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, February 2022

Dear members and friends,

The Securities and Exchange Commission has issued its annual Staff Report on Nationally Recognized Statistical Rating Organizations (NRSROs), providing a summary of the SEC staff's examinations of NRSROs and discussing the state of competition, transparency, and conflicts of interest among NRSROs.

In past years, the SEC's Office of Credit Ratings (OCR) covered these subject areas in two separate annual reports. The combined report includes a variety of substantive and organizational changes to provide greater transparency about NRSROs and their credit ratings businesses, and the market more broadly.

"The oversight of Nationally Recognized Statistical Rating Organizations is critical to the Commission's focus on investor protection," said SEC Chair Gary Gensler. "The Office of Credit Ratings' work contributes to our efforts to promote accuracy in credit ratings and help ensure that credit ratings are not unduly influenced by conflicts of interest."

"OCR's examinations protect investors by scrutinizing NRSRO compliance with applicable laws and rules and identifying instances of non-compliance," said OCR Director Ahmed Abonamah. "The report provides a comprehensive and integrated overview of OCR's activities, demonstrating the exceptional work of my colleagues in their efforts to protect investors."

The report highlights the risk-based approach of OCR's examination program. As described in the report, in addition to the eight statutorily mandated review areas, OCR staff examined the NRSROs':

- Consideration of ESG factors and products;
- COVID-19 related risk areas;
- Activities related to collateralized loan obligations, commercial real estate, and consumer asset-backed securities;
- Adherence to policies, procedures, and methodologies with respect to rating low-investment grade corporate securities; and
- Controls, policies, and procedures for ratings of municipal securities.

To read more: https://www.sec.gov/news/press-release/2022-15

The report: https://www.sec.gov/files/2022-ocr-staff-report.pdf

CHARTS ii

I. MESSAGE FROM THE DIRECTOR 1

II. INTRODUCTION 3
A. Status of Registrants and Applicants 4

III. EXAMINATIONS AND MONITORING. 7
A. Overview 7
B. Risk Assessment 7
C. Monitoring. 9
D. 2021 Section 15E(p)(3) Examinations 10
1. 2021 Section 15E Examinations 10
2. Terms Used in This Report 11
3. Summary of Essential Findings and Responses to Material Regulatory Deficiencies. . 12
4. Responses to Recommendations from the 2020 Section 15E Examinations 18
5. Essential Findings Trends 19

IV. STATE OF COMPETITION, TRANSPARENCY, AND CONFLICTS OF INTEREST 21
A. Competition. 21
1. Select NRSRO Statistics. 21
2. Developments in the State of Competition Among NRSROs 32
3. Barriers to Entry 41
B. Transparency 43
C. Conflicts of Interest 45

V. ACTIVITIES RELATING TO NRSROS 49
A. Commission Orders and Releases. 49
B. Staff Publications. 50
C. Advisory Committees 50

VI. APPENDIX: SUMMARY OF STATUTORY FRAMEWORK AND RULES 51

Federal Reserve Board invites public comment on proposed guidance to implement a framework for the supervision of certain insurance organizations overseen by the Board

The Federal Reserve Board invited public comment on proposed guidance to implement a framework for the supervision of certain **insurance** organizations overseen by the Board.

The proposed supervisory framework—for depository institution holding companies significantly engaged in insurance activities—would apply guidance and allocate supervisory resources based on the risk of a firm.

It would also formalize a supervisory rating system for these companies and describe how examiners work with state insurance regulators.

The proposed guidance would apply to any depository institution holding company that is an insurance underwriting company or that has over 25 percent of its consolidated assets held by insurance underwriting subsidiaries.

Comments will be accepted for 60 days after publication in the Federal Register.

Summary

The Board is seeking comment on a new supervisory framework for depository institution holding companies significantly engaged in insurance activities, or supervised insurance organizations.

The proposed framework would provide a supervisory approach that is designed specifically to reflect the differences between banking and insurance.

Within the framework, the application of supervisory guidance and the assignment of supervisory resources would be based explicitly on a supervised insurance organization's complexity and individual risk profile.

The proposed framework would formalize the ratings applicable to these firms with rating definitions that reflect specific supervisory requirements and expectations.

It would also emphasize the Board's policy to rely to the fullest extent possible on work done by other relevant supervisors, describing, in particular, the way it will rely more fully on reports and other supervisory information provided by state insurance regulators to minimize the burden associated with supervisory duplication.

To read more:
https://www.federalreserve.gov/newsevents/pressreleases/bcreg20220128a.htm

https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20220128a2.pdf

Cybersecurity at US federal agencies

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

According to Shalanda Young, the acting director for the Office of Management and Budget (OMB), agencies will be transitioning to a "zero trust" approach that assumes no actor, system or network operating outside the security perimeter is to be trusted.

M-22-09

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Shalanda D. Young
Acting Director

SUBJECT: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles

This memorandum sets forth a Federal zero trust architecture (ZTA) strategy, requiring agencies to meet specific cybersecurity standards and objectives by the end of Fiscal Year (FY) 2024 in order to reinforce the Government's defenses against increasingly sophisticated and persistent threat campaigns. Those campaigns target Federal technology infrastructure, threatening public safety and privacy, damaging the American economy, and weakening trust in Government.

I. OVERVIEW

Every day, the Federal Government executes unique and deeply challenging missions: agencies [1] safeguard our nation's critical infrastructure, conduct scientific research, engage in diplomacy, and provide benefits and services for the American people, among many other public functions. To deliver on these missions effectively, our nation must make intelligent and vigorous use of modern technology and security practices, while avoiding disruption by malicious cyber campaigns.

Successfully modernizing the Federal Government's approach to security requires a Government-wide endeavor. In May of 2021, the President issued Executive Order (EO) 14028, *Improving the Nation's Cybersecurity*,[2] initiating a sweeping Government-wide effort to ensure that baseline security practices are in place, to migrate the Federal Government to a zero trust architecture, and to realize the security benefits of cloud-based infrastructure while mitigating associated risks.

This memorandum requires agencies to achieve specific zero trust security goals by the **end of Fiscal Year (FY) 2024**. These goals are organized using the zero trust maturity model developed by CISA. CISA's zero trust model describes five complementary areas of effort (pillars) (Identity, Devices, Networks, Applications and Workloads, and Data), with three themes that cut across these areas (Visibility and Analytics, Automation and Orchestration, and Governance).

The strategic goals set forth in this memorandum align with CISA's five pillars:

1. Identity: Agency staff use enterprise-managed identities to access the applications they use in their work. Phishing-resistant MFA protects those personnel from sophisticated online attacks.

2. Devices: The Federal Government has a complete inventory of every device it operates and authorizes for Government use, and can prevent, detect, and respond to incidents on those devices.

3. Networks: Agencies encrypt all DNS requests and HTTP traffic within their environment, and begin executing a plan to break down their perimeters into isolated environments.

4. Applications and Workloads: Agencies treat all applications as internet-connected, routinely subject their applications to rigorous empirical testing, and welcome external vulnerability reports.

5. Data: Agencies are on a clear, shared path to deploy protections that make use of thorough data categorization. Agencies are taking advantage of cloud security services to monitor access to their sensitive data, and have implemented enterprise-wide logging and information sharing.

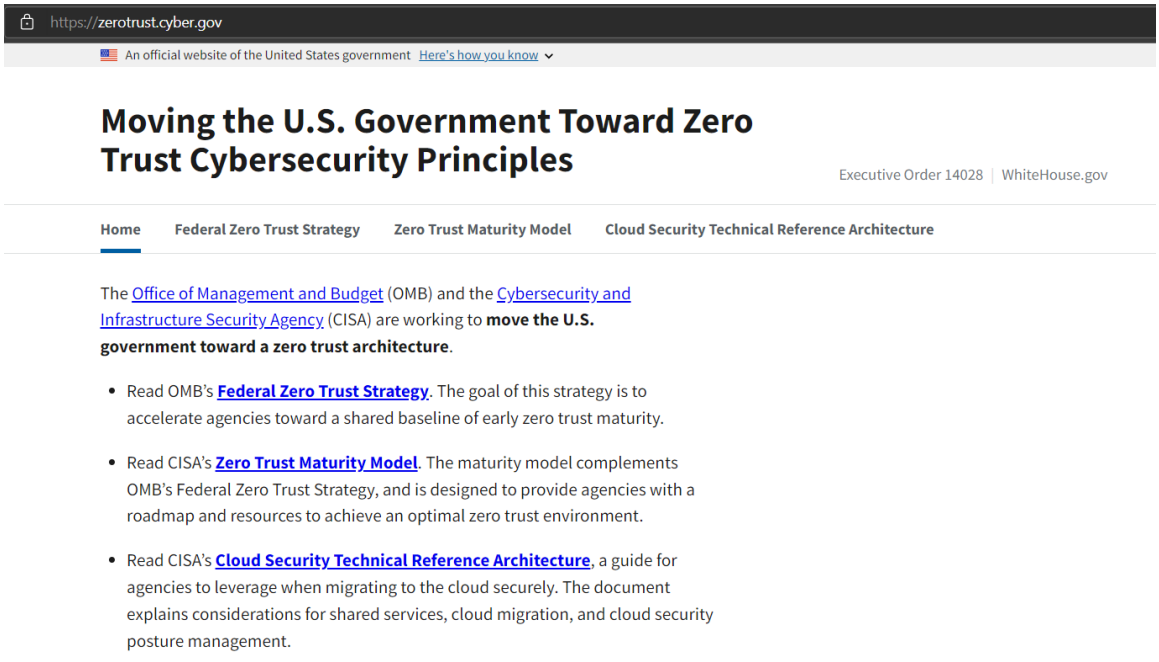
EO 14028 required agencies to develop their own plans for implementing zero trust architecture. Within 60 days of the date of this memorandum, agencies must build upon those plans by incorporating the additional requirements identified in this document and submitting to OMB and CISA an implementation plan for FY22-FY24 for OMB concurrence, and a budget estimate for FY24.

Agencies should internally source funding in FY22 and FY23 to achieve priority goals, or seek funding from alternative sources, such as working capital funds or the Technology Modernization Fund.

Agencies will have 30 days from the publication of this memorandum to designate and identify a **zero trust strategy implementation lead** for their organization.

OMB will rely on these designated leads for Government-wide coordination and for engagement on planning and implementation efforts within each organization.

OMB and CISA will work with agencies throughout zero trust implementations to capture best practices, lessons learned, and additional agency guidance on a jointly maintained website at https://zerotrust.cyber.gov/



To read more: https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf

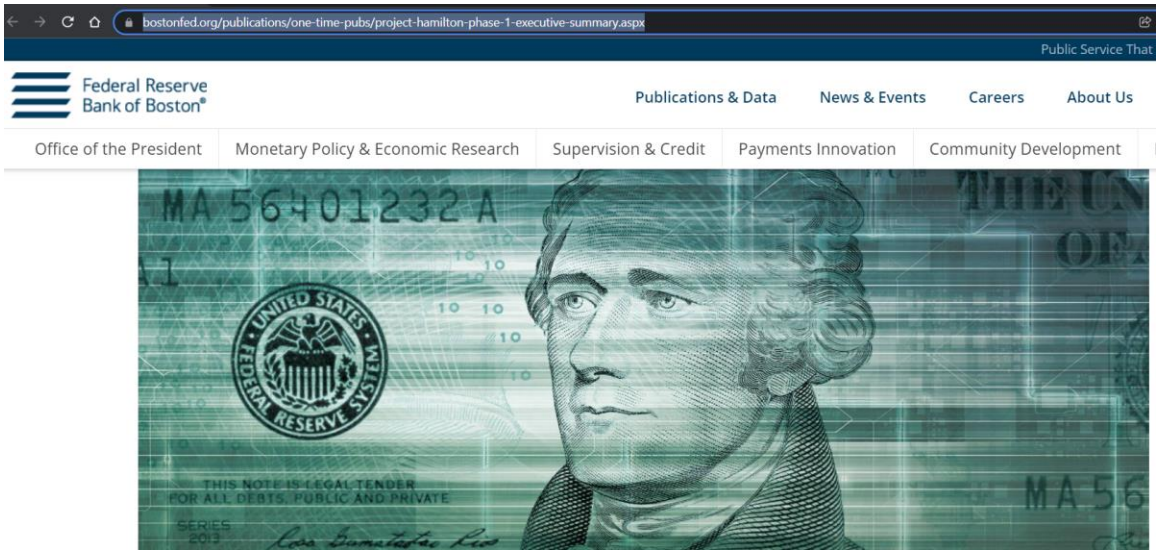
The Federal Reserve Bank of Boston and Massachusetts Institute of Technology release technological research on a central bank digital currency

Federal Reserve Bank of Boston®

The Federal Reserve Bank of Boston and the Digital Currency Initiative (https://dci.mit.edu/)at the Massachusetts Institute of Technology released the findings of their initial technological research into a central bank digital currency, or CBDC.

digital currency initiative | mit media lab

The published research describes a theoretical high-performance and resilient transaction processor for a CBDC that was developed using open-source research software, OpenCBDC. You may visit: https://www.bostonfed.org/publications/one-time-pubs/project-hamilton-phase-1-executive-summary.aspx



This collaborative effort, known as Project Hamilton, focuses on technological experimentation and does not aim to create a usable CBDC for the United States. The research is separate from the Federal Reserve's Board's evaluation of the pros and cons of a CBDC.

