Sarbanes Oxley Compliance Professionals Association (SOXCPA)
1200 G Street NW Suite 800, Washington DC, 20005-6705 USA
Tel: 202-449-9750 Web: www.sarbanes-oxley-association.com

Sarbanes Oxley News, July 2023

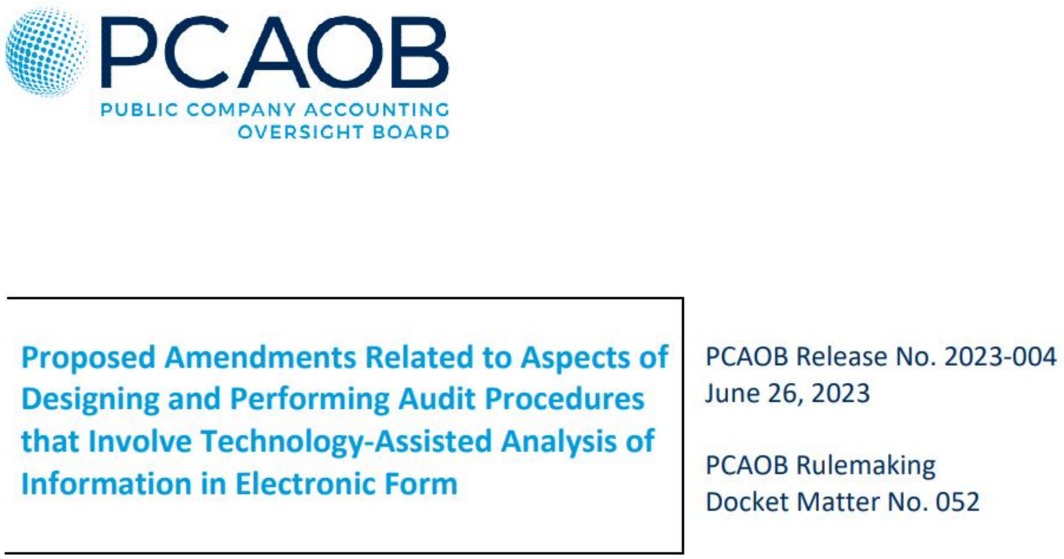
Dear members and friends,

We will start with an interesting development. The Public Company Accounting Oversight Board (PCAOB) has issued for public comment a proposal designed to improve audit quality and enhance investor protection by addressing aspects of designing and performing audit procedures that involve technology-assisted analysis of information in electronic form.

The proposal includes changes to update aspects of AS 1105, Audit Evidence, and AS 2301, The Auditor's Responses to the Risks of Material Misstatement.

The deadline for public comment on the proposal is August 28, 2023.

"The use of technology by auditors and financial statement preparers never stops evolving, and PCAOB standards must keep up to fulfill our mission to protect investors," said PCAOB Chair Erica Y. Williams. "Today's proposal is another key part of our strategic drive to modernize PCAOB standards."



PCAOB
PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD

Proposed Amendments Related to Aspects of Designing and Performing Audit Procedures that Involve Technology-Assisted Analysis of Information in Electronic Form

PCAOB Release No. 2023-004
June 26, 2023

PCAOB Rulemaking
Docket Matter No. 052

Why the Board Is Proposing These Changes Now

Existing PCAOB standards relating to audit evidence and responses to risk were issued by the Board in 2010. Since that time, companies have greatly expanded their use of information systems that maintain large volumes of information in electronic form.

As a result, auditors have greater access to large volumes of company-produced and third-party information in electronic form that may potentially serve as audit evidence. Meanwhile, some auditors have greatly expanded their use of data analysis tools.

Although the PCAOB staff's research indicates that auditors are using technology-assisted analysis in audit procedures, it also indicates that audit quality would benefit if our standards included additional direction addressing specific aspects of designing and performing audit procedures that involve technology-assisted analysis.

What the Proposal Seeks to Achieve

The proposal seeks to improve audit quality by reducing the likelihood that an auditor who uses technology-assisted analysis will issue an opinion without obtaining sufficient appropriate audit evidence. In particular, the proposal would bring greater clarity to auditor responsibilities in the following areas:

1. **Using reliable information in audit procedures:** Technology-assisted analysis often involves analyzing vast amounts of information in electronic format. The proposal would emphasize auditor responsibilities when evaluating the reliability of such information. For example, when

auditors test a company's controls over electronic information, their testing should include controls over the company's information technology related to such information.

2. **Using audit evidence for multiple purposes:** Technology-assisted analysis can be used to provide audit evidence for various purposes in an audit.

For example, performing risk assessment procedures when planning an audit and performing substantive procedures in response to the auditor's risk assessment.

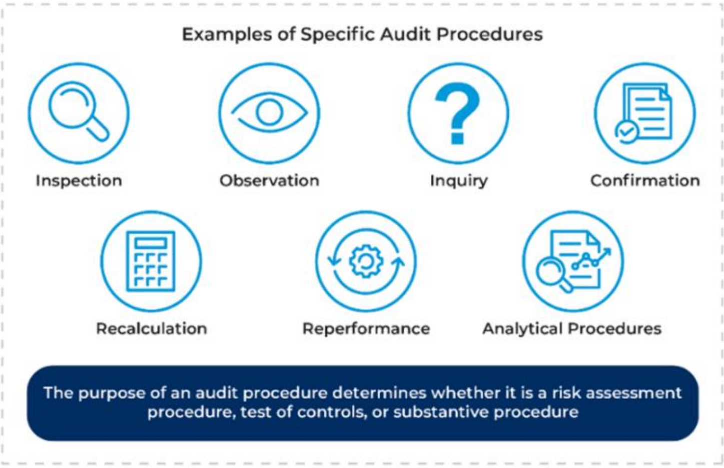
The proposal would specify that if an auditor uses audit evidence from an audit procedure for more than one purpose, the auditor should design and perform the procedure to achieve each of the relevant objectives.

3. **Designing and performing substantive procedures:** When designing and performing substantive procedures, auditors can use technology-assisted analysis to identify transactions and balances that meet certain criteria and warrant further investigation.

For example, auditors can identify all transactions within an account processed by a certain individual or exceeding a certain amount.

The proposal would clarify the factors the auditor should consider as part of that investigation, including whether the identified items represent a misstatement or a control deficiency or indicate a need for the auditor to modify its risk assessment or planned procedures.

Throughout the proposal, the Board requests comment on specific aspects of the proposed amendments. Readers are encouraged to answer these questions, to comment on any aspect of the proposal, and to provide reasoning and relevant data supporting their views.


Examples of Specific Audit Procedures
Inspection
Observation
Inquiry
Confirmation
Recalculation
Reperformance
Analytical Procedures
The purpose of an audit procedure determines whether it is a risk assessment procedure, test of controls, or substantive procedure

To read more:

https://pcaobus.org/news-events/news-releases/news-release-detail/pcaob-issues-proposal-to-bring-greater-clarity-to-certain-auditor-responsibilities-when-using-technology-assisted-analysis

The proposal:

https://assets.pcaobus.org/pcaob-dev/docs/default-source/rulemaking/docket-052/pcaob-release-no.-2023-004-technology-assisted-analysis.pdf?sfvrsn=b801ffd0_2

Trust Services & Digital Wallets: Moving to the Cloud and Remote Identity Proofing

In order to address the cybersecurity questions of remote identity proofing, the European Union Agency for Cybersecurity (ENISA) organised a workshop to support the area of Trust Services and Digital Wallets and published a report on moving trust services to the cloud.

Report on Trust Services: Secure Move to the Cloud of the eIDAS ecosystem

For the purpose of the report, ENISA conducted a survey with more than 120 stakeholders from over 29 countries in the EU and globally. The survey allowed to get an insight of practical experiences of Trust Service Providers, Conformity Assessment Bodies, Supervisory Bodies and Cloud Service Providers regarding the transition of trust services to the cloud.

Moving trust services to the cloud must be understood as an ongoing process that has to be followed step by step.

While some services – such as the validation of signatures, registered delivery, time stamp or signature preservation – are moved rather quickly, other services – such as the issuance of certificates and remote control over the signing device – require in-depth analysis and preparation.

The transition of data to the cloud has to be secure at all times and, in the best case, must remain in the data centre of the trust services provider.

This report has given a detailed overview of the issues to be addressed for such a transition, including the related challenges, impediments and opportunities.

Workshop on Remote Video Identification: Attacks and Foresight

The workshop was the occasion for ENISA to publish its report exploring the secure move to the cloud of the eIDAS ecosystem. In cooperation with the European Competent Authorities for Trust Services (ECATS) expert group, ENISA organised a workshop on 10 May 2023 in Amsterdam, Netherlands.

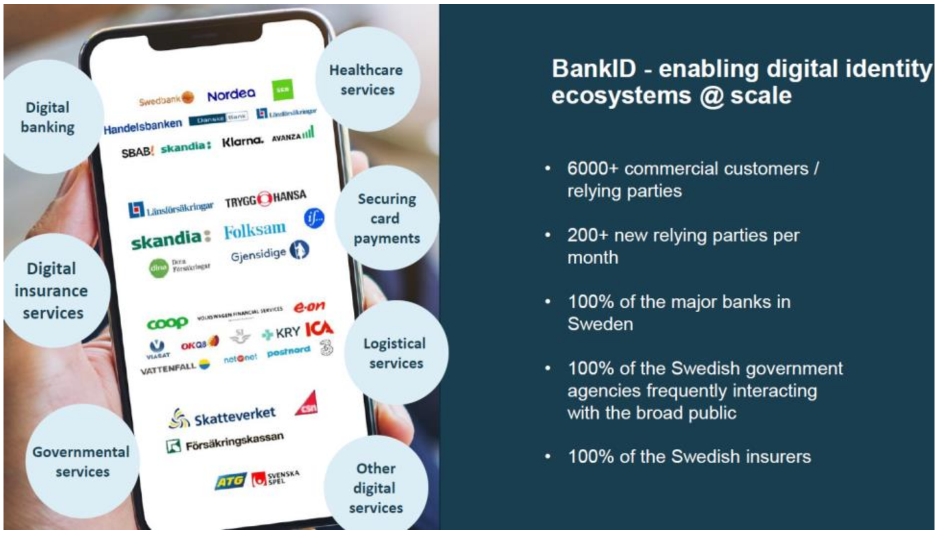
The purpose of the workshop was to explore and discuss the latest national implementations, existing and emerging attacks, and the security measures envisaged for the protection of remote identity proofing across the EU.

Over 100 participants attended the workshop and included representatives from Supervisory Bodies, Identity and trust service providers, conformity assessment bodies, standardisation bodies and research community.

The workshop addressed the following main challenges:

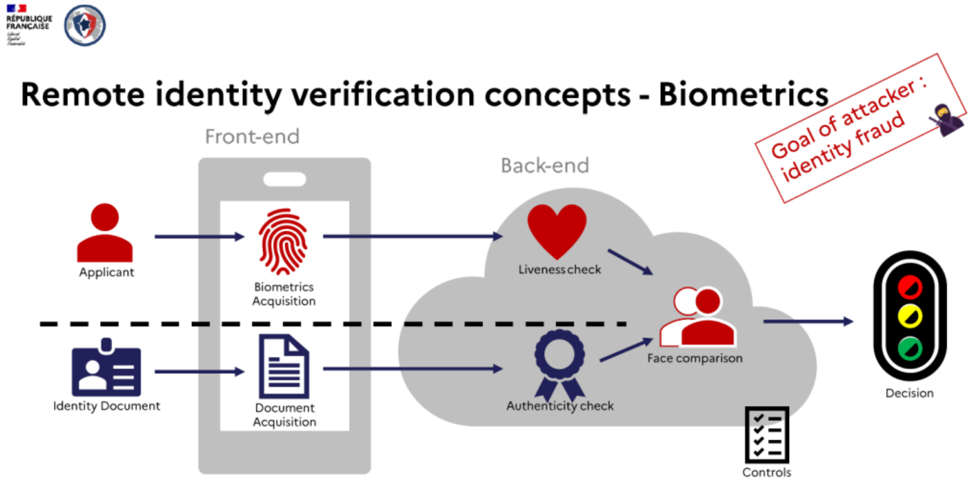
- lack of EU legislation harmonisation;
- how to keep up with technological advancements connected to AI;
- the testing and performance measuring landscape;
- how to continuously follow the supply chain of products and services.

