Management Office (UDPMO) chief.

Rovnak was reflecting on how the U.S. Office of War Information's campaign to protect critical information focused on specific rules of conduct established to protect strategic military plans, national security, the American people, and warfighters deployed on two fronts and around the globe.

"Deterring, detecting and mitigating unauthorized disclosure is everyone's responsibility – it's our military, government and civic duty," said Rovnak in a February 2024 interview with DCSA Gatekeeper magazine.

"We've got to be very careful in what we say and do. We're not just talking on the phone – we're on cyber while people are trying to compromise the integrity of our networks and our cyber capability. It's where we are right now in the state of the world, and we must avoid any release of classified or secure information which could damage our national security."

Rovnak leads the UDPMO team – one of several DCSA counter insider threat teams comprising the DOD Insider Threat Management and Analysis Center (DITMAC) – in their efforts to help prevent unauthorized disclosure or leaks of non-public information, crucial to maintaining the nation's security, personnel safety and public trust.

"The 'loose lips sink ships' campaign also applies to the unauthorized disclosure of sensitive unclassified information," he said. "Although unclassified, this sensitive material could enable our adversaries and any potential adversaries to identify and exploit vulnerabilities. It would allow them to steal and use our intellectual property and technology against us, leading to an increased risk of mission failure and potential loss of life."

An unauthorized disclosure occurs when trusted individuals inside an organization communicates or physically transfers classified national security

information or controlled unclassified information — including Operations Security critical information and indicators — to an unauthorized recipient.

“There are multiple threats out there and we’re losing intellectual property to unauthorized recipients,” said Rovnak, pointing out that recipients span external threats such as nation state actors to criminal entities who target the federal government, defense industrial base and American citizens.

“If information in the care of government on behalf of its citizens to protect the nation is exposed – someone will take advantage of it. The same is true with personal information. The technological revolution and transformation into a digital society since the World War II era resulted in a fragility in how we operate from an information standpoint that didn't exist back then. Someone without nation-state capabilities can interfere and cause a significant amount of damage. They're able to get the information quicker now and turn it around faster against us. If someone knows about a vulnerability, that person can use ChatGPT and write code that may go out to exploit that vulnerability.”

This knowledge released through an unauthorized disclosure of classified information or controlled unclassified information (CUI) can happen in various ways.

It could be disclosed intentionally, negligently or inadvertently through leaks, data spills, espionage and improper safeguarding of national security information.

When classified information is involved, unauthorized disclosure can be categorized as a type of threat or security incident, characterized as an infraction or violation depending on the seriousness of the incident.

“My UDPMO team coordinates the reporting of unauthorized disclosures within the Department of Defense to ensure prompt and complete delivery of case referrals to the Department of Justice and DOD senior officials for administrative action, civil remedies or criminal prosecution,” Rovnak explained.

“We are also charged with promoting collaboration and information sharing of unauthorized disclosure information across DOD and the intelligence community.”

Since April 2023 when he arrived at DCSA, Rovnak carried out his UDPMO vision to provide continuous workforce engagement activities that reinforce the importance of protecting DOD information from unauthorized access or disclosure while providing it to those who need it, plus gaining efficiencies to deter, detect and mitigate instances of unauthorized disclosure.

“This requires a deliberate enterprise-wide effort to ensure everyone understands the importance of appropriate information sharing and safeguarding across the department and the role they have in providing protection of classified national security Information and CUI from those who don’t have an appropriate need to know,” said Rovnak.

"Our goal for this year is to provide a measurable reduction of DOD unauthorized disclosures through focused security awareness training activities that change human behavior toward the direction of prevention. We are planning to increase collaboration and engagement with the workforce as key elements to improve the identification, investigation, tracking and reporting of unauthorized disclosures in 2024."

The Unauthorized Disclosure of Classified Information and CUI course – available on the Center for Development of Security Excellence (CDSE) Security Awareness Hub – provides an overview of unauthorized disclosure, including specific types of unauthorized disclosure and some common misconceptions about unauthorized disclosure.

The course also discusses the types of damage caused by unauthorized disclosure and the various sanctions one could face if caught engaging in unauthorized disclosure. CDSE also provides resources to bring security expertise straight to any organization, including those for unauthorized disclosure.

In support of the January 2024 OPSEC Awareness Month, the Unauthorized Disclosure Program Management Office held three 'Unauthorized Disclosure 101' briefs to the DOD workforce, attended by over 350 individuals.