"It is critical to understand how emerging technologies could support a CBDC and what challenges remain," said Boston Fed Executive Vice President and Interim Chief Operating Officer Jim Cunha. "This

collaboration between MIT and our technologists has created a scalable CBDC research model that allows us to learn more about these technologies and the choices that should be considered when designing a CBDC."

The whitepaper released today details findings from the first research phase. In this phase, researchers selected concepts from cryptography, distributed systems, and blockchain technology to build and test platforms that would give policymakers substantial flexibility in the potential creation of a CBDC. The paper describes the following findings:

- The team met its goal of creating a core processing engine for a hypothetical general purpose CBDC and explored it in two architectures.

- The work produced one code base capable of handling 1.7 million transactions per second.

- The vast majority of transactions reached settlement finality in under two seconds within architectures that support secure, resilient performance and offer the significant technological flexibility required to adjust to future policy direction.

Researchers with MIT and the Boston Fed released the code for Project Hamilton, OpenCBDC.

"There are still many remaining challenges in determining whether or how to adopt a central bank payment system for the United States," said Neha Narula, director of the Digital Currency Initiative at MIT. "What is clear is that open-source software provides an important way to collaborate, experiment, and implement. In addition to supporting collaboration, monetary systems benefit from transparency and verifiability, which open-source offers."

About Project Hamilton

Project Hamilton is a multi-year collaboration between the Boston Fed and MIT's Digital Currency Initiative that was announced in 2020. The project explores the use of existing and new technologies to build and test a hypothetical digital currency platform.

The project's first phase produced the research and code released today for a high-performance transaction processor. The code is the first contribution to OpenCBDC, a project maintained by MIT which will serve as a platform for further CBDC research. Project Hamilton aims to inform future contributions to the code and inform policy discussions about CBDC.

In the coming years, the second phase of this partnership will allow Project Hamilton to explore alternative technical designs to improve the already robust privacy, resiliency, and functionality of the technology outlined in the first phase.

The Federal Reserve Bank of Boston serves the First Federal Reserve District, which includes all of New England except Fairfield County, Connecticut.

Within the district, the Bank monitors local economic conditions to aid in the formulation of monetary policy; engages in outreach to promote economic growth, community revitalization, and economic and financial education; supervises banks and bank holding companies; and provides financial services to facilitate banking operations.

Recent Cyber Events: Considerations for Military and National Security Decision Makers

Reflections on 2021

2021 was an exciting year from a cybersecurity and cyber defence perspective. After dealing with the Solarwinds breach at the beginning of the year, the world experienced a series of serious ransomware incidents, in some cases causing disturbances to essential services.

We also saw governments expressing their commitment to protecting critical services and to responding forcefully to nations carrying out malicious cyber operations or allowing criminals to do so.

While impossible to cover all these developments in a brief report, we will take this opportunity to reflect on three important topics: ransomware, software supply chain security and spyware.

Perhaps looking at these from a little distance will help us see the larger picture and allow us to prepare better for the future.

The ransomware threat

Malicious cyber activity has grown substantially over the past two years while the world has been learning how to keep turning with the omnipresent pandemic.

One particular malware category, ransomware, made headlines frequently in 2021, partly because the operations were increasingly targeting high-value targets.

One of the first major ransomware incidents in 2021 may have been against the automakers Kia and Hyundai, although this has been denied by the alleged victims.

The actors behind the compromise appear to have used the now common double extortion tactics, not only causing an outage but also threatening to expose data exfiltrated from the victims' systems.

In March, CNA Financial, the seventh-largest commercial insurer in the US, fell victim to ransomware.

Shortly thereafter in April, the North American division of Brenntag, a German chemical distributor, faced a ransomware infection of their systems as well.

One of the most public ransomware incidents of this year was against Colonial Pipeline in May, an incident that was discussed in a previous issue of this series.

The largest fuel pipeline was shut down as a result of a ransomware attack. This led to fuel shortages across the US East Coast and an increase in fuel prices.

In the same month JBS, one of the largest meat suppliers in the US, suffered a compromise which caused it to temporarily shut down five of its plants and this also affected operations in the UK and Australia.

In July, Kaseya, an international IT service provider, announced it had fallen victim to ransomware which affected and shut down numerous companies in several countries.

For example, Sweden's third largest grocery chain had to close down 800 stores for several days, some of them in remote areas with very few to no alternatives.

Over the past two years, hospitals have also seen an increase in malicious cyber operations, though not limited to ransomware.

One of the most prominent victims was Ireland's health service which resulted in stolen patient data, the cancellation of appointments and delayed treatment.

Other known incidents targeted health companies in the US and New Zealand.

These attacks not only show how closely linked our society and systems have become, but also how vulnerable and highly dependent on the functioning of national critical infrastructure (CI) our societies now are.

According to the Department of Homeland Security (DHS), 16 CI sectors are considered to be of vital importance for the population of the US.

Similar examples of sectorial divisions of CI can be found in almost any country; for example, 12 have been identified in France and 13 in the UK.

The incidents mentioned above have all affected one or more of those sectors.

Due to the close interconnection of systems and services, all sectors are potential targets and a compromise of one can have a domino effect on others with severe consequences.

It is therefore of the utmost importance that nations define and strengthen their CI sectors and put in place contingencies to deal with any compromise.

Resilience need not only be built by having more robust or redundant digital systems. In many instances, we need to be prepared to operate without industrial control systems, or even to compensate for services affected by a cyberattack by other means, such as using local electrical generators to compensate for a power outage or to ship oil by sea or rail if pipelines are not operational.

Most of the companies targeted in the examples ended up paying ransom up to as high as $40 Million, even though the FBI and others advise against paying a ransom as it is no guarantee of getting data back and it incentivises criminals.

Discussions of public response to cyber threats have entered the military and political level as never before, with many states beginning to take steps both towards increasing the cyber security of CI on a national level through regulations or imposing costs on those responsible for malicious cyber operations.

This is intended to constitute deterrence both by denial of benefits and by the threat of retaliation.

The US government, for example, has taken a more active stance and combined resources from Cyber Command, NSA and other agencies and from international partners to lift responsibility to an all-of-government effort, including law enforcement.

Public declarations will need to be followed by clear action such as the reported capture of 12 suspects for involvement in ransomware operations by Europol in November 2021.

This type of layered approach to deterrence is critical to any kind of success and we can only hope that this will continue in the new year and that the results of such an approach will soon grow.

To read more:
https://ccdcoe.org/uploads/2022/02/Report_Reflections_on_2021_A4.pdf

DARPA Researchers Use Light on Chip to Drive Next-Generation RF Platforms

Integrated optical approaches could allow tuning over multiple frequency bands

Radio frequency (RF) and microwave signals invisibly permeate the environment around us, carrying everything from radar signatures to the data from our mobile phones.

Within RF systems, electronic oscillators can act as precise clocks or directly generate the baseline microwave tones.

While an ideal oscillator provides a tone at a singular frequency, component imperfections and coupling to the environment introduce significant phase noise to real-world sources.

Military and commercial drivers for better oscillators are plentiful: Close-to-carrier phase noise is a primary factor preventing the detection of small or slow-moving targets in Doppler radar, while in RF communications, timing jitter dictates the sampling precision of receivers and limits signaling bandwidth.

In the last decade, major advances in RF oscillator performance have been realized using optical techniques to synthesize high-fidelity microwave signals (i.e., frequencies from 1 to 100 GHz). Such RF oscillators typically employ optical frequency division (OFD) to achieve low phase noise that can reach record-setting levels.

Current solutions sacrifice other important attributes, however, in pursuit of spectral purity. Such trade-offs are problematic because module size, cost, tunability, and environmental sensitivity are also critical factors that determine the applicability of microwave sources to commercial and military systems.

The Generating RF with Photonic Oscillators for Low Noise (GRYPHON) program seeks to defy today's tradeoffs by leveraging recent advancements in the miniaturization, integration, and volume production of precision optical components through lithographic microelectronic fabrication.

"Nonlinear integrated photonics provides a path to achieve incredible oscillator performance while reducing system size by orders of magnitude," says Dr. Gordon Keeler, program manager in DARPA's Microsystem Technologies Office. "Beyond the cost and size advantages, integrated optical approaches could allow tuning over multiple frequency bands and

environmental robustness. There is potential for very broad impact if our teams are successful."

The first technical area the GRYPHON program will pursue is to develop low noise, compact, and frequency-agile prototypes that can provide outputs spanning 1-40 GHz.

The prototype target performance metrics are geared toward rapid adoption by military and commercial entities alike. Program success will also hinge on proving robustness to environmental effects and demonstrating a roadmap to high-volume, low-cost domestic manufacturing.

The research teams selected for this endeavor include: Honeywell, Nexus Photonics, BAE Systems, Caltech, and hQphotonics. Due to the highly interdisciplinary nature of the work, most performers have engaged additional partners to complement their core competencies.

GRYPHON's second technical area encourages performers to pursue advanced techniques that offer even lower phase noise or ultra-wide tunability to inform future oscillator architectures. Teams from Columbia University and University of Virginia have been selected to push the boundaries in materials and system integration to this end.

With a diversity of approaches, materials, and performer teams, the GRYPHON program promises to deliver high impact solutions in the near term and germinate future directions for exploration.

Statement before the Financial Stability Oversight Council on Money Market Funds, Open-End Bond Funds, and Hedge Funds

U.S. SECURITIES AND EXCHANGE COMMISSION

Thank you, Secretary Yellen, for focusing the Council's attention on financial resiliency with regard to three key parts of our capital markets — particularly money market funds, open-end bond funds, and hedge funds.

The fund industry gives retail and institutional investors the opportunity to pool their assets, get investment advice, and attain diversification and efficiency.

These pools of assets have become a significant part of our markets. There's $5 trillion in money market funds, nearly $7 trillion in open-end bond funds, and $9 trillion in gross assets under management in hedge funds.

The nature, scale, and interconnectedness of these fund sectors, though, also pose issues for financial stability. This is not just based on financial economic theory, but also upon the practical lessons of the past.

We've seen such risks emanate from these sectors during the 2008 financial crisis, at the start of the COVID crisis in March 2020, and in 1998, when the hedge fund Long-Term Capital Management failed.

Money market funds and open-end bond funds, by their design, have a potential liquidity mismatch — between investors' ability to redeem daily on the one hand, and funds' securities that may have lower liquidity.

While this might not be as significant a concern in normal markets, we've seen that in stress times, these funds' liquidity mismatches can raise systemic issues. Hedge funds can present financial resiliency risks through leverage or derivatives positions.

I think the Securities and Exchange Commission has a responsibility to help protect for financial stability, which maps onto many parts of our statutes, but particularly onto the "orderly" part of our mission. Thus, I've asked SEC staff to make recommendations for the Commission's consideration with regard to bolstering the resiliency of each of these fund sectors.

