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

News for the Board of Directors, March 2019

Dear members and friends,

Today we will start with the presentation of Commissioner Hester M. Peirce, *Remarks at Protecting the Public While Fostering Innovation and Entrepreneurship: First Principles for Optimal Regulation,* University of Missouri School of Law.

Regulation: A View from Inside the Machine

Thank you, Thom [Lambert], for that kind introduction. I am delighted to be part of this conference, but am sorry that I cannot be there in person. I had high expectations when I picked up Thom's book on regulation shortly after it first came out several years ago.

Those expectations were exceeded by the clear and compelling way in which the book wrestles with the difficulties faced by regulators as they seek to design regulations that solve problems without creating larger problems in the process. As the book explains, "regulation . . . always involves trade-offs. The $64,000 question is how policymakers should proceed to ensure that they strike those trade-offs in a manner that creates as much social welfare as possible."

I appreciate the book even more now that I am sitting in a regulator's seat. Incidentally, as a regulator, I must give the standard disclaimer that the views I express today are my own and do not necessarily represent those of the Securities and Exchange Commission or my fellow Commissioners.

Entrepreneurship and innovation do not have the happiest of relationships with regulation.

Regulators get used to dealing with the existing players in an industry, and those players tend to have teams of people dedicated to dealing with regulators.

Entrepreneurs trying to start something new are often much more focused on that new thing than on how it fits into a regulator's dog-eared rulebook.

Regulators, for their part, tend to be skeptical of change because its consequences are difficult to foresee and figuring out how it fits into existing regulatory frameworks is difficult.

Society, however, often pushes regulators to accept change. After all, society benefits from entrepreneurs' imaginative approaches to solving problems and willingness to go out on a limb with a new idea.

Society welcomes innovations that make our lives easier, more enjoyable, and more productive. In many sectors, therefore, entrepreneurship and innovation evoke overwhelmingly positive responses.

In the financial industry, entrepreneurship and innovation do not always face such a warm reception. Financial innovations, for example, were fingered by some as the cause of the last financial crisis.

Former Federal Reserve Chairman, Paul Volcker, in a negative post-crisis appraisal of financial innovation, concluded that:

The most important financial innovation that I have seen the past 20 years is the automatic teller machine . . . . How many other innovations can you tell me of that have been as important to the individual as the automatic teller machine, which is more of a mechanical innovation than a financial one?

I have found very little evidence that vast amounts of innovation in financial markets in recent years has had a visible effect on the productivity of the economy . . . .

Some people might disagree with Chairman Volcker. Take for example the man who got stuck inside an ATM a couple years ago.

In the course of repairing the machine, he got locked inside it. Without a cellphone or any other obvious way to contact the outside world, he was stuck.

It is good that he thought to slip written pleas for help to undoubtedly baffled customers. Instead of a receipt, customers got a note reading "Please help. I'm stuck in here and I don't have my phone. Please call my boss at . . . "

A customer heeded the call, and the police rescued the repairman.

The moral of the story is that every innovation—even one that almost everyone agrees is good—carries with it some risk.

Some people may get hurt by the innovation in ways we would never have imagined. Others may be helped by the innovation in ways we would never have imagined.

Some people will use the innovation in ways we wish they would not. We would be better off without some innovations, but we might not know that until after enough time has passed to see the harm they cause. In other instances, the true value of an innovation may not come to light for years.

Technological progress in the financial industry offers the same mix of hope, promise, and risk that technological progress in other parts of our society offers.

As regulators, therefore, we must allow innovation to proceed, even as we put in reasonable safeguards and watch for unanticipated consequences.

The SEC's attitude toward innovation is important because we regulate an industry that is a key gatekeeper for progress and productivity in the rest of the economy.

The United States has benefited greatly from the relative importance of non-bank financing. Without the funds that the capital markets provide, companies in other sectors of the economy would not be able to explore new ideas and develop new products and processes.

As a regulator, when I think about protecting the public, I think not only of protecting investors, but also of ensuring that the capital markets are able to serve the rest of the economy without undue barriers.

Because of the central role the markets we regulate play in ensuring that the rest of the economy is funded, we need to be open to innovations that will make the capital markets function better and serve parts of the population that were previously not able to access those markets.

Can we, for example, look for ways for unaccredited investors to pool their resources to invest in private companies?

Can we change rules that mandate the use of outdated technology in, for example, our recordkeeping rules so that financial institutions can incorporate new technology and thus lower the costs of the services they provide?

Can we allow more experimentation in the way that funds and investment advisers communicate with investors?