The UDPMO team is immediately notified of all incidents involving the release of classified national security information and CUI in the public domain.

Notifications to UDPMO include the release or enabled theft of information relating to any defense operation, system or technology determined to be classified national security information or CUI.

The team is also alerted to incidents of classified information or CUI disclosed to an unauthorized person or persons resulting in an individual's administrative action, referral for criminal or counterintelligence investigation, or the suspension or revocation of a security clearance.

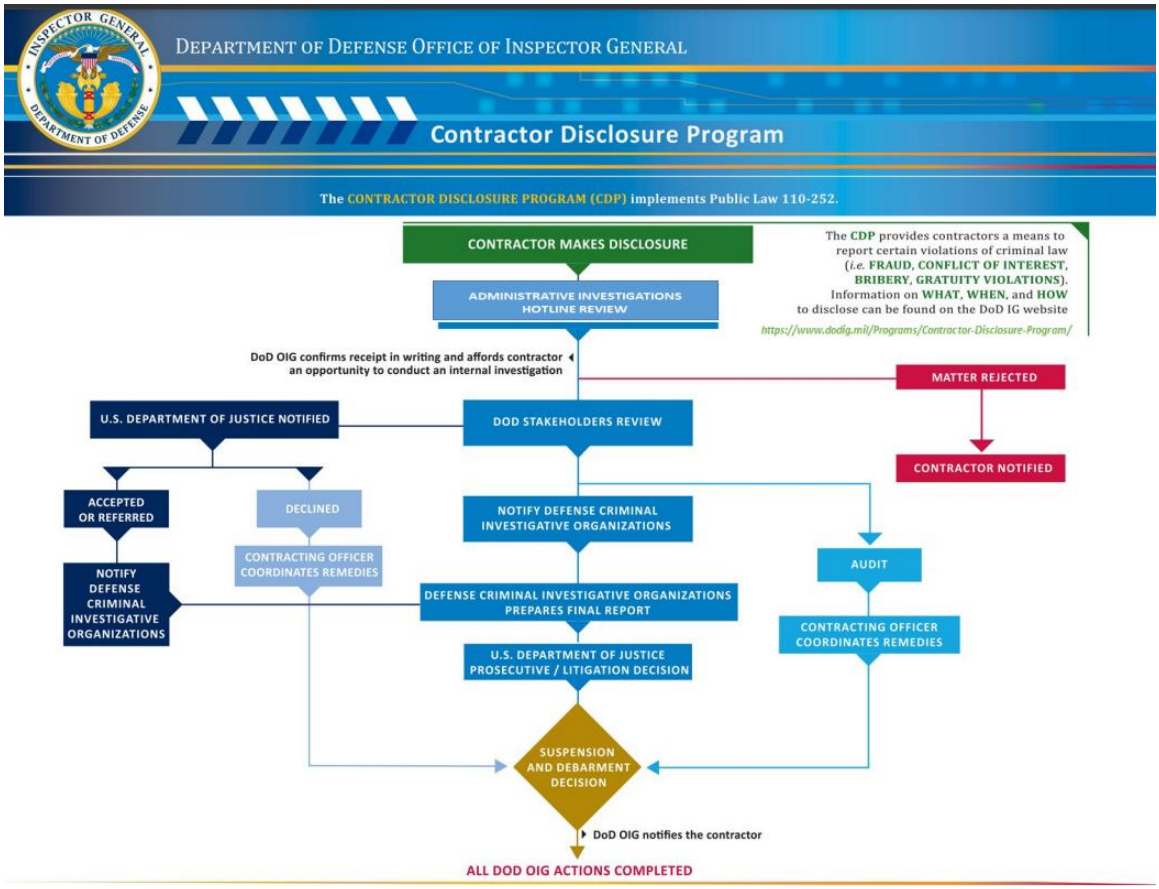
"Everyone has a civic duty to say something if they see an unauthorized disclosure," said Rovnak. "If they report it to us, we can work to mitigate it, but I need to be informed. It's crucial to report a potential unauthorized disclosure to the appropriate authorities."

When UDPMO receives a confirmed report of unauthorized disclosure in the public domain, the team submits a crime report to the Department of Justice. Included in the report are findings from a preliminary inquiry conducted by the affected component; a damage and impact assessment; and a media leaks questionnaire for the unauthorized disclosures appearing in the media.

In terms of reporting unauthorized disclosures, the DOD Whistleblower Protection allows individuals to report information they reasonably believe provides evidence of a violation of any law, rule, or regulation, gross mismanagement, a gross waste of funds, abuse of authority, or a substantial danger to public health and safety to designated officials via specific channels.