The Commission recently voted to propose amendments to rules that govern money market funds. I'd like to thank William Birdthistle and Sarah ten Siethoff for their work and today's presentation on the SEC's proposal.

With respect to open-end bond funds, I've asked staff whether there are improvements we can consider regarding the fund liquidity rule or through other reforms to enhance fund liquidity, pricing, and resiliency in possible future stress events.

With respect to hedge funds, in January, the Commission voted to propose amendments to Form PF — a form first adopted after the financial crisis that provides certain private fund information to the SEC and other financial regulators.

Among other things, the proposed amendments would require certain advisers to hedge funds to provide current reporting of events that could be relevant to financial stability.

Looking ahead, I've asked staff to work jointly with staff at the Commodity Futures Trading Commission to consider whether they would recommend amending the joint portions of Form PF related to the periodic reports of hedge funds.

Further, in November, the Commission proposed a rule to require public reporting of large security-based swap positions. Total return swaps, a type of security-based swaps, contributed to the transmission of risk during the failure of Archegos Capital Management last year. We also re-proposed a new rule to prevent fraud, manipulation, and deception in connection with security-based swap transactions.

I support the FSOC Statement on Nonbank Financial Intermediation today and welcome FSOC members' input on the SEC's ongoing consideration on how to best enhance resiliency in these critical fund sectors.

Thank you.

Survey highlights cyber security risks of remote working

National Cyber Security Centre

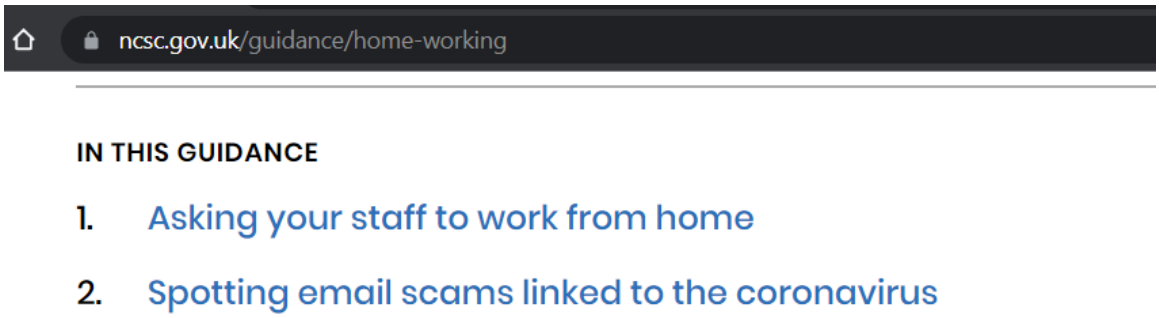
Maintaining an element of remote working beyond the pandemic is a prospect for many UK organisations. It's important, therefore, that we remain conscious of the potential cyber security risks attached to working from home.

A new survey by software provider Dilligent revealed this week that UK businesses lost £374 million in 2021 due to cyberbreaches largely linked to staff working from home. You may visit: https://www.diligent.com/news/diligent-finds-cyberbreaches-due-to-work-from-home-have-cost-surveyed-uk-businesses-374-million-in-the-last-18-months

450 senior finance and risk professionals at UK listed companies responded to the survey.

64% of respondents said their company had experienced a cyberattack or data breach in the last 18 months. Out of those who reported an attack or breach, 82% said tech issues or behaviour linked to remote working was the cause and 75% said they had lost money as a result.

The NCSC's home working guidance urges organisations to make security considerations unique to remote working environment around the use of business tools, including VPNs and SaaS applications, as well as security threats like phishing. You may visit: https://www.ncsc.gov.uk/guidance/home-working



Preparing your staff for home working

Working from home can be daunting for people who haven't done it before, especially if it's a sudden decision. There are also practical considerations; staff who are used to sharing an office space will now be remote. Think about whether you need **new** services, or to just **extend** existing ones, so that teams can continue to collaborate. For, example you may want to consider services that provide chat rooms, video teleconferencing (VTC) and document sharing.

The NCSC guidance on implementing Software as a Service (SaaS) applications can help you choose and roll out a range of popular services. If you are already providing such services, you'll need to plan for a potentially large increase in users, and any new services you provide will also need to be supported.

Here are some general recommendations to support secure home working.

- Remote users may need to use different software (or use familiar applications in a different way) compared to what they do when in the office. You should produce written guides for these features, and test that the software works as described.
- Depending on the experience of your staff (and the applications you provide), you should consider producing a series of 'How do I?' guides so that your already stretched support team isn't overwhelmed with requests for help. For example, you might produce a 'How to log into and use an online collaboration tool' guide.
- Remember, many of your staff are already stressed, so they're not in an ideal position to learn new technologies. In addition, they might not be able to ask an office workmate for help, as they normally might. You should check how staff are coping; not just in terms of how to use new technologies, but also how they are adapting to having to work in very different ways.
- Staff are more likely to have their devices stolen (or lose them) when they are away from the office or home. Make sure devices encrypt data whilst at rest, which will protect data on the device if it is lost or stolen. Most modern devices have encryption built in, but encryption may still need to be turned on and configured.

The NCSC has produced a 'Top Tips for Staff' e-learning training package for organisations to share cyber security best practices with their staff. Organisations can test their defences against a cyber attack linked to remote working by using the NCSC's free Exercise in a Box toolkit. You may visit: https://www.ncsc.gov.uk/blog-post/ncsc-cyber-security-training-for-staff-now-available

The NCSC's e-learning package 'Top Tips For Staff' can be completed online, or built into your own training platform.

To learn more: https://www.ncsc.gov.uk/report/weekly-threat-report-4th-february-2022

Helping users stay safe: Blocking internet macros by default in Office

Kellie Eickmeyer

Microsoft

It's a challenging time in software security; migration to the modern cloud, the largest number of remote workers ever, and a global pandemic impacting staffing and supply chains all contribute to changes in organizations. Unfortunately, these changes also give bad actors opportunities to exploit organizations:

> *"Cybercriminals are targeting and attacking all sectors of critical infrastructure, including healthcare and public health, information technology (IT), financial services, and energy sectors. Ransomware attacks are increasingly successful, crippling governments and businesses, and the profits from these attacks are soaring."*
>
> - Microsoft Digital Defense Report, Oct 2021

For years Microsoft Office has shipped powerful automation capabilities called active content, the most common kind are macros. While we provided a notification bar to warn users about these macros, users could still decide to enable the macros by clicking a button. Bad actors send macros in Office files to end users who unknowingly enable them, malicious payloads are delivered, and the impact can be severe including malware, compromised identity, data loss, and remote access. See more in this blog post:

> *"A wide range of threat actors continue to target our customers by sending documents and luring them into enabling malicious macro code. Usually, the malicious code is part of a document that originates from the internet (email attachment, link, internet download, etc.). Once enabled, the malicious code gains access to the identity, documents, and network of the person who enabled it."*
>
> - Tom Gallagher, Partner Group Engineering Manager, Office Security

For the protection of our customers, we need to make it more difficult to enable macros in files obtained from the internet.

Changing Default Behavior

We're introducing a default change for five Office apps that run macros:

VBA macros obtained from the internet will now be blocked by default.

For macros in files obtained from the internet, users will no longer be able to enable content with a click of a button. A message bar will appear for users notifying them with a button to learn more. The default is more

secure and is expected to keep more users safe including home users and information workers in managed organizations.

This change only affects Office on devices running Windows and only affects the following applications: Access, Excel, PowerPoint, Visio, and Word. The change will begin rolling out in Version 2203, starting with Current Channel (Preview) in early April 2022. Later, the change will be available in the other update channels, such as Current Channel, Monthly Enterprise Channel, and Semi-Annual Enterprise Channel.

At a future date to be determined, we also plan to make this change to Office LTSC, Office 2021, Office 2019, Office 2016, and Office 2013.

To read more: https://techcommunity.microsoft.com/t5/microsoft-365-blog/helping-users-stay-safe-blocking-internet-macros-by-default-in/ba-p/3071805

2021 Trends Show Increased Globalized Threat of Ransomware

In 2021, cybersecurity authorities in the United States, Australia, and the United Kingdom observed an increase in sophisticated, high-impact ransomware incidents against critical infrastructure organizations globally.

The Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), and the National Security Agency (NSA) observed incidents involving ransomware against 14 of the 16 U.S. critical infrastructure sectors, including the Defense Industrial Base, Emergency Services, Food and Agriculture, Government Facilities, and Information Technology Sectors.

The Australian Cyber Security Centre (ACSC) observed continued ransomware targeting of Australian critical infrastructure entities, including in the Healthcare and Medical, Financial Services and Markets, Higher Education and Research, and Energy Sectors.

The United Kingdom's National Cyber Security Centre (NCSC-UK) recognizes ransomware as the biggest cyber threat facing the United Kingdom.

Education is one of the top UK sectors targeted by ransomware actors, but the NCSC-UK has also seen attacks targeting businesses, charities, the legal profession, and public services in the Local Government and Health Sectors.

Ransomware tactics and techniques continued to evolve in 2021, which demonstrates ransomware threat actors' growing technological sophistication and an increased ransomware threat to organizations globally.

This joint Cybersecurity Advisory—authored by cybersecurity authorities in the United States, Australia, and the United Kingdom—provides observed behaviors and trends as well as mitigation recommendations to help network defenders reduce their risk of compromise by ransomware.

TECHNICAL DETAILS

Cybersecurity authorities in the United States, Australia, and the United Kingdom observed the following behaviors and trends among cyber criminals in 2021:

• *Gaining access to networks via phishing, stolen Remote Desktop Protocols (RDP) credentials or brute force, and exploiting vulnerabilities.* Phishing emails, RDP exploitation, and exploitation of software vulnerabilities remained the top three initial infection vectors for ransomware incidents in 2021. Once a ransomware threat actor has gained code execution on a device or network access, they can deploy ransomware.

Note: these infection vectors likely remain popular because of the increased use of remote work and schooling starting in 2020 and continuing through 2021. This increase expanded the remote attack surface and left network defenders struggling to keep pace with routine software patching.

• *Using cybercriminal services-for-hire*. The market for ransomware became increasingly "professional" in 2021, and the criminal business model of ransomware is now well established.

In addition to their increased use of ransomware-as-a-service (RaaS), ransomware threat actors employed independent services to negotiate payments, assist victims with making payments, and arbitrate payment disputes between themselves and other cyber criminals.

NCSC-UK observed that some ransomware threat actors offered their victims the services of a 24/7 help center to expedite ransom payment and restoration of encrypted systems or data.

Note: cybersecurity authorities in the United States, Australia, and the United Kingdom assess that if the ransomware criminal business model continues to yield financial returns for ransomware actors, ransomware incidents will become more frequent. Every time a ransom is paid, it confirms the viability and financial attractiveness of the ransomware criminal business model.

Additionally, cybersecurity authorities in the United States, Australia, and the United Kingdom note that the criminal business model often complicates attribution because there are complex networks of developers, affiliates, and freelancers; it is often difficult to identify conclusively the actors behind a ransomware incident.

• *Sharing victim information.* Eurasian ransomware groups have shared victim information with each other, diversifying the threat to targeted organizations.
For example, after announcing its shutdown, the BlackMatter ransomware group transferred its existing victims to infrastructure owned by another group, known as Lockbit 2.0. In October 2021, Conti ransomware actors began selling access to victims' networks, enabling follow-on attacks by other cyber threat actors.

To read more:
https://www.ncsc.gov.uk/files/2021%20Trends%20show%20increased%20global ised%20threat%20of%20ransomware.pdf

NIST Updates FIPS 201 Personal Identity Credential Standard

The standard now goes beyond physical ID cards to include electronic tokens and one-time passwords.

To ensure that federal employees have a broader set of modern options for accessing facilities and electronic resources, the National Institute of Standards and Technology (NIST) has increased the number of acceptable types of credentials that federal agencies can permit as official digital identity.

The increase is part of the latest update to Federal Information Processing Standard (FIPS) 201, which specifies the credentials that can be used by federal employees and contractors to access federal sites.