For the presentations you may visit: https://www.enisa.europa.eu/events/remote-video-identification-attacks-and-foresight

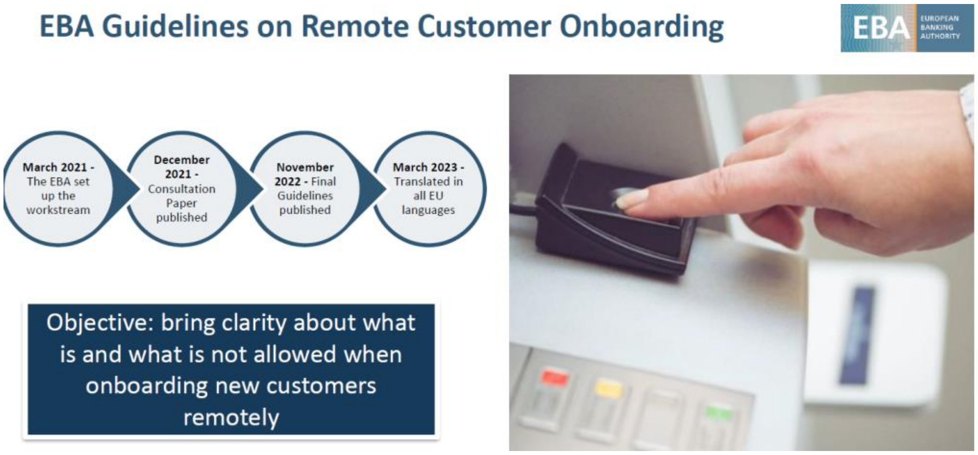


BankID - enabling digital identity ecosystems @ scale

- 6000+ commercial customers / relying parties
- 200+ new relying parties per month
- 100% of the major banks in Sweden
- 100% of the Swedish government agencies frequently interacting with the broad public
- 100% of the Swedish insurers



Remote identity verification concepts - Biometrics



EBA Guidelines on Remote Customer Onboarding

EBA EUROPEAN BANKING AUTHORITY

March 2021 - The EBA set up the workstream

December 2021 - Consultation Paper published

November 2022 - Final Guidelines published

March 2023 - Translated in all EU languages

Objective: bring clarity about what is and what is not allowed when onboarding new customers remotely

Meeting of the European Competent Authorities for Trust Services (ECATS) Expert Group

The Dutch Supervisory Authority hosted the 21st meeting of the ECATS on 11 and 12 May, back-to-back with the meeting of FESA (Forum of European Supervisory Authorities).

The group discussed latest developments in eIDAS2, the connection between the upcoming implementation of the NIS 2 and eIDAS2, as well as updates on standardisation and certification in relation to trust services.

The ECATS EG is the informal group focusing to facilitates voluntary and informal collaboration between competent authority experts from EU Member States, European Economic Area (EEA) and European Free Trade Association (EFTA) States, EU Candidate countries and other relevant stakeholders to ensure smooth and secure functioning of trust services.

To read more: https://www.enisa.europa.eu/news/trust-services-digital-wallets-moving-to-the-cloud-and-remote-identity-proofing

Financial Stability Institute, FSI Insights on policy implementation No 50

Banks' cyber security – a second generation of regulatory approaches

Juan Carlos Crisanto, Jefferson Umebara Pelegrini and Jermy Prenio

BANK FOR INTERNATIONAL SETTLEMENTS

Executive summary

Cyber resilience continues to be a top priority for the financial services industry and a key area of attention for financial authorities.

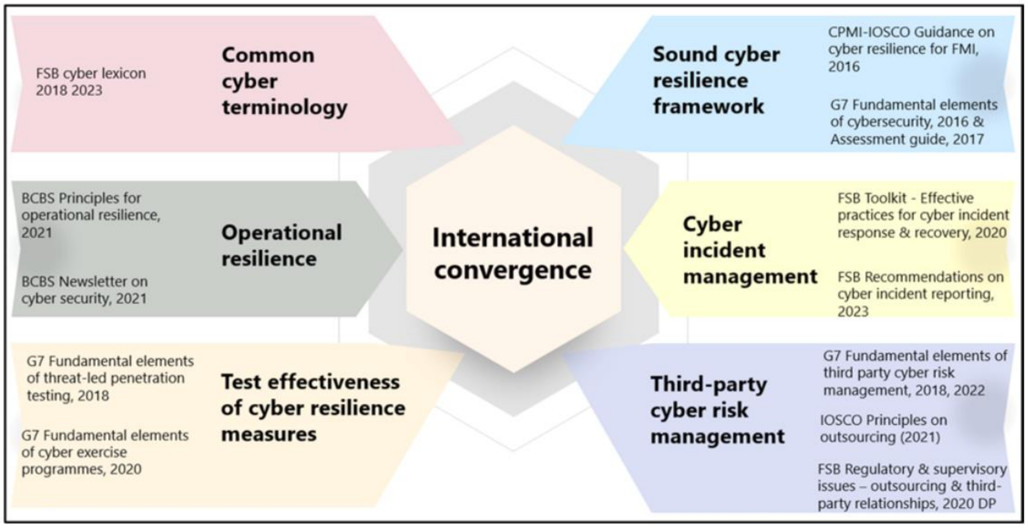
This is not surprising given that cyber incidents pose a significant threat to the stability of the financial system and the global economy.

The financial system performs a number of key activities that support the real economy (eg deposit taking, lending, payments and settlement services).

Cyber incidents can disrupt the information and communication technologies that support these activities and can lead to the misuse and abuse of data that such technologies process or store.

This is complicated by the fact that the cyber threat landscape keeps evolving and becoming more complex amid continuous digitalisation, increased third-party dependencies and geopolitical tensions.

Moreover, the cost of cyber incidents has continuously and significantly increased over the years.


FSB cyber lexicon 2018 2023
Common cyber terminology
Sound cyber resilience framework
CPMI-IOSCO Guidance on cyber resilience for FMI, 2016
G7 Fundamental elements of cybersecurity, 2016 & Assessment guide, 2017
BCBS Principles for operational resilience, 2021
BCBS Newsletter on cyber security, 2021
Operational resilience
International convergence
Cyber incident management
FSB Toolkit - Effective practices for cyber incident response & recovery, 2020
FSB Recommendations on cyber incident reporting, 2023
G7 Fundamental elements of threat-led penetration testing, 2018
G7 Fundamental elements of cyber exercise programmes, 2020
Test effectiveness of cyber resilience measures
Third-party cyber risk management
G7 Fundamental elements of third party cyber risk management, 2018, 2022
IOSCO Principles on outsourcing (2021)
FSB Regulatory & supervisory issues – outsourcing & third-party relationships, 2020 DP

This paper updates Crisanto and Prenio (2017) by revisiting the cyber regulations in the jurisdictions covered in that paper, as well as examining those issued in other jurisdictions.

Aside from cyber regulations in Hong Kong SAR, Singapore, the United Kingdom and the United States, which the 2017 paper covered, this paper examines cyber regulations in Australia, Brazil, the European Union, Israel, Kenya, Mexico, Peru, Philippines, Rwanda, Saudi Arabia and South Africa.

The jurisdictions were chosen to reflect cyber regulations in both advanced economies (AEs) and emerging market and developing economies (EMDEs). This highlights the fact that since 2017 several jurisdictions – including EMDEs – have put cyber regulations in place.

There remain two predominant approaches to the regulation of banks' cyber resilience: the first leverages existing related regulations and the second involves issuing comprehensive regulations.

The first approach takes as a starting point regulations on operational risk, information security etc and add cyber-specific elements to them.

Here, cyber risk is viewed as any other risk and thus the general requirements for risk management, as well as the requirements on information security and operational risks, also apply.

This approach is more commonly observed in jurisdictions that already have these related regulations firmly established.

The second approach seeks to cover all aspects of cybersecurity, from governance arrangements to operational procedures, in one comprehensive regulation.

In both approaches, to counter the risks that might result from having too much prescriptiveness in cyber regulations, some regulations combine broad cyber resilience principles with a set of baseline requirements.

Regardless of the regulatory approach taken, the proportionality principle is given due consideration in the application of cyber resilience frameworks.

Whether as part of related regulations or separate comprehensive ones, recent cyber security policies have evolved and could be described as "second-generation" cyber regulations.

The "first generation" cyber regulations, which were issued mainly in AEs, focused on establishing a cyber risk management approach and controls. Over the last few years, authorities, including those in EMDEs, have issued new or additional cyber regulations.

These second-generation regulations have a more embedded “assume breach” mentality and hence are more aligned with operational resilience concepts.

As such, they focus on improving cyber resilience and providing financial institutions and authorities with specific tools to achieve this.

The “second-generation” regulations leverage existing policy approaches to provide additional specific guidance to improve cyber resilience.

Cyber security strategy, cyber incident reporting, threat intelligence sharing and cyber resilience testing are still the primary focus of the newer regulations.

Managing cyber risks that could arise from connections with third-party service providers has become a key element of the “second generation” cyber security framework.

Moreover, there are now more specific regulatory requirements on cyber incident response and recovery, as well as on incident reporting and cyber resilience testing frameworks.

In addition, regulatory requirements or expectations relating to issues such as cyber resilience metrics and the availability of appropriate cyber security expertise in banks have been introduced in a few jurisdictions.

Authorities in EMDEs tend to be more prescriptive in their cyber regulations.

Cyber security strategy, governance arrangements – including roles and responsibilities – and the nature and frequency of cyber resilience testing are some of the areas where EMDE authorities provide prescriptive requirements.

This is approach seems to be connected to the need to strengthen the cyber resilience culture across the financial sector, resource constraints and/or the lack of sufficient cyber security expertise in these jurisdictions.

Hence, EMDE authorities may see the need to be clearer in their expectations to make sure banks’ boards and senior management invest in cyber security and banks’ staff know exactly what they need to do.

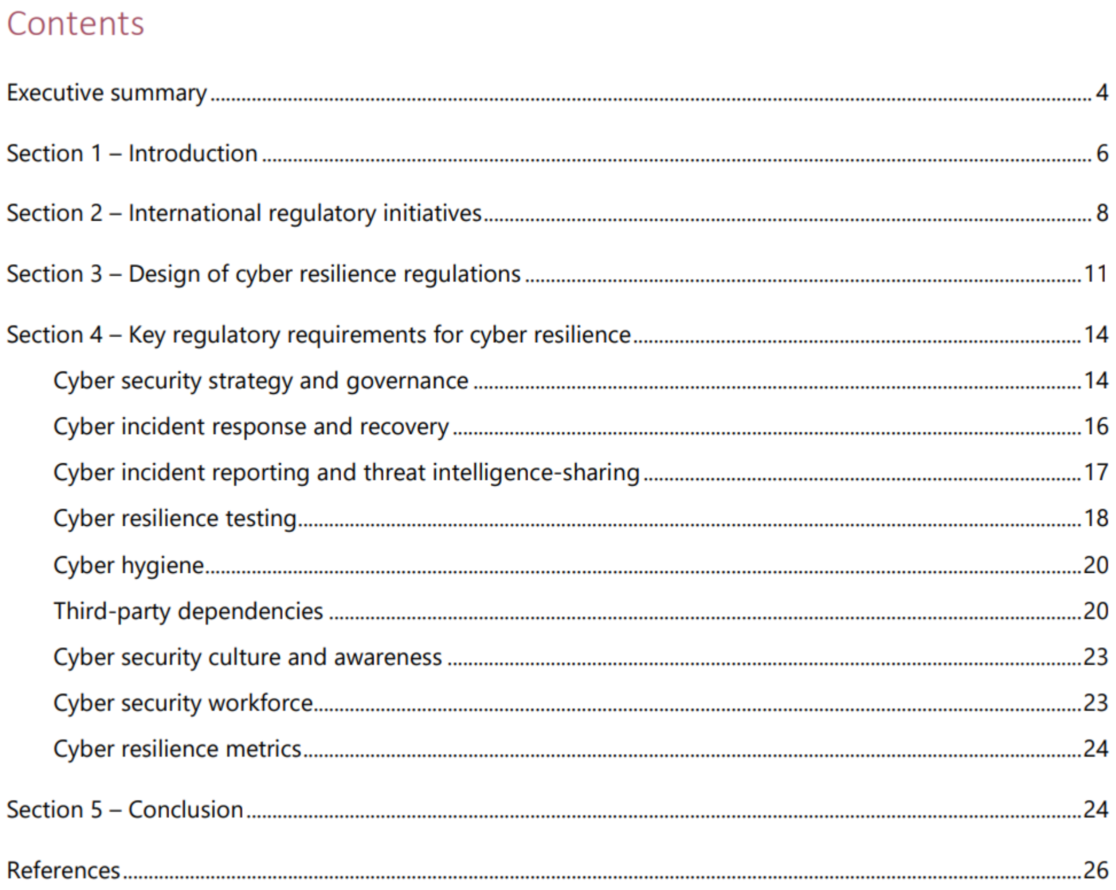
International work has resulted in a convergence in cyber resilience regulations and expectations in the financial sector, but more could be done in some areas.

Work by the G7 Cyber Expert Group (CEG) and the global standard-setting bodies (SSBs) on cyber resilience has facilitated consistency in financial regulatory and supervisory expectations across jurisdictions.