Additional information regarding DoD Whistleblower Protection is available on the DoD Inspector General website at www.dodig.mil

Those making contractor disclosures in response to Federal Acquisition Regulation clause 52.203-13 – Contractor Business Ethics Compliance Program and Disclosure Requirements – can find relevant instructions at www.dodig.mil/Programs/Contractor-Disclosure-Program.



The differences between unauthorized disclosure and protected whistleblowing are further clarified at:
https://www.cdse.edu/Training/Toolkits/Unauthorized-Disclosure-Toolkit

To read more:
https://www.dvidshub.net/news/466044/world-war-ii-slogan-crucial-preventing-unauthorized-disclosure-2024-ditmac-team-working-reduce-unauthorized-disclosures-training

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 individual or entity;

- should not be relied on in the 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 regarding such problems incurred because of using this site or any linked external sites.

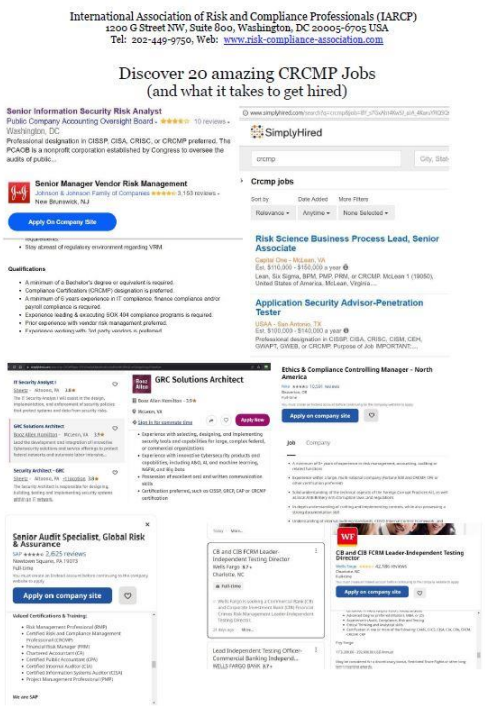
International Association of Risk and Compliance Professionals (IARCP)

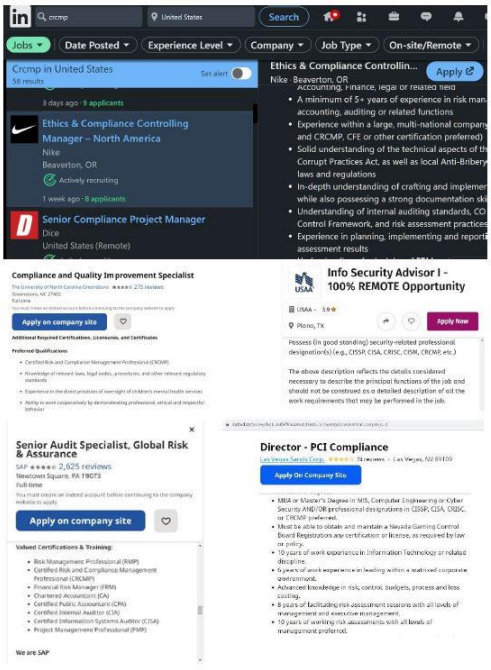
Our training and certification programs:

1. Certified Risk and Compliance Management Professional (CRCMP), distance learning and online certification program. You may visit: https://www.risk-compliance-association.com/Distance_Learning_and_Certification.htm

The CRCMP has become one of the most recognized certificates in risk management and compliance. There are CRCMPs in 57 countries. Companies and organizations around the world consider the CRCMP a preferred certificate.

You can find more about the demand for CRCMPs at: https://www.risk-compliance-association.com/CRCMP_Jobs_Careers.pdf





2. Certified Information Systems Risk and Compliance Professional (CISRCP), distance learning and online certification program. You may visit: https://www.risk-compliance-association.com/CISRCP_Distance_Learning_and_Certification.htm

3. 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

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

5. 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

The International Association of Risk and Compliance Professionals (IARCP) is a business unit of Compliance LLC, incorporated in Wilmington NC and offices in Washington DC, a provider of risk and compliance training and executive coaching in 57 countries. To learn more: https://www.risk-compliance-association.com/Privacy.htm

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
Email: lekatis@risk-compliance-association.com
Web: www.risk-compliance-association.com
HQ: 1220 N. Market Street Suite 804,
Wilmington DE 19801, USA