The update, formally titled FIPS 201-3: Personal Identity Verification (PIV) of Federal Employees and Contractors, also allows for remote identity proofing and issuing, in addition to doing so in-person as was previously required.

“We have expanded the set of credentials that can be used for gaining access to federal facilities and also for logging onto workstations and other IT resources,” said Hildegard Ferraiolo, a NIST computer scientist. “It’s not all about PIV cards anymore.”

The preceding FIPS standard, version 201-2, came out in 2013 and specified credentials embedded on PIV cards as the primary means for authentication, with limited exceptions for credentials designed for mobile devices that lacked PIV card readers. Millions of PIV cards have been issued to federal employees.

The 201-3 update, the result of a regular review cycle, still specifies that PIV cards can be used but now offers additional options.

It keeps the standard aligned with the most recent federal policies, including the Office of Management and Budget’s Memorandum M-19-17 on identity, credential and access management.

It also ensures that the standard reflects current technological capabilities and needs, Ferraiolo said.

“It has become important to provide more flexibility to agencies in choosing credentials to use for authentication,” she said. “Not all laptop computers are available with built-in PIV card slots, for example, and often, there are cloud-based applications that don’t use public-key

infrastructure that PIV cards provide. For these situations we need alternatives."

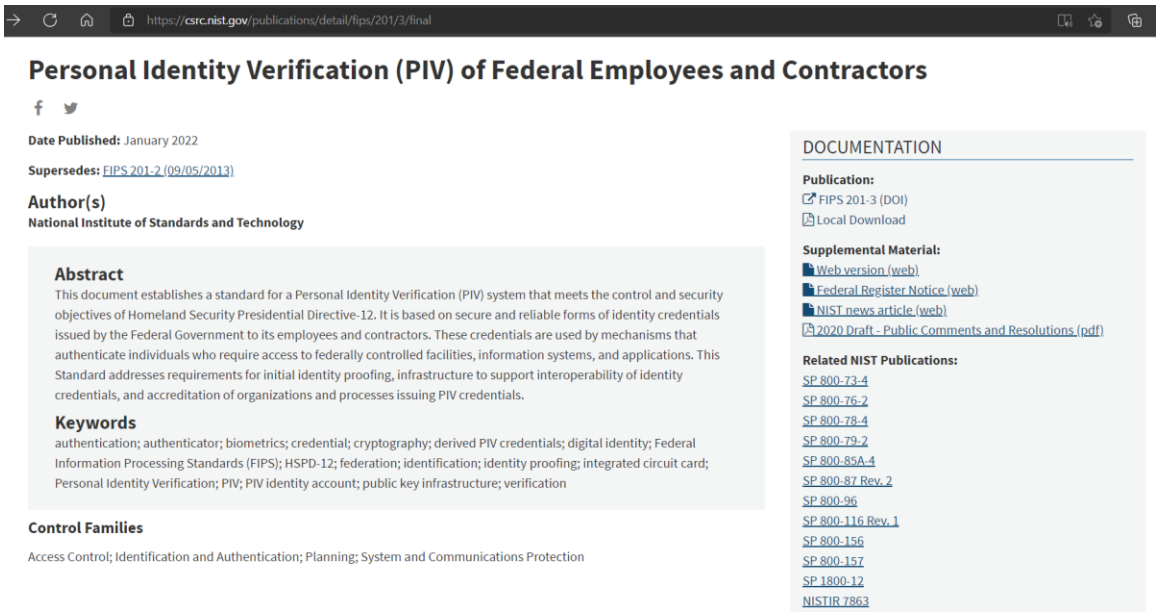
The new options are a subset of credentials that are specified in NIST SP 800-63-3, a multivolume publication on digital identity. Branches of the government will have a richer set of multifactor credentials for different devices — including, for example, FIDO (Fast ID Online) tokens and one-time passwords (OTP).

With the revision milestone now complete, the focus for NIST has shifted to providing additional guidelines and implementation details, Ferraiolo said. NIST is currently in the process of updating guidelines for the expanded set of PIV credentials in Revision 1 of NIST SP 800-157.

Additionally, to ensure that different credentials are interoperable across different agencies, a concept known as "federation," NIST will provide guidelines in NIST SP 800-217.

Ferraiolo said these and other NIST publications associated with FIPS 201-3 would be updated in coming months.

For more information, see the complete FIPS update, which is available online at: https://csrc.nist.gov/publications/detail/fips/201/3/final



FIPS PUB 201-3

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION
(Supersedes FIPS 201-2)

Personal Identity Verification (PIV) of Federal Employees and Contractors

CATEGORY: INFORMATION SECURITY **SUBCATEGORY: IDENTITY**

Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

This publication is available free of charge from:
https://doi.org/10.6028/NIST.FIPS.201-3

Issued January 2022

Statement on Pay versus Performance

Chair Gary Gensler, U.S. Securities and Exchange Commission

The Commission is reopening the comment period for a proposed rule for corporate disclosure of "pay versus performance." I support this proposed rule because, if adopted, it would strengthen the transparency and quality of executive compensation disclosure.

The rule proposal would fulfill a mandate from Congress under the Dodd-Frank Act of 2010, passed after the 2008 financial crisis.

"Pay versus performance" disclosures describe the relationship between the executive compensation an issuer actually paid and the financial performance of that issuer. Such disclosures would make it easier for shareholders to assess the company's decision-making with respect to its executive compensation policies.

The Commission has long recognized the value of information on executive compensation to investors. The first requirements to make disclosures about executive compensation originated in the 1933 Act. Since then, from time to time the Commission has continued to update compensation disclosure requirements.

In 2015, the Commission proposed rules to implement the Dodd-Frank Act's "pay versus performance" requirement. These proposed rules relied upon total shareholder return as the sole measure of financial performance. Some commenters expressed concerns that total shareholder return would provide an incomplete picture of performance.

In this reopening release, we are considering whether additional performance metrics would better reflect Congress's intention in the Dodd-Frank Act and would provide shareholders with information they need to evaluate a company's executive compensation policies.

I'm pleased to support today's reopening release and look forward to the public's feedback. I'd like to extend my gratitude to the members of the SEC staff who worked on this item, including:

- Renee Jones, Erik Gerding, Connor Raso, Lindsay McCord, Jennifer Zepralka, Anne Krauskopf, Angie Kim, and Jeb Byrne in the Division of Corporation Finance;

- Bryant Morris, Dorothy McCuaig, and Ken Alcé in the Office of the General Counsel;

- Jessica Wachter, Vlad Ivanov, Tara Bhandari, Mike Willis, Julie Marlowe, PJ Hamidi, Robert Miller, and Lauren Moore in the Division of Economic and Risk Analysis;

- Brian Johnson, Amanda Wagner, and Amy Miller in the Division of Investment Management; and

- Kristin Pauley, Marc Johnson, and Laura Metcalfe in the Division of Enforcement;

- Jonathan Wiggins, Omid Harraf, Larry Yusuf, and Mark Jacoby in the Office of Chief Accountant.

On returning inflation back to target

Catherine L. Mann, External Member of the Monetary Policy Committee, Bank of England

Introduction and summary

As an international economist, I have always studied domestic economic conditions through the lens of global influences.

This year the UK offers an excellent laboratory. Global factors have been at the forefront of the inflation surge in the UK, and their effects will persist into early 2022. However, expectations for wages and prices for this year, if realized, could keep UK inflation strong for longer, which might then generate a reinforcing cost-price dynamic.

To return inflation to target, the Monetary Policy Committee's first line of defence is to dampen expectations of future price increases. Achieving an inflection in these expectations along with tailwinds from global factors could mean that a shallower path of future rate rises is needed to bring inflation back to target.

In the last half of 2021, UK CPI inflation surged, more than doubling from 2% in July to 5.4% in December.

Previously, average earnings had rebounded strongly from their trough in 2020 leading to headline wage inflation rates as high as 9% in the summer.

While some of these increases are due to base and compositional effects, demand and supply imbalances both in goods and labour markets built very quickly over the second half of the year.

Residual strength in both wages and prices likely will continue for a time into 2022 as the domestic and global mismatch of supply and demand slowly resolve, as firms try to recover margins eroded in 2021, and as labour markets stay tight.

Indeed, firms in the latest DMP panel (from December) expect to raise their prices by 5% in 2022 – a bit more than the 4% in 2021. Meanwhile, firms expect continued upward pressure on pay growth in 2022 on the top of the 2-3.5% increases of 2021.

These expectations for prices and wages, if realized, are ingredients for headline inflationary pressures that could stay strong for longer, well into 2023. The question for monetary policy then becomes whether the real factors on the one hand and expectations on the other could together create a reinforcing cost-price dynamic.

Certainly, there are headwinds facing these price and wage expectations. Most importantly, will domestic and global demand in 2022 be strong enough for firms to pass through wage and cost increases into their prices? In the end, it is the collective outturns of business pricing that translates into inflation.

Monetary policy has a role to play in managing expectations as well as ensuring that the economic and financial conditions facing firms and workers are consistent with the 2% target.

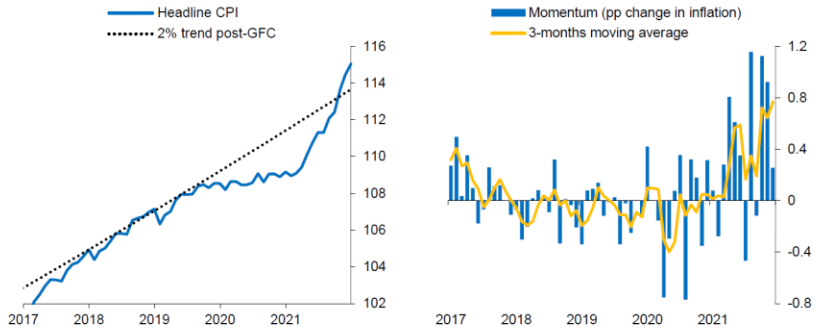
Initial conditions and the 2021 surge

Before we can assess the prospects for returning inflation to the 2% target, we need to recall initial conditions and review sources of the 2021 inflation surge.

Going into the pandemic, the UK CPI price level was roughly trending along its 2% inflation path, unlike in the US or the euro area which had seen persistently lower inflation than intended.

In the first year of the pandemic with lockdowns disrupting a wide range of activities, some firms did cut prices in the UK (and some markets simply did not exist, so there were no prices at all) and the aggregate price level flat-lined.

Chart 1: CPI level (index, LHS) and momentum (percentage points, RHS)

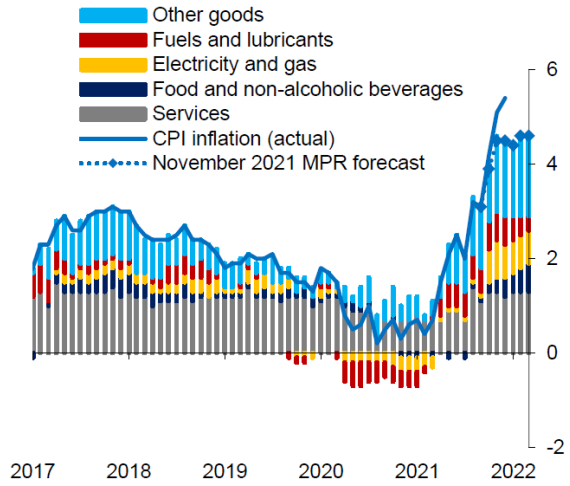


Sources: ONS and Bank calculations. Notes: Trend on LHS shows the level of prices if CPI had grown at 2% annualised rates in every month since December 2010. RHS shows momentum of CPI, i.e. the month-to-month percentage point change of year-on-year inflation. Thus, positive momentum means rising inflation (accelerating prices) and negative momentum falling inflation (decelerating prices). Latest observation: December 2021.

Both demand recovery and supply limitations in 2021 have now yielded robust inflation momentum, which if price expectations are realized, is poised to continue into 2022 moving the price level further away from the 2% trend. (Chart 1).

Reviewing key sources of the 2021 inflation surge – energy and core goods – both are importantly driven by sources external to the UK economy. (Chart 2).