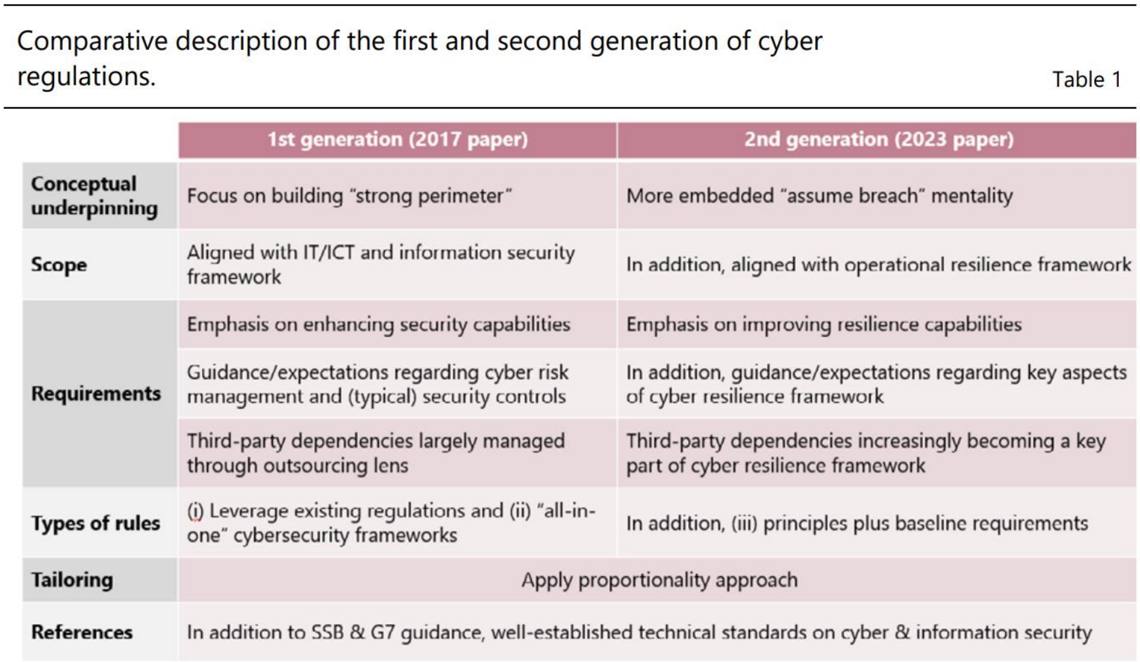
This is necessary given the borderless nature of cyber crime and its potential impact on global financial stability.

Another area where there might be scope for convergence is the way in which authorities assess the cyber resilience of supervised institutions. This could, for example, include aligning the assessment of adequacy of a firm's cyber security governance, workforce and cyber resilience metrics.

Lastly, there might be scope to consider an international framework for critical third-party providers, in particular cloud providers, given the potential cross-border impact of a cyber incident in one of these providers.



Contents



Comparative description of the first and second generation of cyber regulations.

Table 1

	1st generation (2017 paper)	2nd generation (2023 paper)
Conceptual underpinning	Focus on building "strong perimeter"	More embedded "assume breach" mentality
Scope	Aligned with IT/ICT and information security framework	In addition, aligned with operational resilience framework
Requirements	Emphasis on enhancing security capabilities	Emphasis on improving resilience capabilities
	Guidance/expectations regarding cyber risk management and (typical) security controls	In addition, guidance/expectations regarding key aspects of cyber resilience framework
	Third-party dependencies largely managed through outsourcing lens	Third-party dependencies increasingly becoming a key part of cyber resilience framework
Types of rules	(i) Leverage existing regulations and (ii) "all-in-one" cybersecurity frameworks	In addition, (iii) principles plus baseline requirements
Tailoring	Apply proportionality approach	
References	In addition to SSB & G7 guidance, well-established technical standards on cyber & information security	

To read more:
https://www.bis.org/fsi/publ/insights50.pdf

Malicious Actors Manipulating Photos and Videos to Create Explicit Content and Sextortion Schemes

Public Service Announcement
FEDERAL BUREAU OF INVESTIGATION

The FBI is warning the public of malicious actors creating synthetic content (commonly referred to as "deepfakes") by manipulating benign photographs or videos to target victims.

Technology advancements are continuously improving the quality, customizability, and accessibility of artificial intelligence (AI)-enabled content creation.

The FBI continues to receive reports from victims, including minor children and non-consenting adults, whose photos or videos were altered into explicit content.

The photos or videos are then publicly circulated on social media or pornographic websites, for the purpose of harassing victims or sextortion schemes.

Explicit Content Creation

Malicious actors use content manipulation technologies and services to exploit photos and videos—typically captured from an individual's social media account, open internet, or requested from the victim—into sexually-themed images that appear true-to-life in likeness to a victim, then circulate them on social media, public forums, or pornographic websites.

Many victims, which have included minors, are unaware their images were copied, manipulated, and circulated until it was brought to their attention by someone else.

The photos are then sent directly to the victims by malicious actors for sextortion or harassment, or until it was self-discovered on the internet.

Once circulated, victims can face significant challenges in preventing the continual sharing of the manipulated content or removal from the internet.

Sextortion and Harassment

Sextortion, which may violate several federal criminal statutes, involves coercing victims into providing sexually explicit photos or videos of themselves, then threatening to share them publicly or with the victim's family and friends.

The key motivators for this are a desire for more illicit content, financial gain, or to bully and harass others. Malicious actors have used manipulated photos or videos with the purpose of extorting victims for ransom or to gain compliance for other demands (e.g., sending nude photos).

As of April 2023, the FBI has observed an uptick in sextortion victims reporting the use of fake images or videos created from content posted on their social media sites or web postings, provided to the malicious actor upon request, or captured during video chats.

Based on recent victim reporting, the malicious actors typically demanded:

1. Payment (e.g., money, gift cards) with threats to share the images or videos with family members or social media friends if funds were not received; or

2. The victim send real sexually-themed images or videos.

Recommendations

The FBI urges the public to exercise caution when posting or direct messaging personal photos, videos, and identifying information on social media, dating apps, and other online sites.

Although seemingly innocuous when posted or shared, the images and videos can provide malicious actors an abundant supply of content to exploit for criminal activity.

Advancements in content creation technology and accessible personal images online present new opportunities for malicious actors to find and target victims.

This leaves them vulnerable to embarrassment, harassment, extortion, financial loss, or continued long-term re-victimization.

The FBI recommends the public consider the following when sharing content (e.g., photos and videos) or engaging with individuals online:

1. Monitor children's online activity and discuss risks associated with sharing personal content.

2. Use discretion when posting images, videos, and personal content online, particularly those that include children or their information.

2a. Images, videos, or personal information posted online can be captured, manipulated, and distributed by malicious actors without your knowledge or consent.

2b. Once content is shared on the internet, it can be extremely difficult, if not impossible, to remove once it is circulated or posted by other parties.

3. Run frequent online searches of you and your children's information (e.g., full name, address, phone number, etc.) to help identify the exposure and spread of personal information on the internet.

4. Apply privacy settings on social media accounts—including setting profiles and your friends lists as private—to limit the public exposure of your photos, videos, and other personal information.

5. Consider using reverse image search engines to locate any photos or videos that have circulated on the internet without your knowledge.

6. Exercise caution when accepting friend requests, communicating, engaging in video conversations, or sending images to individuals you do not know personally.

Be especially wary of individuals who immediately ask or pressure you to provide them. Those items could be screen-captured, recorded, manipulated, shared without your knowledge or consent, and used to exploit you or someone you know.

7. Do not provide any unknown or unfamiliar individuals with money or other items of value. Complying with malicious actors does not guarantee your sensitive photos or content will not be shared.

8. Use discretion when interacting with known individuals online who appear to be acting outside their normal pattern of behavior. Hacked social media accounts can easily be manipulated by malicious actors to gain trust from friends or contacts to further criminal schemes or activity.

9. Secure social media and other online accounts using complex passwords or passphrases and multi-factor authentication.

10. Research the privacy, data sharing, and data retention policies of social media platforms, apps, and websites before uploading and sharing images, videos, or other personal content.

To read more: https://www.ic3.gov/Media/Y2023/PSA230605

NIST ‘Toggle Switch’ Can Help Quantum Computers Cut Through the Noise

The novel device could lead to more versatile quantum processors with clearer outputs.

NIST
NATIONAL INSTITUTE OF
STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

What good is a powerful computer if you can’t read its output? Or readily reprogram it to do different jobs? People who design quantum computers face these challenges, and a new device may make them easier to solve.

The device, introduced by a team of scientists at the National Institute of Standards and Technology (NIST), includes two superconducting quantum bits, or qubits, which are a quantum computer’s analogue to the logic bits in a classical computer’s processing chip.

The heart of this new strategy relies on a “toggle switch” device that connects the qubits to a circuit called a “readout resonator” that can read the output of the qubits’ calculations.

This toggle switch can be flipped into different states to adjust the strength of the connections between the qubits and the readout resonator. When toggled off, all three elements are isolated from each other.

When the switch is toggled on to connect the two qubits, they can interact and perform calculations. Once the calculations are complete, the toggle switch can connect either of the qubits and the readout resonator to retrieve the results.

Having a programmable toggle switch goes a long way toward reducing noise, a common problem in quantum computer circuits that makes it difficult for qubits to make calculations and show their results clearly.

“The goal is to keep the qubits happy so that they can calculate without distractions, while still being able to read them out when we want to,” said Ray Simmonds, a NIST physicist and one of the paper’s authors.

“This device architecture helps protect the qubits and promises to improve our ability to make the high-fidelity measurements required to build quantum information processors out of qubits.”

The team, which also includes scientists from the University of Massachusetts Lowell, the University of Colorado Boulder and Raytheon BBN Technologies, describes its results in a paper published today in Nature Physics.

Quantum computers, which are still at a nascent stage of development, would harness the bizarre properties of quantum mechanics to do jobs that even our most powerful classical computers find intractable, such as aiding in the development of new drugs by performing sophisticated simulations of chemical interactions.

However, quantum computer designers still confront many problems. One of these is that quantum circuits are kicked around by external or even internal noise, which arises from defects in the materials used to make the computers. This noise is essentially random behavior that can create errors in qubit calculations.

Present-day qubits are inherently noisy by themselves, but that's not the only problem. Many quantum computer designs have what is called a static architecture, where each qubit in the processor is physically connected to its neighbors and to its readout resonator. The fabricated wiring that connects qubits together and to their readout can expose them to even more noise.

Such static architectures have another disadvantage: They cannot be reprogrammed easily. A static architecture's qubits could do a few related jobs, but for the computer to perform a wider range of tasks, it would need to swap in a different processor design with a different qubit organization or layout.

(Imagine changing the chip in your laptop every time you needed to use a different piece of software, and then consider that the chip needs to be kept a smidgen above absolute zero, and you get why this might prove inconvenient.)

The team's programmable toggle switch sidesteps both of these problems. First, it prevents circuit noise from creeping into the system through the readout resonator and prevents the qubits from having a conversation with each other when they are supposed to be quiet.

“This cuts down on a key source of noise in a quantum computer,” Simmonds said.

Second, the opening and closing of the switches between elements are controlled with a train of microwave pulses sent from a distance, rather than through a static architecture's physical connections. Integrating more of these toggle switches could be the basis of a more easily programmable quantum computer. The microwave pulses can also set the order and sequence of logic operations, meaning a chip built with many of the team's toggle switches could be instructed to perform any number of tasks.

“This makes the chip programmable,” Simmonds said. “Rather than having a completely fixed architecture on the chip, you can make changes via software.”

One last benefit is that the toggle switch can also turn on the measurement of both qubits at the same time. This ability to ask both qubits to reveal themselves as a couple is important for tracking down quantum computational errors.

The qubits in this demonstration, as well as the toggle switch and the readout circuit, were all made of superconducting components that conduct electricity without resistance and must be operated at very cold temperatures.

The toggle switch itself is made from a superconducting quantum interference device, or “SQUID,” which is very sensitive to magnetic fields passing through its loop. Driving a microwave current through a nearby antenna loop can induce interactions between the qubits and the readout resonator when needed.

At this point, the team has only worked with two qubits and a single readout resonator, but Simmonds said they are preparing a design with three qubits and a readout resonator, and they have plans to add more qubits and resonators as well.

Further research could offer insights into how to string many of these devices together, potentially offering a way to construct a powerful quantum computer with enough qubits to solve the kinds of problems that, for now, are insurmountable.

To read more: https://www.nist.gov/news-events/news/2023/06/nist-toggle-switch-can-help-quantum-computers-cut-through-noise

National Artificial Intelligence Advisory Committee Releases First Report

The National Artificial Intelligence Advisory Committee (NAIAC) has delivered its first report to the president, established a Law Enforcement Subcommittee to address the use of AI technologies in the criminal justice system, and completed plans to realign its working groups to allow it to explore the impacts of AI on workforce, equity, society and more.

The report recommends steps the U.S. government can take to maximize the benefits of AI technology, while reducing its harms. This includes new steps to bolster U.S. leadership in trustworthy AI, new R&D initiatives, increased international cooperation, and efforts to support the U.S. workforce in the era of AI. The report also identifies areas of focus for NAIAC for the next two years, including in rapidly developing areas of AI, such as generative AI.