Can we reexamine our assumptions about the types and methods of disclosure we require in light of the enormous changes in communication technology that have occurred since the federal securities laws were written in the 1930s?

Can we permit more issuer communication with investors, which perhaps could open the door to a back-and-forth style of disclosure facilitated by online chats and message boards?

These and other innovations in the capital markets often require regulatory approvals or regulatory forbearance, both of which my agency historically has been slow to provide.

The SEC now has a wonderful opportunity to consider its approach to innovation and entrepreneurship. We have just hired our first Advocate for Small Business Capital Formation, Martha Miller.

She brings a much needed voice to an agency that has not been particularly open to thinking about the benefits that come from eliminating regulatory barriers to small issuers seeking capital.

It is not the SEC's job to shift capital flows toward small or emerging businesses; capital should flow to the companies—old, new, large, or small—that can best use it.

We ought, however, to consider whether the rules we have in place have the effect of putting a thumb on the scale in favor of large and established companies.

Having someone at the SEC whose job it is to ensure that the Commission is aware of the types of difficulties small companies face in the capital markets is an important step.

Martha's enthusiasm, knowledge, and experience suit her well for the important job she has taken on.

The agency's opportunity to rethink its approach to innovation also arises out of a decade of technological development related to blockchain and cryptocurrencies.

This area has challenged many regulators around the world, and the SEC is certainly no exception.

We, along with other regulators, are asking how existing rules apply in this space and whether a new regulatory framework would work better.

If we act appropriately, we can enable innovation on this new frontier to proceed without compromising the objectives of our securities laws—protecting investors, facilitating capital formation, and ensuring fair, orderly, and efficient markets.

One of the things that makes regulating in this space challenging is that its very essence is decentralization.

Decentralization is nothing new; it is at the root of our economic system; free markets draw on the talents and knowledge of people all across society to produce what society needs.

No person or group of persons can serve as central coordinator because such a master planner would be inherently less smart and less plugged in than the market, composed as it is of diverse individuals communicating with one another in the brutally blunt language of prices.

Yet, there is formal coordination too. Corporations, along with individuals, are key players in our markets. By joining together in a common enterprise, people are able to combine efforts and talents in ways that otherwise would not be possible.

Our securities markets have thus grown up around markets composed of individuals and corporations.

Corporations issue securities, make the attendant disclosures, and have other responsibilities under the securities laws.

Our securities laws are designed with the assumption that every issuer has someone at the helm who can authoritatively disclose the relevant material information about the organization.

Blockchain-based networks offer a new way of coordinating human action that does not fit as neatly within our securities framework. Satoshi Nakamoto, in the white paper that introduced bitcoin to the world, envisioned a “network [that] is robust in its unstructured simplicity.” Uncoordinated nodes work together toward a common end “with little coordination.”

Other blockchain projects likewise seek to build networks that operate organically, without a central organizer.

Some projects seek to facilitate various forms of authentication to replace traditional recordkeeping transactions or to allow individuals to interact without using trusted intermediaries.

The objective of many of these blockchain projects is to build networks that run on diffuse contributions, rather than to create centralized entities that run networks. In the end, there may not be anyone steering the ship.

Yet many of these projects begin in a centralized manner that looks about the same as any other start-up. A group of people get together to build something and they need to find investors to fund their efforts so they sell securities, sometimes called tokens.

The SEC applies existing securities laws to these securities offerings, which means that they must be conducted in accordance with the securities laws or under an exemption.

When the tokens are not being sold as investment contracts, however, they are not securities at all. Tokens sold for use in a functioning network, rather than as investment contracts, fall outside the definition of securities.

The Supreme Court's Howey test, which sprang from a dispute about orange groves seven decades ago, is the tool the SEC uses for discerning whether or not something is an investment contract, which is a particular type of security that includes some token offerings.

A case once only on the lips of eager law students is thus now the hot topic in crypto conversations. In a now famous speech, the SEC's Director of Corporation Finance, Bill Hinman, explained how that case, along with Gary Plastics, has informed the SEC's approach to digital assets.

As Director Hinman noted in his speech, it is the nature of the transaction that determines whether an offering of securities has occurred, not the item being sold.

The oranges in Howey were not securities standing on their own, nor were the groves in which they grew.

By contrast, the overall package sold to investors—the "opportunity to contribute money and to share in the profits of a large citrus fruit enterprise managed and partly owned by [third parties]"—was a securities offering and therefore triggered federal securities law. Purchasers' "respective shares in this enterprise are evidenced by land sales contracts and warranty deeds, which serve as a convenient method of determining the investors' allocable shares of the profits.

The resulting transfer of rights in land is purely incidental."