Chart 2: Decomposition of CPI inflation in the November 2021 MPR forecast (% year-on-year)



Source: November 2021 Monetary Policy Report. Latest observation: December 2021 (actual), March 2022 (forecast).

Global goods prices have been elevated by the rotation away from consumer-facing services towards goods purchases.

The dominant driver of global goods price dynamics is the interplay of three successive US fiscal stimuli combined with geographical mismatches of containers and production stoppages in key economies and for key materials. But, a domestic equivalent to the global supply-demand imbalance has also been apparent in the UK, with production constraints and shortages of HGV drivers.

To read more:
https://www.bankofengland.co.uk/speech/2022/january/catherine-l-mann-speech-on-the-economy-and-monetary-policy-at-omfif

Romance Scams

Romance scams occur when a criminal adopts a fake online identity to gain a victim's affection and trust. The scammer then uses the illusion of a romantic or close relationship to manipulate and/or steal from the victim.

The criminals who carry out romance scams are experts at what they do and will seem genuine, caring, and believable. Con artists are present on most dating and social media sites.

The scammer's intention is to establish a relationship as quickly as possible, endear himself to the victim, and gain trust. Scammers may propose marriage and make plans to meet in person, but that will never happen. Eventually, they will ask for money.

Scam artists often say they are in the building and construction industry and are engaged in projects outside the U.S. That makes it easier to avoid meeting in person—and more plausible when they ask for money for a medical emergency or unexpected legal fee.

If someone you meet online needs your bank account information to deposit money, they are most likely using your account to carry out other theft and fraud schemes.

Tips for Avoiding Romance Scams:

- Be careful what you post and make public online. Scammers can use details shared on social media and dating sites to better understand and target you.

- Research the person's photo and profile using online searches to see if the image, name, or details have been used elsewhere.

- Go slowly and ask lots of questions.

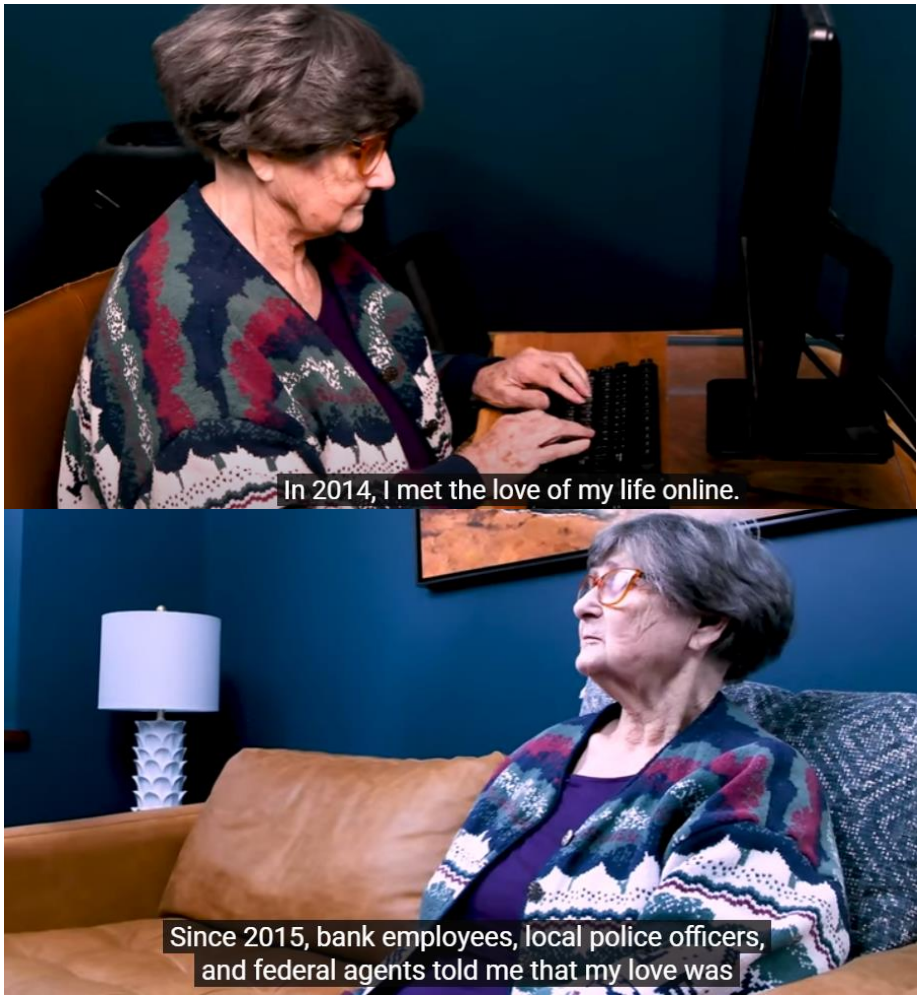
- Beware if the individual seems too perfect or quickly asks you to leave a dating service or social media site to communicate directly.

- Beware if the individual attempts to isolate you from friends and family or requests inappropriate photos or financial information that could later be used to extort you.

- Beware if the individual promises to meet in person but then always comes up with an excuse why he or she can't. If you haven't met the person after a few months, for whatever reason, you have good reason to be suspicious.

- Never send money to anyone you have only communicated with online or by phone.

To learn more: https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/romance-scams



https://www.youtube.com/watch?v=vthPmLORVrM

https://youtu.be/108UWM1jsF8
https://youtu.be/BmIvqOYwGGU

https://www.ic3.gov/Media/Y2019/PSA190805

Cyber Actors Use Online Dating Sites To Conduct Confidence/Romance Fraud And Recruit Money Mules

WHAT IS CONFIDENCE/ROMANCE FRAUD?

Confidence/romance fraud occurs when an actor deceives a victim into believing they have a trust relationship—whether family, friendly, or romantic—and leverages the relationship to persuade the victim to send money, provide personal and financial information, or purchase items of value for the actor. In some cases, the victim is persuaded to launder money on behalf of the actor.

Actors often use online dating sites to pose as U.S. citizens located in a foreign country, U.S. military members deployed overseas, or U.S. business owners seeking assistance with lucrative investments.

Third annual threat assessment

Mike Burgess, Director-General of Security, in charge of the Australian Security Intelligence Organisation (ASIO).

Australian Government
Australian Security Intelligence Organisation

Good evening. Welcome to ASIO and to my Annual Threat Assessment.

I'd like to recognise our partners and colleagues represented here tonight – Excellencies, MP's and Senators, the Inspector-General, Directors-General, Secretaries, Military Chiefs, Commissioners, ladies and gentlemen.

Can I start with an admission? While I am pleased to host this event and welcome you to the Ben Chifley Building, a lectern is not my happy place. I loathe public speaking.

So you might be thinking, why would someone like me choose to do something like this?

There are three key reasons, and I'd like to explain them.

The first is trust.

ASIO protects Australia and Australians from threats to their security. Our ability to deliver our mission requires us to maintain the confidence and trust of our stakeholders, including the Australian people.

A vibrant liberal democracy requires a Security Service that is transparent and trusted.

I believe this imposes a responsibility on ASIO to be as open as possible about what the Organisation does, and why we do it.

Giving this address, and inviting you into our building, is a tangible expression of how seriously I take that responsibility.

It's why I was one of the first intelligence leaders anywhere in the world to have a personal, identifiable Twitter account; why I give speeches and do occasional media interviews; why ASIO is on social media; and why I've

declassified operations and case studies to give a clearer picture of the threats we face.

None of that was easy. Some of it was controversial. But all of it was important.

Transparency matters. Transparency is a precursor for trust.

My thinking on transparency crystallised at a time in my career when the Defence Signals Directorate was accused of an illegal act.

The allegations were proved to be completely unfounded, but damage was done, reputations were stained, and confidence was bruised.

The affair taught me how difficult it can be for a secret organisation to defend itself, even when it's done nothing wrong—it's assumed that if you're in the shadows, you're shadowy.

We can dispel this with sunlight—by explaining who we are, what we do, and why we matter.

Not long after that incident, a journalist put a salacious and inaccurate claim to a certain intelligence agency—I won't say which one, or even in which country. Instead of saying, 'that's ridiculous'—or 'hell no', which would have been my response—the brains trust replied with, 'no comment—and that's off the record'.

The story got published and the next morning there was much head-shaking and tut-tutting as spy chiefs wondered how the newspaper could get it so wrong. The journalist got it so wrong because the agency ignored an opportunity to make it right!

Obviously there are things a spy agency cannot talk about—especially one where human sources and technical capabilities are critical to its success.

We need to be able to do things our adversaries think are impossible. But as I rose through the ranks, it became increasingly clear that there is much more we can say than 'no comment'.

We don't talk about our operations but we can reveal their outcomes.

We must be secretive about our capabilities, but we can be open about our values.

We cannot identify our undeclared staff, but we can celebrate the difference they make.

That brings me to the second principle of my transparency push— ASIO's people. Transparency is a powerful recruitment tool. People won't work for an agency if they don't know what it does and what it values; they can't apply for jobs they don't know exist.

I want more people to choose ASIO, and I want ASIO to be able to choose more people from more diverse backgrounds. This is a challenge intelligence agencies around the world are grappling with.

We need to do better. We should reflect the community we protect.

It's never too early to start planning a career at ASIO.

I recently received a letter from seven-year-old Ava, who wants to be a surveillance officer. She told me she's good at spying because she is small and nobody notices her.

Ava volunteered her mum to drive her around on her surveillance shifts. Clearly, young Ava already possesses some of the skills we're looking for—she's creative, shows initiative, and can communicate. But hide-and-seek isn't just for kids, and surveillance isn't just hide and seek. We are actually hiring surveillance officers right now.

While surveillance is a traditional spy role, we have many other roles too. Many of the jobs we are advertising, or are about to advertise, are not usually associated with spy agencies, but are integral to our success:

- Trades professionals such as electricians and plumbers.

- Technology graduates who can design, build and deliver systems, access data and help our analysts make sense of data.

- Business analysts and project managers to drive our capability uplift.

- Intelligence officers and analysts to collect the dots and connect the dots.

- And legal graduates to ensure our covert operations are conducted lawfully, and to work on litigation and corporate matters.

There is no ASIO type. ASIO needs people from all walks of life and I invite you to find your fit.

So that's what an annual threat assessment delivers for ASIO.

The final—and perhaps most important—factor is what's in it for you, ASIO's partners and stakeholders. It's critically important to explain the

threats we are seeing so you are armed with the awareness and advice you need to counter those threats.

Security is a shared responsibility. ASIO cannot stop every terrorist and catch every spy. The scale, persistence and sophistication of the threats Australia is facing demands a broader approach to security. I'll return to this later.

Australia's security outlook remains complex, challenging and changing. COVID-19 and its associated lockdowns added considerable volatility to the mix.

While, thankfully, the time of lockdowns seems to have come to an end, the impacts of the lockdowns are continuing to influence the security environment.

We all spent a lot more time online during the pandemic. This was positive in many respects. During difficult times, the internet helped us maintain connections with families and friends, allowed many of you to work from home, and, of course, enabled plenty of online shopping!

But like many things online, for every benefit the internet delivered, a related downside was created.

More online shopping meant more cyber-crime. More online engagement provided greater opportunities for radicalisation. More working from home increased the risk of cyber-enabled espionage.

I'd like to dive into the last two a little more deeply because they fall squarely within ASIO's remit, and are exerting a significant influence on Australia's security environment.

In the last two years, thousands of Australians with access to sensitive information have been targeted by foreign spies using social media profiles. These spies are adept at using the internet for their recruitment efforts.

On any of the popular social media or internet platforms, they make seemingly innocuous approaches—such as job offers. This then progresses to direct messaging on different, encrypted platforms, or in-person meetings, before a recruitment pitch is made.

I've previously highlighted our concerns about approaches on professional networking sites, but during the pandemic we've seen this threat spread. There's been a jump in suspicious approaches on messaging platforms like WhatsApp, for example.

It's an easy way for foreign intelligence services to target employees of interest.