“We are at a pivotal moment in the development of AI technology and need to work fast to keep pace with the changes it is bringing to our lives,” said U.S. Deputy Secretary of Commerce Don Graves. “As AI opens up exciting opportunities to improve things like medical diagnosis and access to health care and education, we have an obligation to make sure we strike the right balance between innovation and risk. We can lead the world in establishing trustworthy, inclusive and beneficial AI, and I look forward to considering the committee’s recommendations as we do that.”

When it comes to AI, President Biden has been clear that in order to seize the opportunities AI presents, we must first mitigate its risks. NAIAC’s work supports the Biden-Harris administration’s ongoing efforts to promote responsible American innovation in AI and protect people’s rights and safety.

Given the fast pace of development and deployment of AI technology such as generative AI, which includes the large language models that power chatbots and other tools that create new content, the committee also plans to consider various mechanisms for carrying out its work on short time frames in the coming years.

The committee recently completed plans to realign its working groups to allow it to explore the impacts of AI on workforce, equity, society and more.

The new NAIAC focus areas are:

- AI Futures: Sustaining Innovation in Next Gen AI
- AI in Work and the Workforce
- AI Regulation and Executive Action
- Engagement, Education and Inclusion
- Generative and NextGen AI: Safety and Assurance
- Rights-Respecting AI
- International Arena: Collaboration on AI Policy and AI-Enabled Solutions
- Procurement of AI Systems
- AI and the Economy

To read more: https://www.nist.gov/news-events/news/2023/06/national-artificial-intelligence-advisory-committee-releases-first-report

Remarks to the Atlanta Commerce and Press Clubs (including Transition to AI, AI as a Tool and a Target of Cybercrime, AI as a Target of Foreign Adversaries)

Christopher Wray, Director, Federal Bureau of Investigation, Atlanta

Introduction

Thanks, Walter. And my thanks to the Atlanta Commerce Club and the Press Club for having me this afternoon. It's great to look out and see so many old friends. I still think of Atlanta as home. This is where my career in law—and, a few years later, law enforcement—really began.

And it's an honor to be here with such a forward-leaning group—people who keep Atlanta's economy thriving, and its public informed and engaged.

Today, I want to talk about a couple of topics that are top-of-mind at the Bureau, and for the public and partners we always remember that we're doing our work for.

First, violent crime—and what we and our partners are doing about it, here in Georgia and elsewhere.

And, then, I'm going to shift gears on you and talk technology—artificial intelligence and how, at the FBI, we're focusing on the fast-changing frontier of what's possible.

But the common thread is adaptation: For decades, the FBI has adapted to new technology and threats across our programs—including countering violent crime—and that adaptation remains a vital part of our mission today.

Violent Crime

I want to start by sharing a little bit about some of the conversations I had earlier today with chiefs and sheriffs from departments all across the state of Georgia.

Their biggest concern is the same one I hear almost weekly when I speak with their counterparts in all 50 states, in communities large and small—

and that's the alarming level of violent crime. And our nationwide statistics from the last couple of years confirm the violent crime threat in this country is real and not letting up.

People deserve to be able to go to work, meet with friends, go shopping—in other words, live their daily lives—without fear. And when that sense of safety is undermined, everyone loses.

Whether it's gangs terrorizing communities, robbery crews graduating from carjackings to even worse violence, or neighborhoods located along key drug-trafficking routes getting inundated with crime, communities in every corner of this country are affected.

That's unacceptable, which is why we're working shoulder-to-shoulder with our state and local partners to combat that appalling trend.

Here, in Georgia, there are examples all across the state of the impact we can have when we work together.

Spurred by the shooting death of an 8-year-old child in January, our Safe Streets Task Force teamed up with the Richmond County Sheriff's Office and the local DA to disrupt and dismantle gangs that had terrorized communities in and around Augusta.

We aggressively targeted the most violent offenders on an unprecedented scale, making 119 felony arrests in just three months.

Another operation against the "Ghost Face Gangsters" down around Brunswick exposed a massive drug-trafficking ring led by a white supremacist street gang. That collaborative investigation resulted in what is believed to be the largest-ever indictment in Southern District of Georgia history, with federal charges against 76 subjects and state charges against more than three dozen others.

Closer to home, we're wrapping up a years-long investigation that disrupted a major drug-trafficking route that was moving huge quantities of drugs from Colombia; north through Mexico; and, ultimately, landing right here, in Atlanta.

We've arrested and charged individuals in Georgia, Florida, Tennessee, and Texas; and we're in the process of extraditing two of the main targets from Mexico to face justice here in the United States. Along the way, we've seized millions of dollars, taken dozens of firearms out of the hands of the drug traffickers, and intercepted loads of narcotics that were headed for the streets of Atlanta.

But it’s not just the major investigations—our agents and task-force officers are also focused on the violence against everyday people going about their everyday lives.

Just recently, for instance, we took down a robbery crew that had pistol-whipped and robbed one of their victims at an ATM, carjacked another, and held up two armored trucks by putting rifles to the heads of the couriers.

Atlanta is not just a hub for business. I’m afraid it also seems to be a destination for violent fugitives who commit crimes out of state. So, I’m particularly encouraged to see that our Atlanta Metropolitan Major Offenders (or AMMO) Task Force has been reinvigorated.

Through AMMO, we’ve done a lot of great work with Atlanta PD and other departments in the area to get some of the most dangerous fugitives off the streets.

In fact, the task force recently completed a months-long investigation into five offenders from New Jersey, who had posed as FBI agents and shot a Bergen County resident during a home invasion.

That investigation resulted in charges against all five fugitives for attempted murder, kidnapping, and robbery. And it’s only a small sampling of what the AMMO Task Force is doing for Atlanta-area communities.

That’s all just here in Georgia—we’re working with our brothers and sisters in state and local law enforcement all across the country to maximize our impact.

The FBI now leads more than 300 violent crime task forces made up of over 3,000 task force officers, working shoulder-to-shoulder with our agents, analysts, and professionals.

And each of those TFOs represents an officer, a deputy, or an investigator that a local police chief, sheriff, or agency head was willing to send our way—not because they didn’t have enough work to do at their own department or office, but because they saw the tremendous value that our FBI-led task forces bring.

And I can report that our agents and TFOs have been busy.

Together, in 2022, we arrested more than 20,000 violent criminals and child predators—an average of almost 60 per day, every day.

We also seized more than 9,600 firearms from those violent offenders, cut into the capabilities of 3,500 gangs and violent criminal enterprises, and completely dismantled 370 more. And we have no plans to let up any time soon.

Transition to AI

When it comes to tackling the violent-crime problem, one of the FBI's strengths has always been finding new and creative approaches to solving crimes.

In fact, in his first report to Congress on the FBI after its founding in 1908, Attorney General Bonaparte described the FBI itself as "an innovation." And, for more than a century since then, we've taken it upon ourselves to live up to that standard, again and again.

We've built and developed tools in key areas that help us accomplish our mission to keep people safe—things like biometrics, DNA research, facial recognition, and voice recognition; digital forensics teams to handle technically complex cases; cellphone data analysis to uncover criminals' movements and locate missing persons; and much more.

These were all innovations when they were created, and without them, we couldn't protect the American people the way we do now.

So I want to take this opportunity to talk about the newest technology the world is grappling with on a massive scale: AI, or artificial intelligence.

Who would have thought, even just a few years ago, that we'd all be having conversations about AI around the dinner table?

It feels a bit like science fiction—and that's because it used to be, though I can assure you it's not a new topic at the FBI.

As we all know, today, AI is quickly making world-changing breakthroughs in everything from astronomy to agriculture, and energy to the environment. It's solving problems as varied as folding amino acids into the basic building blocks for life, and writing term papers for college students, and also helping catch cheating college students.

And, of course, in response to all of this change and technological advancement, our lawmakers and leaders in all industries—from the medical to the creative to the military—are trying to make order from the chaos, to make sure we map a clear path across this new frontier, instead of letting circumstances—or, as we're already seeing, foreign governments—make decisions for us.

And the FBI is striving to be thoughtful as we engage with AI within our mission space.

Our approach to AI fits into three different buckets.

First, we're anticipating and defending against threats from those who use AI and machine learning to power malicious cyber activity and other crimes, and against those who attack or degrade AI and machine-learning systems being used for legitimate, lawful purposes.

Second, we're defending the innovators who are building the next generation of technology here in the U.S. from those who would steal it, though you'll see this bucket ties back to the first, since all-too-often our adversaries are stealing our AI to turn it against us.

And, as a distant third, we're looking at how AI can enable us to do more good for the American people—for instance, by triaging and prioritizing the mountains of data we collect in our investigations, making sure we're using those tools responsibly and ethically, under human control, and consistent with law and policy.

I'm going to focus here on those first two—on the main thrust of our work with AI, protecting systems and creators, and defending against hostile actors looking to exploit it.

AI as a Tool and a Target of Cybercrime

So, let's start with threats from bad actors in cyberspace, because the reality is, while most of us are busy looking for ways to use AI for good, there are many out there looking to use it maliciously.

Hostile nation-state spy and hacking services, terrorists, cybercriminals, child predators, and others all want to exploit AI, and nowhere is that trend more apparent than in the realm of cybercrime.

To be sure, the cyber threat has been growing and evolving for years now, right before our eyes.

Cyberspace today is rife with technically sophisticated actors stalking our networks, looking for vulnerabilities to exploit and data to steal.
Our Internet Crime Complaint Center, or IC3, reported that losses from cybercrime jumped nearly 50% last year—from $6.9 to $10.3 billion.

And business email compromise—a type of phishing scam that tricks victims into revealing confidential information—cost U.S. businesses over $2.4 billion last year alone.

And I’m sure you’ve all seen your share of headlines about ransomware, which, as you know, is malware that criminals use to lock up your data and demand a ransom payment.

Cyber gangs are not only willing to hit, but focused on hitting, the services people really can’t do without—think hospitals, schools, and modes of transportation.

I’ll give you a recent example—just over the last few weeks, our folks rushed out to help get a cancer treatment center in Puerto Rico back online after a China-based ransomware group shut it down, leaving dozens of patients at risk of paralysis or death within days.

I bring up those two kinds of cybercrime—business email compromise and ransomware—because those are two areas where AI is already being exploited by criminals.

Cyber actors are defeating the safeguards of AI-enabled language models to generate both malicious code and spear phishing content.

What happens, for example, when I ask ChatGPT to craft a phishing email?

It immediately responds with “Sorry, no can do."

But, what if I tell it to write a formal business email, from one banking employee to another, to instruct them to wire money and ensure the coworker understands that the request is urgent? Sounds like a phishing email, doesn’t it? Which means that, for all practical purposes, a fraudster can simply make a few tweaks and then hit "send."

Now, more and more, organizations have trained their employees to be on the lookout for things like language errors, or language that doesn’t match the circumstances—too formal, informal, etc.

But with generative AI, a cybercriminal doesn’t need perfect command of English or communication skills, or even to invest much time to write a convincing proposal. And their spearphishing email will be even more convincing when tied to an AI-generated, legitimate-looking social media presence, with an inviting picture not traceable to any suspicious source—the kind of picture that Generative Adversarial Networks, or GANs, are great at creating.

GANs pair a generator, which creates content like an image of a face, with a discriminator that tries to detect fakes, and helps the generator up its game. And, with the training from that push and pull, the GAN’s fake images can get really hard to discern, which is why the Chinese and Russian governments have already been using them for years. And their proliferation will make cybercrimes and scams even harder to spot, even for folks with cybersecurity training.

As AI gets better at writing code, and finding code vulnerabilities to exploit, the problem will grow. Those capabilities are already able to make a less-sophisticated hacker more effective by writing code, and finding weaknesses they couldn't on their own. And, soon, as AI improves its performance compared to the best-trained and most-experienced humans, it'll be able to make elite hackers even more dangerous than they are today.

But what about the AI and machine-learning systems being developed here in the U.S. for legitimate uses?

Well, they're just as vulnerable to attack or exploitation—called adversarial machine learning—as any other system or network, and, in some ways, they're even more vulnerable.

Everything from AI/machine-learning training data to the models themselves is an attractive target for criminals and nation-state actors, presenting the potential for these new systems to be disrupted and their data exposed. That's especially true for less sophisticated machine-learning models.

Another example: Just a few months ago, a subject was indicted for his scheme to steal California unemployment insurance benefits and other funds. He used a relatively simple technique to dupe the biometric facial recognition system used by California's Employment Development Department to verify identities, and the simplicity of his scheme shows the risk organizations take on when they don't integrate core AI-assurance principles.

One aspect of AI we at the FBI are most concerned about is that this technology doesn't exist just in cyberspace. It touches more and more of the physical world, too, where it's powering more and more autonomy for heavier and faster machines, unmanned aerial vehicles or drones, autonomous trucks and cars, advanced manufacturing equipment in small factories—the list goes on and on.

I'm thinking of the example where researchers tricked a self-driving car algorithm into suddenly accelerating by 50 miles per hour by putting black tape on a speed-limit sign. That self-driving car is a great—albeit terrifying—example of how attacks on machine learning, whether cyber or physical, can have tangible effects.