The Division of Corporation Finance therefore will look to the nature of a token sale to determine whether a securities offering has occurred, and not just at the qualities of the token itself.

Director Hinman went on to explain, however, that because the token "all by itself is not a security, just as the orange groves in Howey were not," a token sold in a securities offering might later be sold in a transaction that does not constitute a securities offering.

Once "a network becomes truly decentralized, the ability to identify an issuer or promoter to make the requisite disclosure becomes less meaningful" and offers and sales of tokens are no longer subject to the securities laws.

Director Hinman's speech has provided a useful framework within which people can analyze their token offerings in connection with the securities laws.

The staff is working on some supplemental guidance to help people think through whether their crypto-fundraising efforts fall under the securities laws.

There is also a standing offer for people to come in for so-called no-action relief in connection with a particular token or project.

The applicant for no-action relief lays out the parameters of what it is trying to do, and the SEC staff can respond by saying that it would not recommend an enforcement action to the Commission based on the parameters set forth in the request for relief.

Of course, the Commission also has spoken indirectly through a number of enforcement actions, which necessarily involved finding that the token offerings at issue were securities offerings.

Enforcement actions are not my preferred method for setting expectations for people trying to figure out how to raise money.

For this reason, it is important for the Commission, in conjunction with Congress and its fellow regulators, to offer something more concrete and carefully considered.

While the application of the Howey test seems generally to make sense in this space, we need to tread carefully. Token offerings do not always map perfectly onto traditional securities offerings.

For example, as a recent report from Coin Center noted, the decentralized nature of token offerings can mean that the capital raised through token sales may not be truly owned or controlled by a company.

Functions traditionally completed by people designated as "issuers" or "promoters" under securities laws—which, importantly, bestow those roles

with certain responsibilities and potential liabilities—may be performed by a number of unaffiliated people, or by no one at all.

Additionally, I am worried that the application of the test will be overly broad. The Supreme Court in Howey embraced a "flexible rather than static principle, one that is capable of adaptation," an unwelcome phrase for people craving clarity.

The subsequent application of the Supreme Court's decision has further added to the ambiguity by diluting factors, such as the prong that asks whether the investors were anticipating "profits to come solely from the efforts of others."

"Solely" has gotten dropped in the application of this prong. In the years since Howey, many courts have instead focused on whether profits are derived in effect principally from the efforts of others.

This approach has been formulated by one appellate court as a question of whether "the efforts made by those other than the investor are the undeniably significant ones, those essential managerial efforts which affect the failure or success of the enterprise."

More to the point, the Commission itself determined in 2017 that tokens issued by the DAO, a decentralized organization based on a distributed ledger, were securities despite the fact that token-holders had certain roles within the organization necessary to its operation.

Given the role that individuals play in some token environments, either through mining, providing development services, or other tasks, the SEC must take care not to cast the Howey net so wide that it swallows the "efforts of others" prong entirely.

In the realm of securities regulation, we often talk of the need for disclosure as a means of addressing information asymmetries between the issuers and the investors. The "efforts of others" prong of Howey aims at the heart of this problem.

If the investors are not in control of the enterprise, that is, if they lack material information about the operation of the organization, they will need to obtain that information from those who are in control in order to make an informed investment decision.

It is possible that some projects may simply not be able to work under the existing Howey framework and the applicable securities laws.

One cryptocurrency project, Basis, has announced that it will shut down operations and return $133 million in capital to investors due to the

difficulty—if not impossibility—of complying with securities regulations given the team's vision for the project.

I am not going to comment on what I think about the merits of any particular project or how the securities laws apply to it, but my antennae will go up when apparently legitimate projects cannot proceed because our securities laws make them unworkable.

Ambiguity is not all bad, of course. We might be able to draw clearer lines once we see more blockchain projects mature. Delay in drawing clear lines may actually allow more freedom for the technology to come into its own.

Congress may resolve the ambiguities engendered by Howey by simply requiring that at least some digital assets be treated as a separate asset class. Congressmen Warren Davidson and Darren Soto recently introduced a bill in the House intended to amend the federal securities laws to do just that, provided that the token truly operated in a decentralized network.

Such an approach would facilitate more tailored disclosure. Indeed there are others who have argued that, whether ICOs can fit within the definition of a securities offering does not answer the question of whether that is how we should regulate them.

In a forthcoming paper, Georgetown Law professor Chris Brummer and his co-authors argue that ICOs have certain features that make the regulatory framework applicable to IPOs inappropriate.

For example, changes to the blockchain may have outsized effects on certain tokens that depend on it.