ASIO is also tracking suspicious approaches on dating platforms such as Tinder, Bumble and Hinge. My message for any potential victims on these sites is a familiar one—if it seems too good to be true, it probably is!

While espionage is one of the most insidious security threats we are dealing with online, it is not the most concerning trend.

The internet is the world's single most potent and powerful incubator of extremism.

Online radicalisation is nothing new, but COVID-19 sent it into overdrive. Isolated individuals spent more time online, exposed to extremist messaging, misinformation and conspiracy theories.

Social media platforms, chat rooms, and algorithms are designed to join up people who share the same views, and push them material they will 'like'. It's like being in an echo chamber where the echo gets louder and louder, generating cycles of exposure and reinforcement.

More time in those online environments—without some of the circuit breakers of everyday life, like family and community engagement, school and work—created more extremists. And in some cases, it accelerated extremists' progression on the radicalisation pathway towards violence.

Back in 2007, ASIO produced an assessment warning about the implications of a pandemic. We did that not because we're health experts, but because it's our job to identify and analyse phenomena that might have security impacts for our country. We assessed that a pandemic would result in an increase in anti-government behaviours, and we have certainly seen that with COVID.

While ASIO's overall terrorism caseload has decreased since this time last year, there's been a distinct increase in radicalisation and specific-issue grievances.

Some Australians believe the government's approach to vaccinations and lockdowns infringed their freedoms. And in a small number of cases, grievance turned to violence.

Obvious examples are the violent incidents at COVID-related protests fuelled by anti-vaccination, anti-lockdown and anti-government agendas.

We have also seen threats against public office holders, an attack on a vaccination clinic, and several physical assaults on healthcare workers.

We assess that these tensions and the associated possibility of violence will persist.

While lockdowns and mandatory quarantine requirements are being eased, the introduction of vaccination requirements for some forms of employment, social engagement and travel will continue to drive anger, uncertainty and fear within a small section of society.

This cohort views the restrictions as an attack on their rights, the creation of a two-tier society and confirmation of their perceived persecution.

ASIO does not have any issue with people who have opinions they want to express. This is a critical part of a vibrant democracy. We do not—and cannot—investigate peaceful protest or dissent. Our concern is where opinions tip into the promotion of violence, or actual acts of violence.

So I should stress that the vast majority of people who choose not to be vaccinated will not engage in violence in response to vaccine mandates. The vast majority of protestors are not violent extremists, and the vast majority of the protests are not violent. ASIO's focus is on a small number of angry and alienated Australians.

This is precisely the concern I identified in this speech last year, and precisely why we changed the language we use to describe violent extremism. As I warned back then:

We are seeing a growing number of individuals and groups that don't fit on the left–right spectrum at all; instead, they're motivated by a fear of societal collapse or a specific social or economic grievance or conspiracy.

The behaviours we are seeing in response to COVID lockdowns and vaccinations are not specifically left or right wing. They are a cocktail of views, fears, frustrations and conspiracies. Individuals who hold these views, and are willing to support violence to further them, are best and most accurately described as ideologically motivated violent extremists.

Some of the alleged violent acts at the recent Old Parliament House protest are a case in point. The individuals involved were driven by a diverse range of grievances, including anti-vaccination agendas, conspiracy theories and anti-government sovereign citizen beliefs.

Assigning the protesters to a specific point on the political spectrum is neither accurate nor helpful.

Of course, this does not mean that people who hold, say, racist and nationalist beliefs never participate in these activities—sometimes they do—but they are just one relatively small part of a much wider and looser group.

This is an important point to make, because we expect to see more of this behaviour in Australia in the medium term. Protests driven by diverse specific-issue grievances will be part of our security environment for the foreseeable future. In some cases, protesters will advocate the use of violence, and in a smaller number of cases, they may use violence.

In this uptick in specific-issue or grievance-motivated violent extremism, many of the actors are newcomers, so it's harder to get a sense of what is simply big talk—and what is genuine planning for violence.

Making the call about which statements indicate a genuine plan for violence, and which are purely sounding off or wishful thinking, is one of the greatest challenges our analysts have. Our information is often incomplete—and the stakes are high.

Every judgement our analysts make affects another: when they decide to continue one investigation they are, in effect, deciding not to continue or launch a different one. With finite resources, it is a zero-sum game.

The most likely terrorist attack scenario in Australia over the next 12 months continues to be a lone-actor attack—and that fact weighs heavily on my mind and the minds of our staff.

While there were no terrorist attacks domestically last year, there were two major disruptions of violent extremist attacks. Globally, violent extremist attacks remain a frequent occurrence. And the transnational nature of terrorism means that events in distant places, such as the fall of the government in Afghanistan, can reverberate much closer to home. We are monitoring this carefully.

While we do not assess it has increased the immediate threat in Australia, we remain concerned that, in the longer term, violent extremists from our region may travel to Afghanistan for militant training.

Two years ago, in my first threat assessment, I noted that ASIO was seeing an increase in the radicalisation of young Australians.

Unfortunately and alarmingly, this trend is continuing. The number of minors being radicalised is getting higher and the age of the minors being radicalised is getting lower.

Most of the radicalisation occurs online, reflecting the dynamic I raised earlier, but some of it also happens in person, face to face. Children as young as 13 are now embracing extremism, and this is happening with religiously motivated violent extremism and ideologically motivated violent extremism.

And unlike past experience, many of these young people do not come from families where a parent or sibling already holds extreme views.

As the Director-General of Security, this trend is deeply concerning. As a parent, it is deeply distressing. As a nation, we need to reflect on why some teenagers are hanging Nazi flags and portraits of the Christchurch killer on their bedroom walls, and why others are sharing beheading videos. And just as importantly, we must reflect on what we can do about it.

A few years ago, minors represented around two to three per cent of our new counter-terrorism investigations. In the last year, though, the figure's been closer to fifteen per cent. And perhaps more disturbingly, these young people are more intense in their extremism.

Where once minors tended to be on the fringe of extremist groups, we are now seeing teenagers in leadership positions, directing adults, and willing to take violent action themselves.

At the end of last year, on average, minors represented more than half of our priority counter-terrorism investigations each week.

This should concern us all. Again, minors made up 15 per cent of our new counter-terrorism investigations, and more than half of our highest priority investigations each week.

ASIO is aware of minors preying on other minors, seeking to turn them to their violent ideology and using grooming techniques similar to those used by paedophiles.

We have seen cases involving young, radicalised violent extremists systematically targeting vulnerable associates who were lonely or going through tough times.

The targeting took place online, and face to face in a variety of settings, even schools. The tactics used by the extremists in these cases involved a combination of attention, flattery and friendship, which shifted to bullying and manipulation. We've seen young ringleaders deliberately desensitise their targets, gradually exposing them to more extreme and more violent propaganda, until the most graphic material imaginable was normalised.

Believe me when I tell you that ASIO finds these kinds of cases challenging — we do not belong in the schoolyard — and while we act when there is a threat of violence, the broader trend of teenage radicalisation demands a different response, one where ASIO and law enforcement are not the answer.

It is very hard to deradicalise an adult extremist, but there are many more options to redirect young people who are experimenting with extremism in response to unhappiness or insecurity.

As a society, we have to recognise the signs and step in early. Radicalisation in young people can happen quickly—in days and weeks, not months and years—and kids are most vulnerable when they are under stress.

In these situations, ASIO's role is at the end—at the point where there is an active threat to security. But before this point there are nearly always off-ramps: opportunities to redirect behaviour.

Government plays a key role in helping to counter violent extremism. Our colleagues in policy agencies, law enforcement and community organisations are doing important work in this space.

But the community can play a pivotal part identifying signs a teenager isn't just going through adolescence, but is heading towards radicalisation. Without knowing about these indicators it is much harder for us to divert them from a dangerous path.

Schools and sports clubs—notice and ask questions if the young people you know are acting antisocially and out of character.

Parents and carers—notice and ask questions if your children are receiving or circulating inappropriate material online. Children often start with moderately objectionable material, which then becomes worse and worse—identifying it early can be critical.
Community leaders—notice and ask questions if young people you know are showing marked changes in their demeanour or views.

Security is a shared responsibility.

While threat to life will always be a priority for ASIO, our attention and resourcing is increasingly being directed towards threats to Australia's way of life.

The first and perhaps most significant thing to say is that espionage and foreign interference has supplanted terrorism as our principal security concern.

This is not to downplay the significance of terrorism.

In terms of scale and sophistication, though, espionage and foreign interference threats are outpacing terrorism threats, and therefore demanding more attention and more resources.

The threat is pervasive, multifaceted and, if left unchecked, could do serious damage to our sovereignty, values and national interest.

Multiple countries are seeking to conduct espionage against us—and not just those countries that might be considered our traditional adversaries. In some instances, espionage is conducted by countries we consider friends—friends with sharp elbows and voracious intelligence requirements.

For decades, foreign spies have been seeking information about Australia's strategic capabilities, economic and policy priorities, world-class research and development, and defence technologies.

Obviously the capabilities and decision-making around AUKUS fall squarely into that category. Foreign intelligence agencies will have already added them to their collection requirements—just as ASIO is already working to thwart them. That should surprise no one; it's one of the reasons I'm flagging a more proactive approach to our security advice and engagement.

Following my previous address, our disruption of a 'nest of spies' got a lot of attention. But dismantling spy networks is business as usual for ASIO. We did it again last year.

Over a series of months, we painstakingly mapped out a foreign intelligence service's onshore network of sources and contacts. And then we picked it apart.

Australians who were targeted by the foreign intelligence service included current and former high-ranking government officials, academics, members of think-tanks, business executives and members of a diaspora community.

When we interviewed members of the network, some of the contacts suspected they'd engaged with spies, but most had no idea—and were shocked when we knocked on their doors.

As a sting in the tail, after we removed the spies, we laid trip wires—just in case the foreign country ever tries to reactivate this network. And this was just one of a number of disruptions we undertook in the past year.

As well as espionage, we've also seen an increase in foreign interference. I want to take a moment to draw out how this is different from foreign influence.

The confusion about where legitimate influence stops and foreign interference begins is understandable. We see our targets engaging in both things, and foreign interference is clandestine, and therefore difficult to discern.

Publicly praising a foreign regime—even an odious one—is not interference.

Transparently lobbying on behalf of a foreign government is not interference.

Diplomacy is not interference. These things are routine acts of statecraft.

But any and all of these acts could become foreign interference if they involve the hidden hand of a foreign state and are contrary to Australia's interests. If the person publicly praising another country is doing so because they've received discreet instructions from an overseas government, it could constitute foreign interference if it's detrimental to Australia's interests or done to affect our political processes.

So what does foreign interference look like in practice? There are two manifestations I'd like to focus on.

One is the harassment of Australia's diaspora communities. This is something ASIO's been warning about for some time. Foreign governments will often monitor and intimidate members of diaspora communities who are critics of the foreign government or express views at odds with the regime's policies. It's unacceptable that people who live in your street—and mine—might be subjected to the strongarm—and long arm—of a foreign state.

Again, it's important to understand exactly what is, and is not, foreign interference in this context. Just as it is perfectly legal to criticise a foreign regime in this country, it is perfectly legal to stage a counter-protest. That is not necessarily foreign interference, it may just be nationalist zeal.

But if a foreign government is clandestinely directing the counter-protest, then my Organisation will be very interested.

Some of the foreign governments we've dealt with seem to think that this sort of community harassment is OK. They think wrong. It's not OK.

One of the most insidious things about foreign interference is that it uses our strengths against us. The perpetrators exploit our values, freedoms and trust, to undermine our values, freedoms and trust.

Foreign interference in our politics is a case in point. The governments—and I emphasise governments—involved in these activities take advantage of the open and accessible nature of our political system.

Attempts at political interference are not confined to one side of politics, and you'd be surprised by the range of countries involved.

It's also important to put it in context. While attempts to interfere in our democratic processes are common, successful interference is not.

Our democracy remains robust, our parliaments remain sovereign, our elections remain free and the overwhelming majority of our politicians remain thoroughly resistant to even the most sophisticated and subtle approaches.

It is critical we do not let fear of foreign interference undermine stakeholder engagement or stoke community division. Were this to happen, it would perversely have the same corrosive impact on our democracy as foreign interference itself.