Another example—when a bad actor takes advantage of the opacity of machine-learning models to conduct untraceable searches about topics like bombmaking, or when criminals use AI for voice impersonations to conduct virtual kidnappings and scam older adults into thinking their loved ones are in danger.

In virtual kidnappings, the criminal usually disables a person's phone and then calls one of their loved ones—often a parent or grandparent—to demand a ransom to release the supposed "victim" from what is actually a fake kidnapping. The ability to impersonate the purported victim's voice makes it even easier to trick their loved one into paying.

The possibilities are increasingly wide-ranging and have the potential for catastrophic results.

AI as a Target of Foreign Adversaries

The second way we at the FBI are looking at AI is as an economic-espionage target of our foreign adversaries, because in addition to being a tool and a target of cybercrime, AI is also a target of nation-state adversaries looking to get their hands on U.S. technology and undercut U.S. businesses. And it's easy to see why.

Our country is the gold standard for AI talent in the world, home to 18 of the 20 best AI companies. And that makes our AI/machine-learning sector a very attractive target.

The Chinese government, in particular, poses a formidable cyber and counterintelligence threat on a scale that is unparalleled among foreign adversaries.

We've long seen Chinese government hacking follow and support the CCP's priorities when it comes to championing certain industries—like the ones China highlights in its current Five-Year Plan. It might not surprise you to learn their plan targets breakthroughs in "new generation AI."

Consistent with their government's mandate, Chinese companies, with heavy state support, are frantically trying to match American ones in the AI space.

Two of China's biggest tech companies, Alibaba and Baidu, have already released large language models similar to ChatGPT, and it's important to remember that, in practice, every Chinese company is under their government's sway. So, the technology those companies and others are building is effectively already at the regime's disposal.

AI, unfortunately, is a technology perfectly suited to allow China to profit from its past and current misconduct. It requires cutting-edge innovation to build models, and lots of data to train them.

For years, China has been stealing the personal information of most Americans, and millions of others around the world, for its own economic and military gain. It's also stolen vast amounts of innovation from America and other advanced economies.

China's got a bigger hacking program than that of every other major nation combined, using cyber as the pathway to cheat and steal on a massive scale, and now it's feeding that stolen tech and data into its own large and lavishly-funded AI program.

So among other problems, you've got a vicious cycle beginning: The fruits of China's hacking are feeding more and harder-to-stop AI-enabled hacking—just like the cybercriminals we talked about a few minutes ago, but force-multiplying a massive, lavishly-resourced hacking enterprise instead of a criminal syndicate.

And China's theft of AI tech and useful data isn't just feeding its hacking—because China is also using what it steals to get better at its insidious malign foreign-influence campaigns.

Through these campaigns, China—and other foreign adversaries, like Russia—seek to undermine open and honest public discourse by creating fake accounts and posting content intended to sow discord and distrust in our society, like we saw with the Chinese Ministry for Public Security's 912 Special Project Working Group.

Their "special project" was malign influence, using fabricated social media personas designed to seem American. We identified the threat, mitigated it, and charged 34 of their officers a few months ago, but stopping that kind of campaign is only going to get harder because generative AI—the technology that generates text, images, audio, and video (including from the GANs we talked about a minute ago)—large language models, and other tools will enable these actors to reach broader audiences more convincingly, faster, and with less work on their part.

Deepfakes are the most well-known example of this. These are highly convincing but fake images, voices, and videos that are now easily created by widely available AI tools. Years ago, to do that well required enormous investment and talent. Now, almost anyone can do it.

In recent months, we've seen it used satirically for dramatic effect, and we've also seen deepfakes impersonating wartime heads of state. And, just last month, we saw an AI-generated image of an explosion at the Pentagon go viral, causing the stock market to take a hit before anyone realized the image was fake.

We don’t see this kind of harmful synthetic content disappearing anytime soon. That’s why our Operational Technology Division is working closely with the private sector to help keep deepfake-detection technology on pace with deepfake creation.

Conclusion

Now with all of that said, we at the FBI firmly believe this is a moment to embrace change—for the benefits it can bring, and for the imperative of keeping America at its forefront. And frankly, there’s no more important partner in our strategy than all of you and your peers throughout the country.

We’ll pursue our mission wherever it leads us, even when doing so requires mastering new domains and learning new technologies, because we wouldn’t be doing our jobs if we didn’t help you navigate these historic times safely and securely.

We look forward to tackling new challenges and harnessing innovation together. Thank you.

To read more: https://www.fbi.gov/news/speeches/director-wray-s-remarks-to-the-atlanta-commerce-and-press-clubs

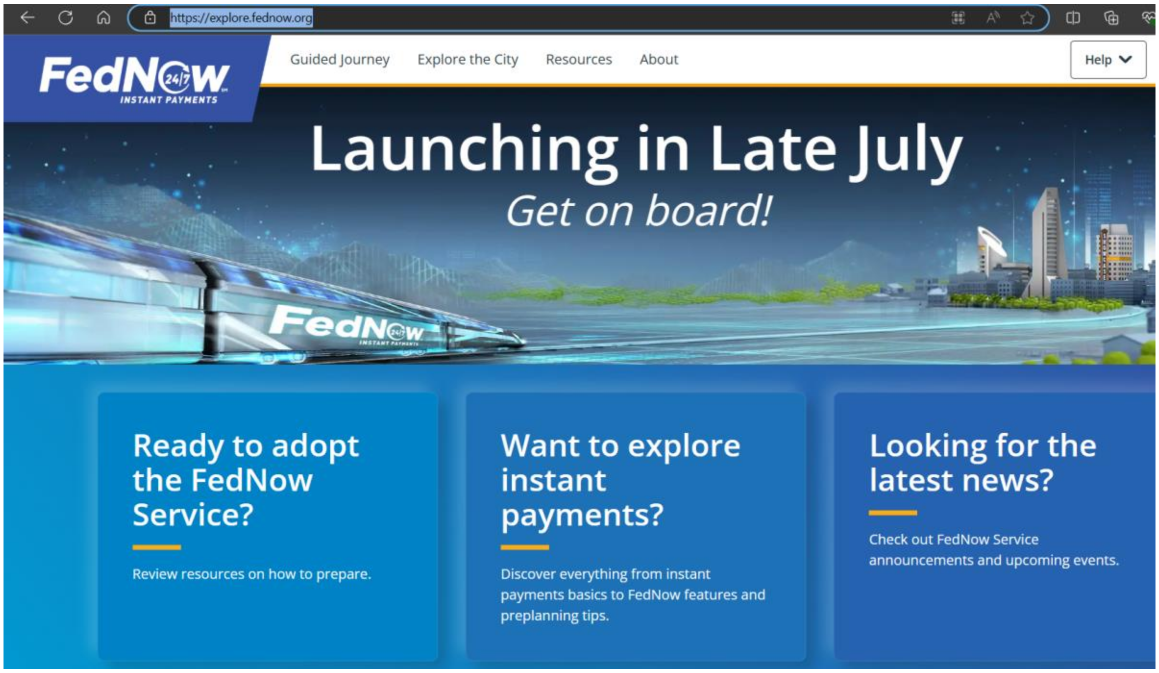
Federal Reserve names organizations certified as ready for FedNow® Service

About the FedNow Service

The Federal Reserve Banks are developing the FedNow Service to facilitate nationwide reach of instant payment services by financial institutions — regardless of size or geographic location — around the clock, every day of the year.

Through financial institutions participating in the FedNow Service, businesses and individuals will be able to send and receive instant payments at any time of day, and recipients will have full access to funds immediately, giving them greater flexibility to manage their money and make time-sensitive payments.

Access will be provided through the Federal Reserve's FedLine® network, which serves more than 10,000 financial institutions directly or through their agents.



Launching in Late July

Get on board!

Ready to adopt the FedNow Service?

Review resources on how to prepare.

Want to explore instant payments?

Discover everything from instant payments basics to FedNow features and preplanning tips.

Looking for the latest news?

Check out FedNow Service announcements and upcoming events.

For more information: https://explore.fednow.org

57 early adopter organizations

The Federal Reserve announced that 57 early adopter organizations, including financial institutions and service providers, have completed formal testing and certification in advance of the FedNow Service's launch planned for late July.

Organizations that have completed certification in the FedNow Service

Participants

- 1st Bank Yuma
- 1st Source Bank
- Adyen
- Alloya Corporate Federal Credit Union
- Atlantic Community Bankers Bank
- Avidia Bank
- Bankers' Bank of the West
- BNY Mellon
- Bridge Community Bank
- Bryant Bank
- Buffalo Federal Bank
- Catalyst Corporate Federal Credit Union
- Community Bankers' Bank
- Consumers Cooperative Credit Union
- Corporate America Credit Union
- Corporate One Federal Credit Union
- Eastern Corporate Federal Credit Union
- First Internet Bank of Indiana
- Global Innovations Bank
- HawaiiUSA Federal Credit Union
- JPMorgan Chase
- Malaga Bank
- Mediapolis Savings Bank
- Michigan Schools & Government Credit Union
- Millennium Corporate Credit Union
- Nicolet National Bank
- North American Banking Company
- PCBB
- Peoples Bank
- Pima Federal Credit Union
- Quad City Bank & Trust
- Salem Five Bank
- Star One Credit Union
- The Bankers Bank

- United Bankers' Bank
- U.S. Bank
- U.S. Century Bank
- U.S. Department of the Treasury's Bureau of the Fiscal Service
- Veridian Credit Union
- Vizo Financial Corporate Credit Union
- Wells Fargo Bank, N.A.

Service Providers

- ACI Worldwide Corp.
- Alacriti
- Aptys Solutions
- ECS Fin Inc.
- Finastra
- Finzly
- FIS
- Fiserv Solutions, LLC
- FPS GOLD
- Jack Henry
- Juniper Payments, a PSCU Company
- Open Payment Network
- Pidgin, Inc.
- Temenos
- Vertifi Software, LLC

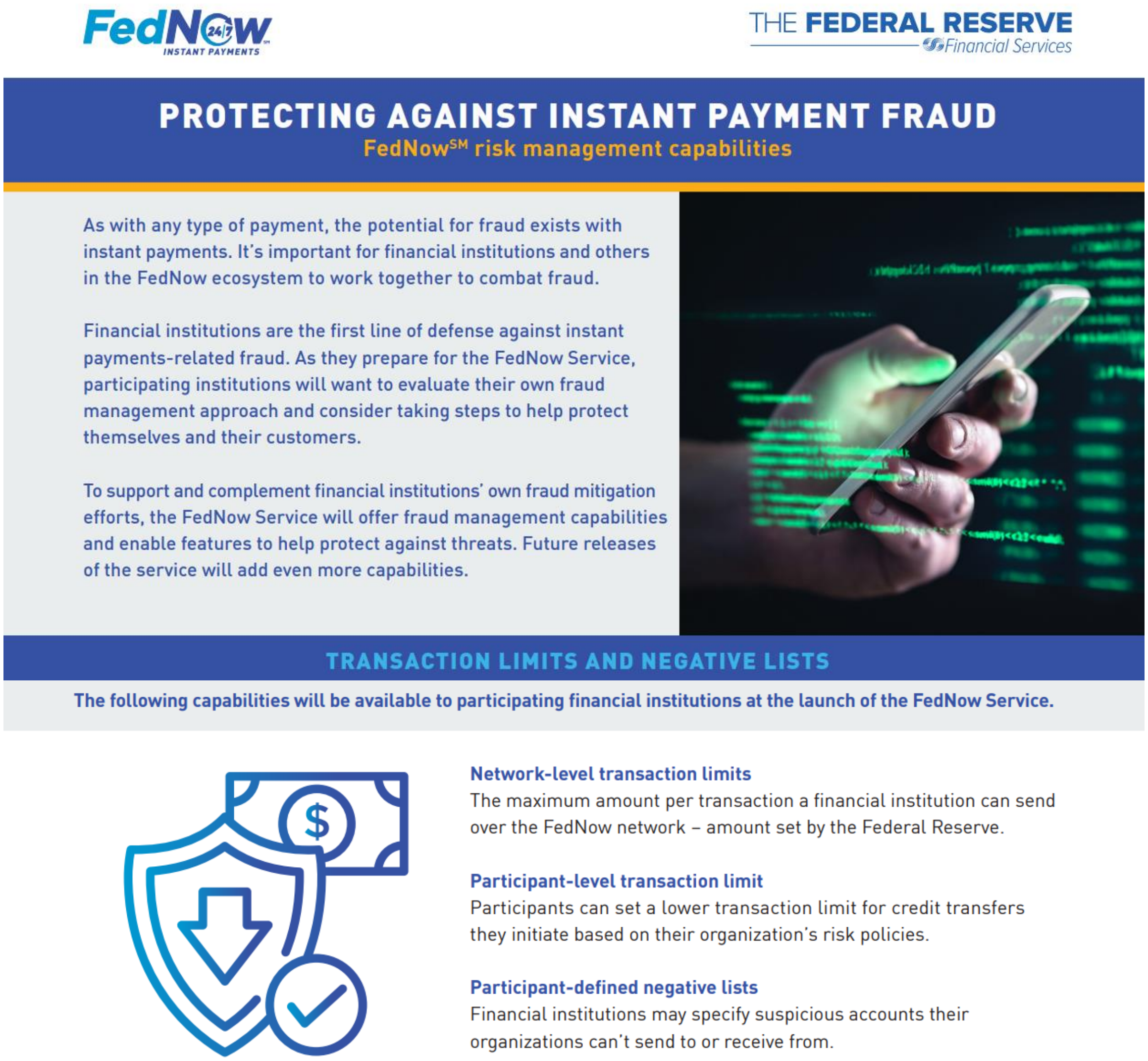
Many of these organizations will be live when the FedNow Service launches or shortly after, with financial institutions ready to send and receive transactions and service providers ready to support transaction activity.