An investor may need to understand, for example, how the blockchain can be changed, and how those changes would affect the relevant token before she could fully appreciate the risks of investing in that crypto asset.

There is also the fact that much of the relevant—in the terms of securities law, arguably "material"—information about a token is often found in a white paper. The terms of this paper may be highly technical and difficult for most investors to understand. In some cases, these white papers have not matched the tokens' actual code.

Whether this is due to honest error, as may be the fact in some cases, or outright fraud, as it has been in others, it raises a unique issue for regulators to address.

Much as we regulators hate to admit it, we ought not to assume that absent the application of the securities laws to the world of tokens, there would never be any order.

As Professor Lambert notes in his book, the disclosure approach built into the securities laws is designed to "prevent adverse selection by requiring informationally advantaged parties to share specified information with their counterparties."

As he explains, however, even in the absence of government directives, the informationally advantaged party may not need the government to tell it to make disclosures.

The market itself sends this message; disclosure is a way to signal quality, something you want to do when you are trying to convince someone to buy your product.

After an initial period of unbridled enthusiasm over ICOs, cooler heads seem to be thinking about ways to assess ICOs—to separate the wheat from the chaff.

Sponsors of ICOs that want to succeed will make voluntary disclosures to signal their quality. Disclosure will happen regardless of whether the securities disclosure regime applies to ICOs.

Moreover, the platforms that trade cryptocurrencies can play a role in forcing such disclosures, much as the stock exchanges did before the securities laws took effect.

Our interactions with cryptocurrencies are not limited to questions about the regulation of token sales and disclosures.

Closely linked to the question of whether tokens are securities is the question of how the platforms on which tokens trade should be regulated.

Some of these platforms want to register with us, and I am eager to make progress on this front.

There are features of crypto trading platforms that may differ from exchanges or alternative trading systems designed for traditional securities.

To identify how regulation may need to change to accommodate these differences we will need to improve our understanding of how the platforms operate.

There is also great interest in exchange-traded products based on bitcoin or other cryptocurrencies.

As I have mentioned in the past, I am concerned that our approach with respect to such products borders on merit-based regulation, which means

that we are substituting our own judgment for that of potential investors in these products.

We rightfully fault investors for jumping blindly at anything labeled crypto, but at times we seem to be equally impulsive in running away from anything labeled crypto.

We owe it to investors to be careful, but we also owe it to them not to define their investment universe with our preferences.

I would like to conclude by drawing again from Professor Lambert's book. His definition of "regulation" as "any threat-backed governmental directive aimed at fixing a defect in 'private ordering' . . ." reminds us of the gravity of the regulator's task.

Private ordering is the baseline because, as the book explains, "when property rights are well defined and transferable, and individuals are able to strike trustworthy exchange agreements, markets will emerge and channel productive resources to … [the] production of the goods and services individuals value most."

Regulation involves overruling private arrangements, substituting a government mandate, and imposing a penalty of some sort on people who fail to comply with that mandate.

Given the potential consequences of doing these things, the regulator and the people on whose behalf it regulates must think carefully about whether and how regulation should be employed.

That careful thinking, however, may mean frustration for the innovators hoping for quick answers about what the relevant regulations are.

Channel that frustration by coming and talking to us about how you think we should approach these regulatory questions.

Sometimes I feel like the repairman in the ATM sending slips of paper to the outside world asking for help.

In my case, I am asking for help on getting the regulations right so that innovators and entrepreneurs can spend their time and attention on making better products, providing better services, and revolutionizing the way we interact with one another.

Recent economic developments and longer-term challenges

Jerome H Powell, Chairman of the Board of Governors of the Federal Reserve System, at the Citizens Budget Commission 87th Annual Awards Dinner, New York City.

It is a pleasure to speak here this evening at the 87th Awards Dinner. Tonight I will start with the near-term outlook for the U.S. economy. Then I will turn to a topic that is inspired by the Citizens Budget Commission's mission statement, which focuses on the "well-being of future New Yorkers."

I imagine that future New Yorkers attending this dinner in 50 years may not look back on the near-term outlook in February 2018 as very interesting or important.

So, tonight, after a brief review of the here and now, I will focus on an issue that is likely to be of more lasting importance: the need for policies that will support and encourage participation in the labor force, promote longer-term growth in our rapidly evolving economy, and spread the benefits of prosperity as widely as possible.