This year—a federal election year—we need to be particularly on guard against foreign political interference.

I can confirm that ASIO recently detected and disrupted a foreign interference plot in the lead-up to an election in Australia. I'm not going to identify the jurisdiction because we are seeing attempts at foreign interference at all levels of government, in all states and territories.

But it is important to explain what political interference actually looks like.

This case involved a wealthy individual who maintained direct and deep connections with a foreign government and its intelligence agencies. This agent of interference has roots in Australia but did the bidding of offshore masters, knowingly and covertly seeking to advance the interests of the foreign power and, in the process, undermine Australia's sovereignty.

I'll call this person 'the puppeteer', although it's important to remember that while the puppeteer pulled the strings, the foreign government called the shots.

The puppeteer hired a person to enable foreign interference operations and used an offshore bank account to provide hundreds of thousands of dollars for operating expenses. Secretly shaping the jurisdiction's political scene to

benefit the foreign power was considered a key performance indicator. It was like a foreign interference start-up.

The employee hired by the puppeteer began identifying candidates likely to run in the election who either supported the interests of the foreign government or who were assessed as vulnerable to inducements and cultivation. The employee used existing relationships with politicians, staffers and journalists to select potential targets, without revealing the secret intent, the foreign connection or the puppeteer's involvement.

The puppeteer and the employee plotted ways of advancing the candidates' political prospects through generous support, placing favourable stories in foreign language news platforms and providing other forms of assistance.

They investigated hiring political consultants, advertising agencies and PR specialists to help individual campaigns. The aim was not just to get the candidates into positions of power, but also to generate a sense of appreciation, obligation and indebtedness that could subsequently be exploited.

The political candidates had no knowledge of the plot. Even if the plan had proceeded, they would not have known who was pulling the strings. The puppeteer used the employee as a cut-out. This deliberate deceit and secrecy about the foreign government connection is what took the case into the realm of foreign interference.

At this point, ASIO acted. Our intervention ensured the plan was not executed, and harm was avoided.

It's impossible to know exactly what would have happened without ASIO's disruption but I can offer an informed scenario. Some of the candidates get elected. The puppeteer's employee then recommends they hire certain other associates as political staffers. These people are also agents or proxies of the foreign government, and will try to influence the politician, shape decision-making and help identify other political figures who can be influenced and recruited.

Down the track, the new parliamentarians might be asked for information about the party's position on defence policy, human rights, foreign investment or trade.

This information will be sent to the foreign power without the knowledge of the parliamentarian. At some point, the politicians might be prevailed upon to vote a particular way on a contentious issue, or lobby colleagues to vote a certain way.

I know that this is how it plays out because we've seen it happen in situations where we uncovered the foreign interference at a later stage. These cases are much more serious.

This is why ASIO's role is crucial. We and our partners use a suite of measures to disrupt foreign interference plots. The tools include defensive briefings to potential victims; interviews of perpetrators and other targeted intelligence activities; visa cancellations if we are dealing with foreign nationals and, of course, law enforcement action.

The first and most effective defence against all forms of foreign interference is awareness. Know who you are dealing with and why. That's why I've given you a level of detail that we would normally not reveal in public.

I want to improve your understanding of what foreign interference is—and, just as importantly, what it is not. The case study I've described makes it clear that foreign interference in our political system is far removed from lobbying, diplomacy or other open and transparent attempts to influence decision-making.

And as I mentioned earlier, I do not want misunderstandings about foreign interference to undermine democratic processes, community engagement or our multicultural society, which I firmly believe is a national asset.

The perpetrators of foreign interference carefully hide their true motivations. But that does not mean politicians are powerless to protect themselves.

The instincts, values and transparency that guide other elements of political engagement are powerful shields against foreign interference. If a supporter wants to provide significant levels of assistance or install a certain staffer in your office, do your due diligence. If business operators want to donate significant resources to your campaign, ask what's in it for them. If a media proprietor promises unlimited positive coverage, query their motives.

To be clear, I'm not suggesting people should reflexively turn down these types of assistance; just that they should be aware of the risks, pose the appropriate questions, and be transparent and accountable about what's received. And, most critically, stay alert to the backers calling in their favours by asking for something that conflicts with Australia's interests.

Security is a shared responsibility.

That's the message I want to leave you with tonight.

I want to assure you of two things: good security is achievable, and good security works.

I find it infuriating when companies say they were done over by an adversary so powerful there was no way to defend against it. That's what I call the Borg defence—'resistance is futile'.

In my experience, resistance is rarely futile.

Certainly, in the cyber field, the overwhelming majority of compromises are foreseeable and avoidable.

While some of these are seriously damaging, many others that are breathlessly called 'cyber-attacks' in the media are not compromises at all—they are reconnaissance missions; if the digital doors are locked, the intruder moves on and tries somewhere else.

At the same time, I'm the first to admit ASIO is not all-seeing or all-knowing—we don't want to be—and while ASIO is part of the answer to the challenges I've outlined, we are not the whole answer.

The acceleration of radicalisation, online propaganda and misinformation, single-issue extremism and minors embracing violent extremism all require a whole-of-government, whole-of-system and whole-of-nation approach.

That's why teamwork is critical.

Our work with law enforcement, the national intelligence community, Home Affairs and our international counterparts is well known—all of you are represented in the room tonight and I want to thank and commend you for being such effective mission enablers, leaders and force multipliers. But ASIO can do more. The scale and scope of Australia's adversaries requires a broader approach to security intelligence, its influence and impact.

The threat environment demands we take our engagement to a new strategic level. It's what we call 'hardening the environment'; making our economy, institutions and political system more difficult and resilient targets for those seeking to undermine them.

I started this address with a personal admission, so I might as well conclude with one, too.

The Director-General of Security is not always the most welcome visitor. All too often when I knock on a door the person who opens it looks like they are thinking, 'Uh oh—here comes the bad news.'

It's time to improve that.

Obviously, ASIO will continue to identify and communicate threats, but I want to put more emphasis on what you can do about them.

How you can protect your people, places, technology and information.

How a good security strategy addresses physical security, IT security and personal security.

As I said before, good security is achievable, and good security works.

The threats facing Australia are serious, but not insurmountable. Our adversaries are sophisticated, but not unstoppable.

In all the case studies I presented this evening—the online radicalisers, the teenage extremists, the nation-state conducting political interference—in all of them, the adversary made a mistake that brought its activities to ASIO's attention and led to the threat being mitigated.
And just in case our adversaries are listening, I should point out that you don't need to make a mistake to come to our attention. ASIO can catch you even if your tradecraft is perfect. I'll back my people any day.

ASIO will always play its part. We will protect Australia's security and safeguard its sovereignty. We will detect and defeat Australia's adversaries, and we will work with our partners to defend our nation's interests. Thank you.

The video: https://www.youtube.com/watch?v=IL2xZhN1vnM

Justice Department Announces First Director of National Cryptocurrency Enforcement Team

The Justice Department today announced the selection and appointment of Eun Young Choi to serve as the first Director of the National Cryptocurrency Enforcement Team (NCET).

Ms. Choi is a seasoned prosecutor with nearly a decade of experience within the department, and most recently served as Senior Counsel to the Deputy Attorney General. She will assume her duties full-time effective today.

“With the rapid innovation of digital assets and distributed ledger technologies, we have seen a rise in their illicit use by criminals who exploit them to fuel cyberattacks and ransomware and extortion schemes; traffic in narcotics, hacking tools and illicit contraband online; commit thefts and scams; and launder the proceeds of their crimes,” said Assistant Attorney General Kenneth A. Polite Jr. of the Justice Department’s Criminal Division. “The NCET will serve as the focal point for the department’s efforts to tackle the growth of crime involving these technologies.

Eun Young is an accomplished leader on cyber and cryptocurrency issues, and I am pleased that she will continue her service as the NCET’s inaugural Director, spearheading the department’s efforts in this area.”

The NCET was established to ensure the department meets the challenge posed by the criminal misuse of cryptocurrencies and digital assets, and comprises attorneys from across the department, including prosecutors with backgrounds in cryptocurrency, cybercrime, money laundering and forfeiture.

The NCET will identify, investigate, support and pursue the department’s cases involving the criminal use of digital assets, with a particular focus on virtual currency exchanges, mixing and tumbling services, infrastructure providers, and other entities that are enabling the misuse of cryptocurrency and related technologies to commit or facilitate criminal activity.

The NCET will set strategic priorities regarding digital asset technologies, identify areas for increased investigative and prosecutorial focus, and lead the department’s efforts to coordinate with domestic and international law enforcement partners, regulatory agencies and private industry to combat the criminal use of digital assets.

Finally, the NCET will enhance the Criminal Division's existing efforts to provide support and training to federal, state, local, and international law enforcement to build capacity to aggressively investigate and prosecute serious crimes involving cryptocurrency and digital assets in the United States and around the world.

The NCET's work will be furthered through close collaboration with components across the department, including the Criminal Division's Computer Crime and Intellectual Property Section and Money Laundering and Asset Recovery Section; the U.S. Attorneys' offices; the National Security Division; and the FBI, including the FBI's new Virtual Asset Exploitation Unit, a specialized team of cryptocurrency experts dedicated to providing analysis, support, and training across the FBI, as well as innovating its cryptocurrency tools to stay ahead of future threats.

"The department has been at the forefront of investigating and prosecuting crimes involving digital currencies since their inception," said Director Choi. "The NCET will play a pivotal role in ensuring that as the technology surrounding digital assets grows and evolves, the department in turn accelerates and expands its efforts to combat their illicit abuse by criminals of all kinds.

I am excited to lead the NCET's incredible and talented team of attorneys, and to get to work on this important priority for the department. I would like to thank Assistant Attorney General Polite and the Criminal Division's leadership for this opportunity."

Prior to her service as Senior Counsel to Deputy Attorney General Lisa O. Monaco, Director Choi began her career at the department as an Assistant U.S. Attorney for the Southern District of New York, where she served as the office's Cybercrime Coordinator and investigated and prosecuted cyber, complex fraud and money laundering crimes, with a particular focus on network intrusions, digital currency, the dark web and national security investigations.

She served as lead prosecutor in a variety of cases, including the investigation of a transnational organization responsible for the hacking of J.P. Morgan Chase and a dozen other financial companies; the operation of Coin.mx, an unlicensed virtual currency exchange; and the only U.S. prosecution brought in connection with the "Panama Papers."

In addition, she successfully argued the appeal before the Second Circuit in the case against Ross Ulbricht, the founder and chief administrator of the Silk Road, the first darknet marketplace.

Earlier in her career, she served as a law clerk to the Honorable Naomi Reice Buchwald of the U.S. District Court for the Southern District of New

York, and the Honorable Reena Raggi of the U.S. Court of Appeals for the Second Circuit. She is a graduate of Harvard College and Harvard Law School.

To read more: https://www.justice.gov/opa/pr/justice-department-announces-first-director-national-cryptocurrency-enforcement-team

Preparing for the Financial System of the Future

Governor Lael Brainard, at the 2022 U.S. Monetary Policy Forum, New York, New York

The financial system is undergoing fast-moving changes associated with digitalization and decentralization. Some of these innovations hold considerable promise to reduce transaction costs and frictions, increase competition, and improve financial inclusion, but there are also potential risks.

With technology driving profound change, it is important we prepare for the financial system of the future and not limit our thinking to the financial system of today.

The Evolving Digitalization and Decentralization of Finance

In recent years, there has been explosive growth in the development and adoption of new digital assets that leverage distributed ledger technologies and cryptography.

The market capitalization of cryptocurrencies grew from less than $100 billion five years ago to a high of almost $3 trillion in November 2021 and is currently around $2 trillion.

In parallel, we have seen rapid growth in the platforms that facilitate the crypto finance ecosystem, including decentralized finance (DeFi) platforms.

These crypto platforms facilitate a variety of activities, including lending, trading, and custodying crypto-assets, in some cases outside the traditional regulatory guardrails for investor and consumer protection, market integrity, and transparency.