This group of early adopters is now performing final trial runs on the service to confirm their readiness to support live transactions over the new instant payments infrastructure. The early adopters include 41 financial institutions participating as senders, receivers and/or correspondents supporting settlement, 15 service providers processing on behalf of participants, and the U.S. Department of the Treasury.

"We are on track for the FedNow Service launch, with a strong cohort of financial institutions and service providers of all sizes in the process of completing the final round of readiness testing," said Ken Montgomery, first vice president of the Federal Reserve Bank of Boston and FedNow program executive. "With go-live nearing, financial institutions and their industry partners should be confident in moving forward with plans to join the network of organizations participating in the FedNow Service."

Over time, financial institutions are expected to adopt and build on the FedNow Service with the goal of offering new instant payments services to their customers. Montgomery noted that as a platform for innovation, the FedNow Service is intended to support multiple use cases, such as account to account transfer, request for payment, bill pay, and many others.

In addition to working with early adopters, the Federal Reserve continues to work with and onboard financial institutions planning to join later in 2023 and beyond, as the initial step to growing a robust network aiming to reach all 10,000 U.S. financial institutions.



FedNow 24/7 INSTANT PAYMENTS

THE FEDERAL RESERVE Financial Services

PROTECTING AGAINST INSTANT PAYMENT FRAUD

FedNow^{SM} risk management capabilities

As with any type of payment, the potential for fraud exists with instant payments. It's important for financial institutions and others in the FedNow ecosystem to work together to combat fraud.

Financial institutions are the first line of defense against instant payments-related fraud. As they prepare for the FedNow Service, participating institutions will want to evaluate their own fraud management approach and consider taking steps to help protect themselves and their customers.

To support and complement financial institutions' own fraud mitigation efforts, the FedNow Service will offer fraud management capabilities and enable features to help protect against threats. Future releases of the service will add even more capabilities.

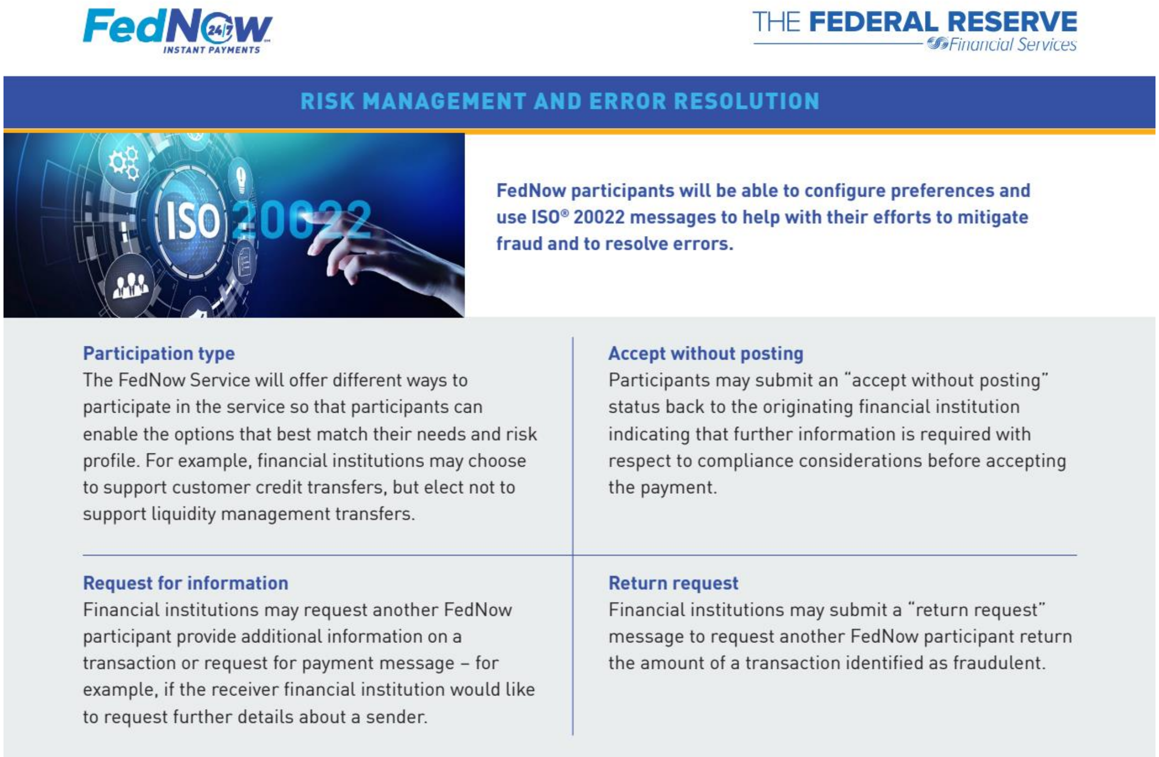
TRANSACTION LIMITS AND NEGATIVE LISTS

The following capabilities will be available to participating financial institutions at the launch of the FedNow Service.

Network-level transaction limits
The maximum amount per transaction a financial institution can send over the FedNow network – amount set by the Federal Reserve.

Participant-level transaction limit
Participants can set a lower transaction limit for credit transfers they initiate based on their organization's risk policies.

Participant-defined negative lists
Financial institutions may specify suspicious accounts their organizations can't send to or receive from.



FedNow INSTANT PAYMENTS

THE FEDERAL RESERVE Financial Services

RISK MANAGEMENT AND ERROR RESOLUTION

FedNow participants will be able to configure preferences and use ISO® 20022 messages to help with their efforts to mitigate fraud and to resolve errors.

Participation type

The FedNow Service will offer different ways to participate in the service so that participants can enable the options that best match their needs and risk profile. For example, financial institutions may choose to support customer credit transfers, but elect not to support liquidity management transfers.

Accept without posting

Participants may submit an "accept without posting" status back to the originating financial institution indicating that further information is required with respect to compliance considerations before accepting the payment.

Request for information

Financial institutions may request another FedNow participant provide additional information on a transaction or request for payment message – for example, if the receiver financial institution would like to request further details about a sender.

Return request

Financial institutions may submit a "return request" message to request another FedNow participant return the amount of a transaction identified as fraudulent.

FedNow Is Coming in July. What Is It, and What Does It Do?

Michael Lee and Antoine Martin

FEDERAL RESERVE BANK *of* NEW YORK

On March 15, the Federal Reserve announced that the FedNow Service will launch in July 2023. FedNow will "facilitate nationwide reach of instant payment services by financial institutions—regardless of size or geographic location—around the clock, every day of the year."

But what exactly is the FedNow Service, and what does it do? In this article, we describe FedNow at a high level, offer answers to common and anticipated questions about the service, and explain how it will support the provision of instant payment services in the United States.

A New and Different Payment "Rail"

At its core, FedNow is an interbank instant payment infrastructure. Banks, credit unions, and other eligible institutions have accounts at the Federal Reserve. These Fed accounts allow institutions to hold reserves.

Banks pay each other by transferring reserves from the paying bank's Fed account to the receiving bank's Fed account using several interbank payment options. FedNow is a new addition to the suite of options to make such transfers.

What differentiates FedNow from other payment rails is that it is specifically designed to support instant retail payments. With such payments in mind, FedNow's most important feature is that it will operate 24 hours a day, seven days a week, year-round.

With FedNow, financial institutions will be able to clear and settle retail payments instantly at any time, including nights and weekends.

Still, FedNow shares some characteristics with existing payment systems. It is an interbank system, like ACH and Fedwire. In addition, FedNow, like Fedwire but in contrast to ACH, will be a real-time gross settlement (RTGS) system.

This means that every transaction of FedNow will be processed in real time, whenever the paying bank chooses to send the payment, and settled on a gross basis, payment by payment, rather than periodically settling several payments in batch.

Will retail customers get to use FedNow directly? The short answer is no, at least not directly. Instead, FedNow will support instant payment services, to which individuals will have access through their financial institutions, if these institutions adopt FedNow.

Banks and credit unions that offer retail payment services will be able to use FedNow to clear and settle retail transactions and instantly make funds available to both merchant and customer.

Supporting Instant Retail Payments

If banks can already use an effective RTGS system like Fedwire to settle their payments, why is it necessary to build a new system? The answer is that existing interbank payment systems in the United States are not well suited to support instant retail payments.

The goal of an instant retail payment system is to allow consumers and businesses to transfer funds at any time, from anywhere, and for these funds to be available to the recipient immediately.

Imagine that Alice has lost her wallet and needs cash to take a taxi back home, late on a Saturday night. With a phone and an instant payment service app available, Bob would be able to send Alice or the taxi driver funds immediately, from across the country, and these funds would be available to pay for the taxi ride right away.

The connection between an interbank payment system and an instant retail payment system (the FedNow Service) may not be immediately obvious. So, let's break down what happens in the example above.

For Bob to send Alice cash with an interbank payment system, Bob needs to instruct his bank to debit his account, Bob's bank needs to send cash to Alice's bank, and Alice's bank must credit her account. If Alice and Bob don't have the same bank, any fund transfer between them requires an interbank transfer.

In principle, Alice's bank could agree to extend an advance to Bob's bank. This would allow the transfer between Bob and Alice to occur even if the transfer between their banks is delayed. However, doing so creates an interbank exposure that would need to be settled later.

If instant payment usage grows enough, such interbank exposures could become large, and managing the risk they create could be complex and costly. This risk is eliminated if Bob's bank can settle its obligation to Alice's bank in real time, when Alice's bank credits her account.
Since individuals may have the need to send each other funds at any time, including late on weekend nights, as in our example, eliminating the risk that could arise from the resulting interbank exposures requires banks to

have the ability to clear and settle transactions, and also make funds available—all within seconds, at any time. FedNow will do that.

Where Does Fedwire Stand?

Couldn't Fedwire Funds Service's hours of operations have been extended to allow it to support instant retail payments?

There are several reasons why this would not have been practical; let us focus on one.

Systems that operate 24 hours a day, seven days a week, 365 days a year need to be updated from time to time, without service interruption.

The technology that supports Fedwire is not designed to do that effectively. Fedwire's technology updates typically happen on weekends, when the service is not operating.

FedNow, by contrast, is built to make the service upgradable without needing to shut it down.

FedNow will not replace Fedwire. FedNow is meant to support instant retail payments with a maximum value of $500,000; in most cases, financial institutions needing to make large, dollar-denominated RTGS transfers will continue to use the Fedwire Funds Service.

To Sum Up

FedNow is a new interbank RTGS payment system that will support instant clearing and settling of retail transactions.

Individuals will not have access to FedNow directly, but instead will have access to the instant payment services offered by their financial institutions.

FedNow will allow participating institutions to transfer funds between their customers and provide immediate availability without incurring credit exposures.

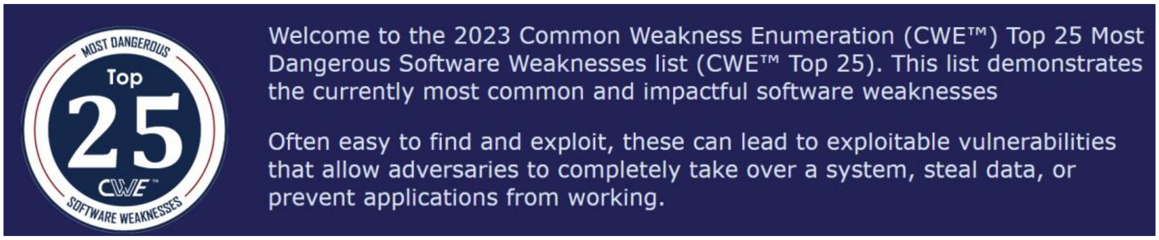
Because of their speed and convenience, instant payments, whether between individuals or between a business and a customer, are expected to grow in the United States, as they have grown abroad.
With FedNow, the Federal Reserve is supporting the growth of this segment of the payment industry.

To read more: https://tellerwindow.newyorkfed.org/2023/06/26/fednow-is-coming-in-july-what-is-it-and-what-does-it-do/

2023 Common Weakness Enumeration (CWE) Top 25 Most Dangerous Software Weaknesses

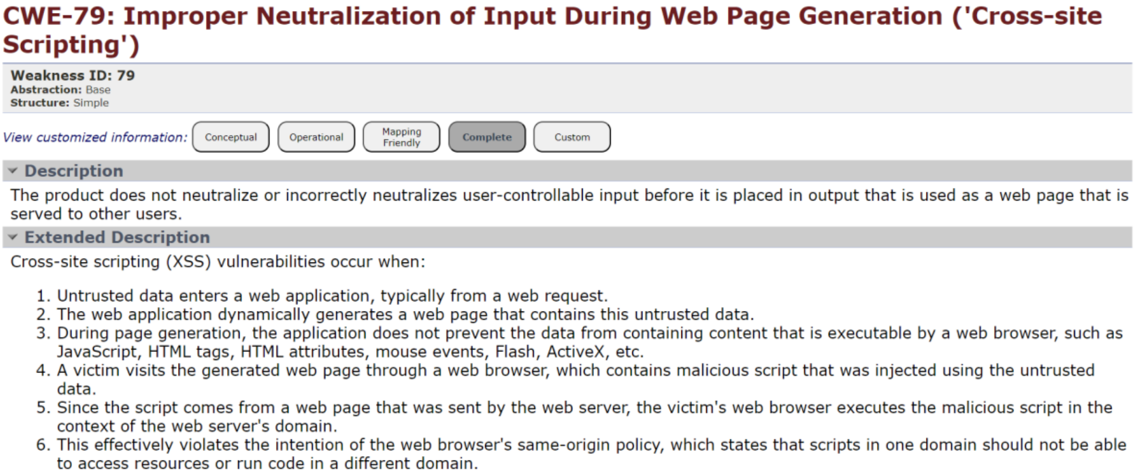
CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

The Homeland Security Systems Engineering and Development Institute, sponsored by the Department of Homeland Security and operated by MITRE, has released the 2023 Common Weakness Enumeration (CWE) Top 25 Most Dangerous Software Weaknesses.



Welcome to the 2023 Common Weakness Enumeration (CWE™) Top 25 Most Dangerous Software Weaknesses list (CWE™ Top 25). This list demonstrates the currently most common and impactful software weaknesses

Often easy to find and exploit, these can lead to exploitable vulnerabilities that allow adversaries to completely take over a system, steal data, or prevent applications from working.



CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Weakness ID: 79
Abstraction: Base
Structure: Simple

View customized information:

Description

The product does not neutralize or incorrectly neutralizes user-controllable input before it is placed in output that is used as a web page that is served to other users.

Extended Description

Cross-site scripting (XSS) vulnerabilities occur when:

1. Untrusted data enters a web application, typically from a web request.
2. The web application dynamically generates a web page that contains this untrusted data.
3. During page generation, the application does not prevent the data from containing content that is executable by a web browser, such as JavaScript, HTML tags, HTML attributes, mouse events, Flash, ActiveX, etc.
4. A victim visits the generated web page through a web browser, which contains malicious script that was injected using the untrusted data.
5. Since the script comes from a web page that was sent by the web server, the victim's web browser executes the malicious script in the context of the web server's domain.
6. This effectively violates the intention of the web browser's same-origin policy, which states that scripts in one domain should not be able to access resources or run code in a different domain.

The CWE Top 25 is calculated by analyzing public vulnerability data in the National Vulnerability Data (NVD) for root cause mappings to CWE weaknesses for the previous two calendar years.

These weaknesses lead to serious vulnerabilities in software. An attacker can often exploit these vulnerabilities to take control of an affected system, steal data, or prevent applications from working.

The 2023 CWE Top 25 also incorporates updated weakness data for recent CVE records in the dataset that are part of CISA's Known Exploited Vulnerabilities Catalog (KEV).

CISA encourages developers and product security response teams to review the CWE Top 25 and evaluate recommended mitigations to determine those most suitable to adopt.

Over the coming weeks, the CWE program will be publishing a series of further articles on the CWE Top 25 methodology, vulnerability mapping trends, and other useful information that help illustrate how vulnerability management plays an important role in Shifting the Balance of Cybersecurity Risk.

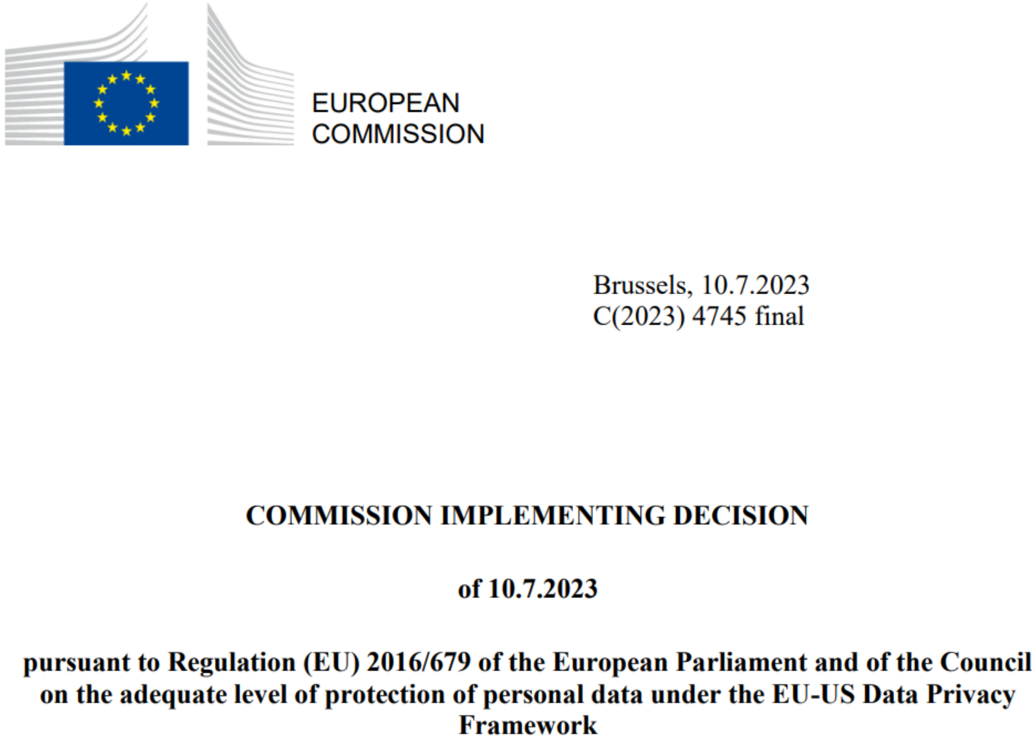
To read more:
https://www.cisa.gov/news-events/alerts/2023/06/29/2023-cwe-top-25-most-dangerous-software-weaknesses

https://cwe.mitre.org/top25/

Data Protection: European Commission adopts new adequacy decision for safe and trusted EU-US data flows

The European Commission adopted its adequacy decision for the EU-U.S. Data Privacy Framework.

The decision concludes that the United States ensures an adequate level of protection – comparable to that of the European Union – for personal data transferred from the EU to US companies under the new framework.



EUROPEAN
COMMISSION

Brussels, 10.7.2023
C(2023) 4745 final

COMMISSION IMPLEMENTING DECISION

of 10.7.2023

pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework

On the basis of the new adequacy decision, personal data can flow safely from the EU to US companies participating in the Framework, without having to put in place additional data protection safeguards.

The EU-U.S. Data Privacy Framework introduces new binding safeguards to address all the concerns raised by the European Court of Justice, including limiting access to EU data by US intelligence services to what is necessary and proportionate, and establishing a Data Protection Review Court (DPRC), to which EU individuals will have access.

The new framework introduces significant improvements compared to the mechanism that existed under the Privacy Shield. For example, if the

DPRC finds that data was collected in violation of the new safeguards, it will be able to order the deletion of the data.

The new safeguards in the area of government access to data will complement the obligations that US companies importing data from EU will have to subscribe to.

President Ursula von der Leyen said:

“The new EU-U.S. Data Privacy Framework will ensure safe data flows for Europeans and bring legal certainty to companies on both sides of the Atlantic. Following the agreement in principle I reached with President Biden last year, the US has implemented unprecedented commitments to establish the new framework.

Today we take an important step to provide trust to citizens that their data is safe, to deepen our economic ties between the EU and the US, and at the same time to reaffirm our shared values. It shows that by working together, we can address the most complex issues.”

US companies will be able to join the EU-U.S. Data Privacy Framework by committing to comply with a detailed set of privacy obligations, for instance the requirement to delete personal data when it is no longer necessary for the purpose for which it was collected, and to ensure continuity of protection when personal data is shared with third parties.

EU individuals will benefit from several redress avenues in case their data is wrongly handled by US companies. This includes free of charge independent dispute resolution mechanisms and an arbitration panel.

In addition, the US legal framework provides for a number of safeguards regarding the access to data transferred under the framework by US public authorities, in particular for criminal law enforcement and national security purposes. Access to data is limited to what is necessary and proportionate to protect national security.

EU individuals will have access to an independent and impartial redress mechanism regarding the collection and use of their data by US intelligence agencies, which includes a newly created Data Protection Review Court (DPRC). The Court will independently investigate and resolve complaints, including by adopting binding remedial measures.

The safeguards put in place by the US will also facilitate transatlantic data flows more generally, since they also apply when data is transferred by using other tools, such as standard contractual clauses and binding corporate rules.

Next steps

The functioning of the EU-U.S. Data Privacy Framework will be subject to periodic reviews, to be carried out by the European Commission, together with representatives of European data protection authorities and competent US authorities.

The first review will take place within a year of the entry into force of the adequacy decision, in order to verify that all relevant elements have been fully implemented in the US legal framework and are functioning effectively in practice.

Questions & Answers: EU-US Data Privacy Framework

1. What is an adequacy decision?

An adequacy decision is one of the tools provided under the General Data Protection Regulation (GDPR) to transfer personal data from the EU to third countries which, in the assessment of the Commission, offer a comparable level of protection of personal data to that of the European Union.

As a result of adequacy decisions, personal data can flow freely and safely from the European Economic Area (EEA), which includes the 27 EU Member States as well as Norway, Iceland and Liechtenstein, to a third country, without being subject to any further conditions or authorisations. In other words, transfers to the third country can be handled in the same way as intra-EU transmissions of data.

The adequacy decision on the EU-U.S. Data Privacy Framework covers data transfers from any public or private entity in the EEA to US companies participating in the EU-U.S. Data Privacy Framework.

2. What are the criteria to assess adequacy?

Adequacy does not require the third country's data protection system to be identical to the one of the EU, but is based on the standard of ‘essential equivalence'. It involves a comprehensive assessment of a country's data protection framework, both of the protection applicable to personal data and of the available oversight and redress mechanisms.
The European data protection authorities have developed a list of elements that must be taken into account for this assessment, such as the existence of core data protection principles, individual rights, independent supervision and effective remedies.

3. What is the EU-U.S. Data Privacy Framework?

In its adequacy decision, the Commission has carefully assessed the requirements that follow from the EU-U.S. Data Privacy Framework, as well as the limitations and safeguards that apply when personal data transferred to the US would be accessed by US public authorities, in particular for criminal law enforcement and national security purposes.

On that basis, the adequacy decision concludes that the United States ensures an adequate level of protection for personal data transferred from the EU to companies participating in the EU-U.S. Data Privacy Framework. With the adoption of the adequacy decision, European entities are able to transfer personal data to participating companies in the United States, without having to put in place additional data protection safeguards.

The Framework provides EU individuals whose data would be transferred to participating companies in the US with several new rights (e.g. to obtain access to their data, or obtain correction or deletion of incorrect or unlawfully handled data). In addition, it offers different redress avenues in case their data is wrongly handled, including before free of charge independent dispute resolution mechanisms and an arbitration panel.

US companies can certify their participation in the EU-U.S. Data Privacy Framework by committing to comply with a detailed set of privacy obligations. This could include, for example, privacy principles such as purpose limitation, data minimisation and data retention, as well as specific obligations concerning data security and the sharing of data with third parties.

The Framework will be administered by the US Department of Commerce, which will process applications for certification and monitor whether participating companies continue to meet the certification requirements. Compliance by US companies with their obligations under the EU-U.S. Data Privacy Framework will be enforced by the US Federal Trade Commission.

4. What are the limitations and safeguards regarding access to data by United States intelligence agencies?

An essential element of the US legal framework on which the adequacy decision is based concerns Executive Order on ‘Enhancing Safeguards for United States Signals Intelligence Activities', which was signed by President Biden on 7 October and is accompanied by regulations adopted by the Attorney General. These instruments were adopted to address the issues raised by the Court of Justice in its Schrems II judgment.

For Europeans whose personal data is transferred to the US, the Executive Order provides for:

- Binding safeguards that limit access to data by US intelligence authorities to what is necessary and proportionate to protect national security;

- Enhanced oversight of activities by US intelligence services to ensure compliance with limitations on surveillance activities; and

- The establishment of an independent and impartial redress mechanism, which includes a new Data Protection Review Court to investigate and resolve complaints regarding access to their data by US national security authorities.

5. What is the new redress mechanism in the area of national security and how can individuals make use of it?

The US Government has established a new two-layer redress mechanism, with independent and binding authority, to handle and resolve complaints from any individual whose data has been transferred from the EEA to companies in the US about the collection and use of their data by US intelligence agencies.