The growth in the crypto finance ecosystem is fueling demand for stablecoins—digital assets that are intended to maintain stable value relative to reference assets, such as the U.S. dollar. Stablecoin supply grew nearly sixfold in 2021, from roughly $29 billion in January 2021 to $165 billion in January 2022.

There is a high degree of concentration among a few dollar-pegged stablecoins: As of January 2022, the largest stablecoin by market capitalization made up almost half of the market, and the four largest stablecoins together made up almost 90 percent.

Today, stablecoins are being used as collateral on DeFi and other crypto platforms, as well as in facilitating trading and monetization of cryptocurrency positions on and between crypto and other platforms.

In the future, some issuers envision that stablecoins will also have an expanded reach in the payment system and be commonly used for everyday transactions, both domestic and cross-border. So it is important to have strong frameworks for the quality and sufficiency of reserves and risk management and governance.

As noted in a recent report on stablecoins by the President's Working Group on Financial Markets, it is important to guard against run risk, whereby the prospect of an issuer not being able to promptly and adequately meet redemption requests for the stablecoin at par could result in a sudden surge in redemption demand.

It is also important to address settlement risk, whereby funds settlement is not certain and final when expected, and systemic risk, whereby the failure or distress of a stablecoin provider could adversely affect the broader financial system.

The prominence of crypto advertisements during the Super Bowl highlighted the growing engagement of retail investors in the crypto ecosystem. In late 2021, Pew Research found that 16 percent of survey respondents reported having personally invested in, traded, or otherwise used a cryptocurrency—up from less than 1 percent of respondents in 2015. There is also rising interest among institutional investors.

So it is perhaps not surprising that established financial intermediaries are undertaking efforts to expand the crypto services and products they offer. If the past year is any guide, the crypto financial system is likely to continue to grow and evolve in ways that increase interconnectedness with the traditional financial system.

As a result, officials in many countries are undertaking efforts to understand and adapt to the transformation of the financial system. Many jurisdictions are making efforts to ensure statutory and regulatory frameworks apply like rules to like risks, and some jurisdictions are issuing or contemplating issuing central bank currency in digital form.

Preparing for the Payment System of the Future

The Federal Reserve needs to be preparing for the payment landscape of the future even as we continue to make improvements to meet today's needs. In light of the rapid digitalization of the financial system, the Federal Reserve has been thinking critically about whether there is a role for a potential U.S. central bank digital currency (CBDC) in the digital payment landscape of the future and about its potential properties, costs, and benefits.

Our financial and payment system delivers important benefits today and is continuing to improve with developments like real-time payments. Nonetheless, certain challenges remain, such as a lack of access to digital banking and payment services for some Americans and expensive and slow cross-border payments.

Growing interest in the digital financial ecosystem suggests that technology is enabling potential improvements that merit consideration.

In addition, it is important to consider how new forms of crypto-assets and digital money may affect the Federal Reserve's responsibilities to maintain financial stability, a safe and efficient payment system, household and business access to safe central bank money, and maximum employment and price stability.

It is prudent to explore whether there is a role for a CBDC to preserve some of the safe and effective elements of the financial system of the present in a way that is complementary to the private sector innovations transforming the financial landscape of the future.

The public and private sector play important complementary roles within the financial system in the United States. From Fedwire to FedNow, the Federal Reserve has over a century of experience working to improve the infrastructure of the U.S. payment system to provide a resilient and adaptable foundation for dynamic private sector activity.

In parallel, private sector banks and nonbanks have competed to build the best possible products and services on top of that foundation and to meet the dollar-denominated needs of consumers and investors at home and around the world. The result is a resilient payment system that is responsive to the changing needs of businesses, consumers, and investors.

While the official sector provides a stable currency, operates some important payment rails, and undertakes regulation and oversight of financial intermediaries and critical financial market infrastructures, the private sector brings competitive forces encouraging efficiency and new product offerings and driving innovation.

Responsible innovation has the potential to increase financial inclusion and efficiency and to lower costs within guardrails that protect consumers and investors and safeguard financial stability.

As we assess the range of future states of the financial system, it is prudent to consider how to preserve ready public access to government-issued, risk-free currency in the digital financial system—the digital equivalent of the Federal Reserve's issuance of physical currency.

The Board recently issued a discussion paper that outlines the Federal Reserve's current thinking on the potential benefits, risks, and policy considerations of a U.S. CBDC.

The paper does not advance any specific policy outcome and does not signal that the Board will make any imminent decisions about the appropriateness of issuing a U.S. CBDC.

It lays out four CBDC design principles that analysis to date suggests would best serve the needs of the United States if one were created.

Those principles are that a potential CBDC should be privacy-protected, so consumer data and privacy are safeguarded; intermediated, such that financial intermediaries rather than the Federal Reserve interface directly with consumers; widely transferable, so the payment system is not fragmented; and identity-verified, so law enforcement can continue to combat money laundering and funding of terrorism.

Financial Stability

Given the Federal Reserve's mandate to promote financial stability, any consideration of a CBDC must include a robust evaluation of its impact on the stability of the financial system—not only as it exists today but also as it may evolve in the future.

In consideration of the financial system today, it would be important to explore design features that would ensure complementarity with established financial intermediation.

A CBDC—depending on its features—could be attractive as a store of value and means of payment to the extent it is seen as the safest form of money.

This could make it attractive to risk-averse users, perhaps leading to increased demand for the CBDC at the expense of other intermediaries during times of stress. So it is important to undertake research regarding the tools and design features that could be introduced to limit such risks, such as offering a non-interest bearing CBDC and limiting the amount of CBDC an end user could hold or transfer.

As I noted at the start, the digital asset and payment ecosystem is evolving at a rapid pace. Thus, it is also important to contemplate the potential role of a CBDC to promote financial stability in a future financial system in which a growing range of consumer payment and financial transactions would be conducted via digital currencies such as stablecoins. If current trends continue, the stablecoin market in the future could come to be dominated by just one or two issuers.

Depending on the characteristics of these stablecoins, there could be large shifts in desired holdings between these stablecoins and deposits, leading to large-scale redemptions by risk-averse users at times of stress that could prove disruptive to financial stability.

In such a future state, the coexistence of CBDC alongside stablecoins and commercial bank money could prove complementary, by providing a safe central bank liability in the digital financial ecosystem, much like cash currently coexists with commercial bank money.

It is essential that policymakers, including the Federal Reserve, plan for the future of the payment system and consider the full range of possible options to bring forward the potential benefits of new technologies, while safeguarding stability.

International Considerations

Analysis of the potential future state of the financial system is not limited to the domestic implications. The dollar is important to global financial markets: It is not only the predominant global reserve currency, but the dollar is also the most widely used currency in international payments.

Decisions by other major jurisdictions to issue CBDCs could bring important changes to global financial markets that may prove more or less disruptive and that could influence the potential risks and benefits of a U.S. CBDC.

Thus, it is wise to consider what the future states of global financial markets and transactions would look like both with and without a Federal Reserve-issued CBDC. For example, the People's Bank of China has been piloting the digital yuan, also known as e-CNY, in numerous Chinese cities over the past two years.

The substantial early progress on the digital yuan may have implications for the evolution of cross-border payments and payment systems. And it may influence the development of norms and standards for cross-border digital financial transactions.

It is prudent to consider how the potential absence or issuance of a U.S. CBDC could affect the use of the dollar in payments globally in future states where one or more major foreign currencies are issued in CBDC form.

A U.S. CBDC may be one potential way to ensure that people around the world who use the dollar can continue to rely on the strength and safety of U.S. currency to transact and conduct business in the digital financial system.

More broadly, it is important to consider how the United States can continue to play a lead role in the development of standards governing international digital financial transactions involving CBDCs consistent with norms such as privacy and security.

Given the dollar's important role as a payment instrument across the world, it is essential that the United States be on the frontier of research and policy development regarding CBDC, as international developments related to CBDC can have implications for the global financial system.

Technology Research and Experimentation

Given the range of possible future states with significant digitization of the financial system, it is important that the Federal Reserve is actively engaging with the underlying technologies.

Our work to build 24x7x365 instant payments rails leverages lessons from some of today's most resilient, high-performing, and large-scale technology platforms across the globe.

It is providing important insights on the clearing and settlement models associated with real time payments as well as on fraud, cyber resilience, cloud computing, and related technologies.

In parallel with the Board's public consultation on CBDC, the Federal Reserve Bank of Boston, in collaboration with the Massachusetts Institute of Technology, has developed a theoretical high-performance transaction processor for CBDC.

They recently published the resulting software under an open-source license as a way of engaging with the broader technical community and promoting transparency and verifiability.

Moreover, the Board is studying how innovations, such as distributed ledger technology, could improve the financial system. This work includes experimentation with stablecoin interoperability and testing of retail payments across multiple distributed payment ledger systems. The Federal

Reserve Bank of New York recently established an Innovation Center, focused on validating, designing, building, and launching new financial technology products and services for the central bank community.

These technology research and development initiatives are vital to our responsibilities to promote a safe and efficient payment system and financial stability, whatever the future may bring.

Conclusion

The financial system is not standing still, and neither can we. The digital financial ecosystem is evolving rapidly and becoming increasingly connected with the traditional financial system.

It is prudent for the Board to understand the evolving payment landscape, the technological advancements and consumer demands driving this evolution, and the consequent policy choices as it seeks to fulfill its congressionally-mandated role to promote a safe, efficient, and inclusive system for U.S. dollar transactions.

To prepare for the financial system of the future, the Federal Reserve is engaging in research and experimentation with these new technologies and consulting closely with public and private sector partners.

Largest South Korean Telecommunications Co. Agrees to Pay the SEC to Settle FCPA Charges

The Securities and Exchange Commission announced that Seoul-based KT Corporation (KT Corp.) will pay $6.3 million to resolve charges that it violated the *Foreign Corrupt Practices Act (FCPA)* by providing improper payments for the benefit of government officials in Korea and Vietnam.

According to the SEC's order, KT Corp., South Korea's largest telecommunications operator, engaged in multiple schemes to make improper payments in Korea and Vietnam.

KT Corp. lacked sufficient internal accounting controls over charitable donations, third-party payments, executive bonuses, and gift card purchases.

As a result, KT Corp. employees, including high-level executives, were able to generate slush funds that were used for gifts and illegal political contributions to government officials in Korea who had influence over KT Corp.'s business.

Other employees were able to make payments in connection with seeking business from government customers in Vietnam.

"For nearly a decade, KT Corp. failed to implement sufficient internal accounting controls with respect to key aspects of its business operations, while at the same time lacking relevant anti-corruption policies or procedures. Issuers must be sure to devote appropriate attention to meeting their obligations under the FCPA," said Charles Cain, Chief of the SEC Enforcement Division's FCPA Unit.

In November 2021, South Korean authorities indicted KT Corp. and 14 executives for criminal violations related to illegal political contributions from the slush funds.

KT Corp. consented to the SEC's order without admitting or denying the findings that it violated the books and records and internal accounting controls provisions of the Securities Exchange Act of 1934, and agreed to pay approximately $3.5 million in civil penalties and $2.8 million in disgorgement.
The SEC's investigation was conducted by Ilana Z. Sultan, Steven Susswein, and M. Shahriar Masud and supervised by Tracy L. Price.

UNITED STATES OF AMERICA
Before the
SECURITIES AND EXCHANGE COMMISSION

SECURITIES EXCHANGE ACT OF 1934
Release No. 94279 / February 17, 2022

ADMINISTRATIVE PROCEEDING
File No. 3-20780

In the Matter of **KT CORPORATION,** **Respondent.**	**ORDER INSTITUTING CEASE-AND-DESIST PROCEEDINGS PURSUANT TO SECTION 21C OF THE SECURITIES EXCHANGE ACT OF 1934, MAKING FINDINGS, AND IMPOSING A CEASE-AND-DESIST ORDER**

You may visit: https://www.sec.gov/news/press-release/2022-30

https://www.sec.gov/litigation/admin/2022/34-94279.pdf

Disclaimer

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

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

This information:

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

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

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

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

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

- is in no way constitutive of an interpretative document;

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

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

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

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

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

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.