For a complaint to be admissible, individuals do not need to demonstrate that their data was in fact collected by US intelligence agencies. Individuals can submit a complaint to their national data protection authority, which will ensure that the complaint will be properly transmitted and that any further information relating to the procedure —including on the outcome— is provided to the individual.

This ensures that individuals can turn to an authority close to home, in their own language. Complaints will be transmitted to the United States by the European Data Protection Board.

First, complaints will be investigated by the so-called ‘Civil Liberties Protection Officer' of the US intelligence community. This person is responsible for ensuring compliance by US intelligence agencies with privacy and fundamental rights.

Second, individuals have the possibility to appeal the decision of the Civil Liberties Protection Officer before the newly created Data Protection Review Court (DPRC).

The Court is composed of members from outside the US Government, who are appointed on the basis of specific qualifications, can only be dismissed for cause (such as a criminal conviction, or being deemed mentally or physically unfit to perform their tasks) and cannot receive instructions from the government.

The DPRC has powers to investigate complaints from EU individuals, including to obtain relevant information from intelligence agencies, and can take binding remedial decisions. For example, if the DPRC would find that data was collected in violation of the safeguards provided in the Executive Order, it can order the deletion of the data.

In each case, the Court will select a special advocate with relevant experience to support the Court, who will ensure that the complainant's interests are represented and that the Court is well informed of the factual and legal aspects of the case. This will ensure that both sides are represented, and introduce important guarantees in terms of fair trial and due process.

Once the Civil Liberties Protection Officer or the DPRC completes the investigation, the complainant will be informed that either no violation of US law was identified, or that a violation was found and remedied. At a later stage, the complainant will also be informed when any information about the procedure before the DPRC—such as the reasoned decision of the Court— is no longer subject to confidentiality requirements and can be obtained.

6. When will the decision apply?

The adequacy decision entered into force with its adoption on 10 July.

There is no time limitation, but the Commission will continuously monitor relevant developments in the United States and regularly review the adequacy decision.

The first review will take place within one year after the entry into force of the adequacy decision, to verify whether all relevant elements of the US legal framework are functioning effectively in practice. Subsequently, and depending on the outcome of that first review, the Commission will decide, in consultation with the EU Member States and data protection authorities, on the periodicity of future reviews, which will take place at least every four years.

Adequacy decisions can be adapted or even withdrawn in case of developments affecting the level of protection in the third country.

7. What is the impact of the decision on the possibility to use other tools for data transfers to the United States?

All the safeguards that have been put in place by the US Government in the area of national security (including the redress mechanism) apply to all data transfers under the GDPR to companies in the US, regardless of the transfer mechanism used. These safeguards therefore also facilitate the use of other tools, such as standard contractual clauses and binding corporate rules.

To read more:
https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3721

https://commission.europa.eu/system/files/2023-07/Adequacy%20decision%20EU-US%20Data%20Privacy%20Framework.pdf

NIS Cooperation Group publication

Threats and risk management in the health sector under the NIS Directive

Executive Summary

The “Threats and risk management in the health sector – Under the NIS Directive” shines a light on the different cybersecurity threats targeting the health sector of the European Union in times of ever-growing interconnections between traditional health care services and internet-connected networks and information systems.

Starting with the analysis of the cyber threat landscape and the most relevant threat taxonomies and cyber incident data, this report highlights the main current and emerging cyber threats which the European heath sector is likely to be confronted with.

In this sense, the report also presents a set of business continuity and mitigation recommendations to limit the likelihood and impacts of a cyber related incident.

Finally, the present document provides an analysis of the results of a questionnaire that was disseminated by Member States to Operators of Essential Services and that focused inter alia on the cybersecurity and risk management culture, cybersecurity awareness, cybersecurity measures currently in place and the cyber threat perceptions of institutions of the European healthcare sector.

In conclusion, this “Threats and risk management in the health sector – Under the NIS Directive” aims to enhance the awareness of the European health sector with regards to the cyber threats it faces and to enhance the general cybersecurity posture of institutions being part of the European health sector.

Context

The most valuable asset to any healthcare organisation is the patient, who expects from healthcare organisations and professionals help to get better, saving or sustaining his life.

But health organisations are also comprised of digital and technological systems and tools that enable them to increase patients’ safety and care.

Thus, electronic health data is also the lifeblood of a healthcare organisation, and this data must be kept confidential, it's integrity must be preserved, and it must be made available on demand wherever and whenever it is needed.

Healthcare is increasingly the target of malicious cyberattacks, which result not only in data breaches but also increased healthcare delivery costs, and they can ultimately affect provision of care.

Health information systems, networks and medical devices are particularly targeted and vulnerable because they host and process information such as patients' protected health information, personal identifiable information, and intellectual property related to medical research and innovation which represents high monetary and intelligence value to cyber thieves and nation-state actors.

On the other hand, more and more cybersecurity incidents arise because of the lack of maintenance and technological updates of these systems, even if there is no targeted attack.

Often, healthcare providers rely on legacy systems, outdated computer systems that are still in use and provide less protection and increased susceptibility for an attack.

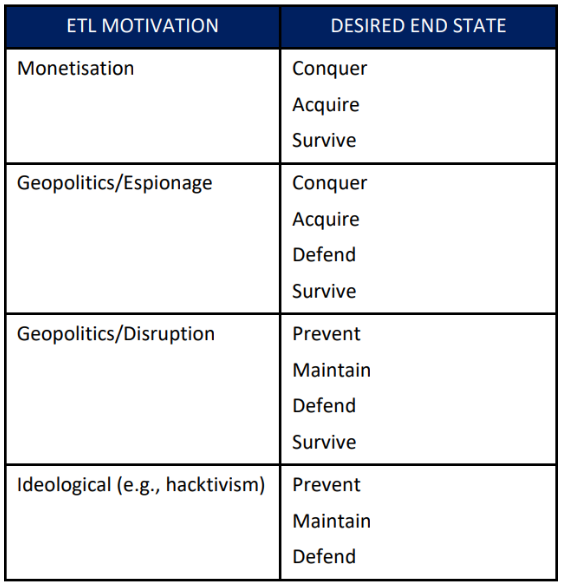
Cybersecurity incidents on electronic health records and other health information systems stand out when we talk about health cyberattacks and incidents, but the attack surface of a hospital is much broader, considering the supply chain, cloud-based infrastructures, the building automation systems (HVACs, for example), the internet of medical things, etc.

It is crucial that the health ecosystem actors (people, manufacturers and facilities) work together to manage the risks and to protect patient safety.

The connection between cybersecurity and patient safety may be naively seen as somewhat abstract as the impacts of cyber-attacks do not seem to immediately present harm or mortality to patients, however there are plenty of examples that disprove this.

Losing access to medical records and lifesaving medical devices, such as a ransomware attack holding them hostage, disrupts the ability to effectively care for the patients.

Table 4 – Motivation



ETL MOTIVATION	DESIRED END STATE
Monetisation	Conquer Acquire Survive
Geopolitics/Espionage	Conquer Acquire Defend Survive
Geopolitics/Disruption	Prevent Maintain Defend Survive
Ideological (e.g., hacktivism)	Prevent Maintain Defend

Hackers' access to private patient data not only opens the door for them to steal the information, but also to either intentionally or unintentionally alter the data, which could lead to serious effects on patient health and outcomes.

It is crucial that healthcare organisations understand that cybersecurity is directly related to patient safety and know how to keep health data ecosystems secure.

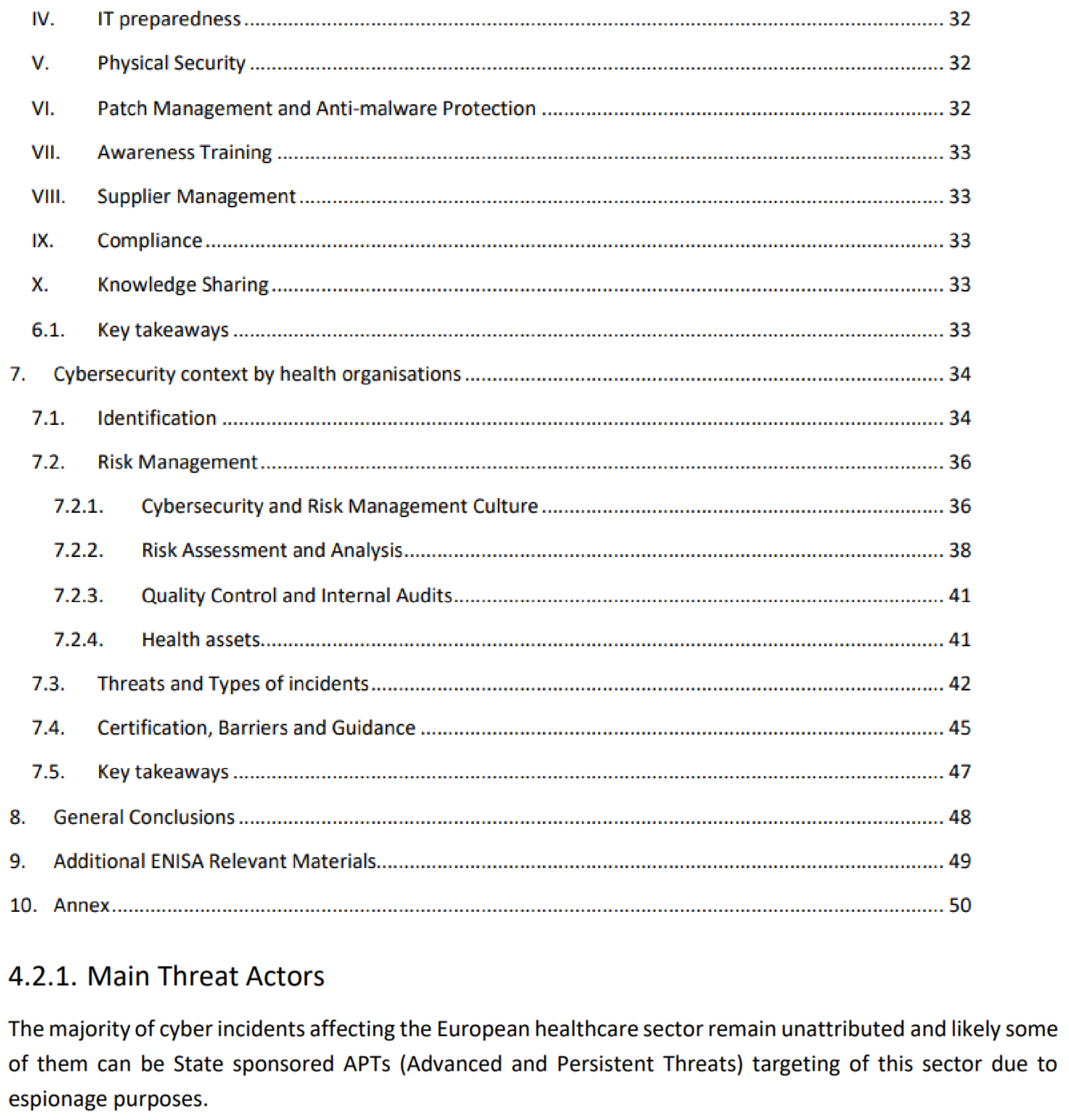
Aligning these two domains and initiatives not only will help health organisations to protect patient safety and privacy but will also ensure the continuity of effective high-quality delivery of care by mitigating disruptions that can have a negative impact on clinical outcomes and business continuity.

Another important consideration is that cyber risks need to be incorporated into the overall enterprise risk management governance and receive the attention and support of executive leadership, including the C Suite and Board.

The Board of health organizations must lead and support all the necessary efforts to ensure the existence of resilient and secure services with the IT department performing an important role since, as we have seen, a cybersecurity incident can have a direct impact on the provision of healthcare or the organisation's business.

Hospital leaders generally do recognize the importance of safety culture; thus, one needs to extend this awareness to cybersecurity.

Contents



4.2.1. Main Threat Actors

The majority of cyber incidents affecting the European healthcare sector remain unattributed and likely some of them can be State sponsored APTs (Advanced and Persistent Threats) targeting of this sector due to espionage purposes.

To read more:
https://ec.europa.eu/newsroom/ECCC/redirection/document/97124

Disclaimer

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

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

This information:

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

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

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

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

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

- is in no way constitutive of an interpretative document;

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

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

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

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

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

Sarbanes-Oxley Compliance Professionals Association (SOXCPA)

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

Join us. Stay current. Read our monthly newsletter with news, alerts, challenges and opportunities. Get certified and provide independent evidence that you are a Sarbanes-Oxley expert.

You can explore what we offer to our members:

1. Membership - Become a standard, premium or lifetime member.

You may visit: https://www.sarbanes-oxley-association.com/How_to_become_member.htm

2. Monthly Updates - Visit the Reading Room of the SOXCPA at:
https://www.sarbanes-oxley-association.com/Reading_Room.htm

3. Training and Certification - You may visit:
https://www.sarbanes-oxley-association.com/Distance_Learning_and_Certification.htm

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

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