The State of the Economy and Near-Term Prospects

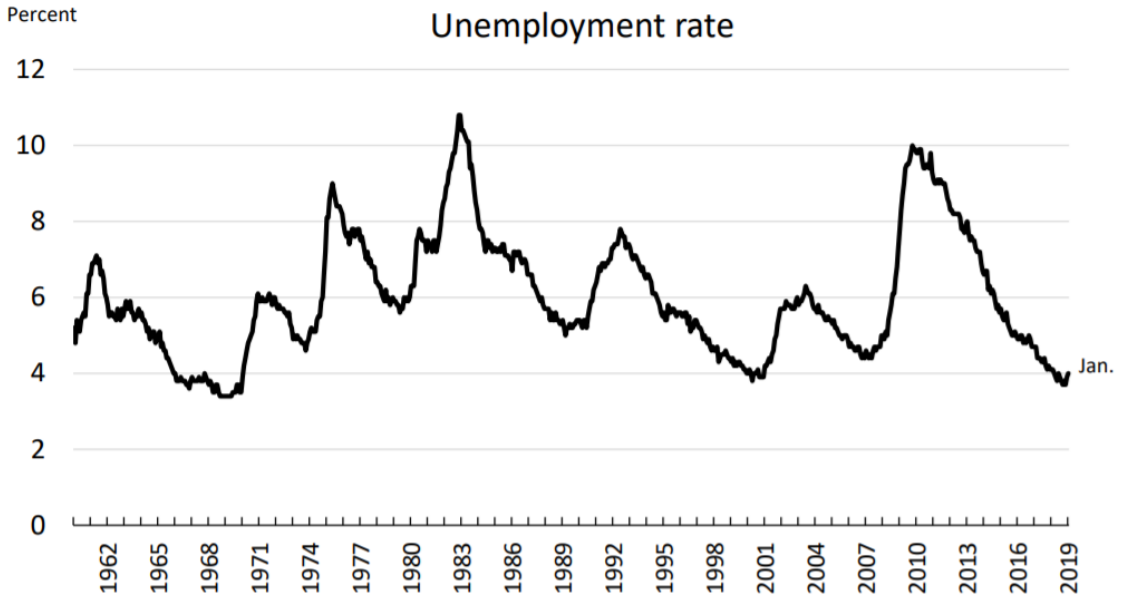
Beginning with the here and now, Congress has charged the Federal Reserve with achieving maximum employment and stable prices, two objectives that together are called the dual mandate.

I am pleased to say that, judged against these goals, the economy is in a good place.

The current economic expansion has been under way for almost 10 years.

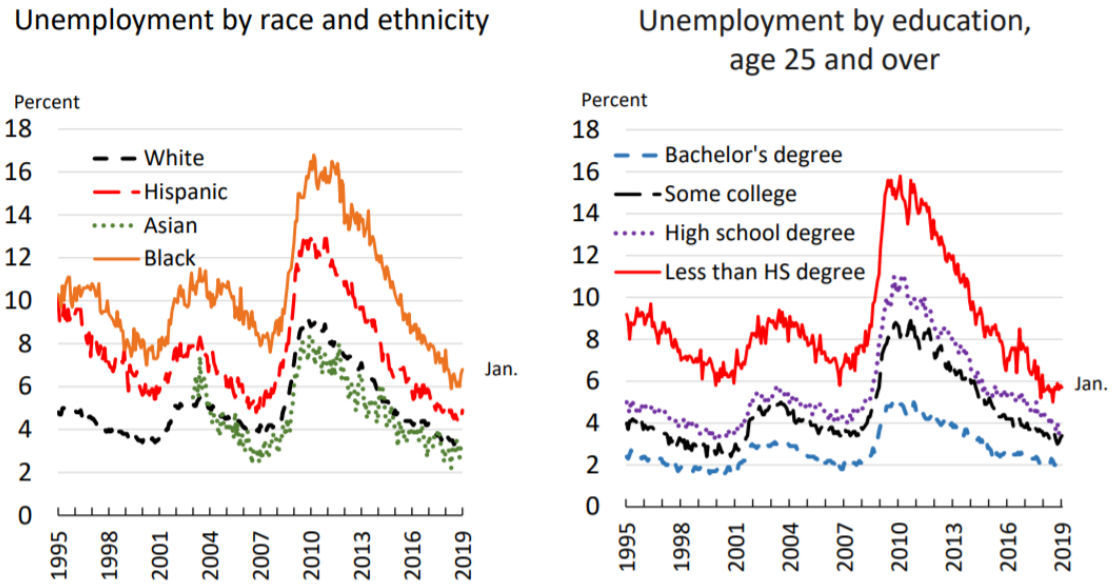
This long period of growth has pushed the unemployment rate down near historic lows.
The employment gains have been broad based across all racial and ethnic groups and all levels of educational attainment as well as among the disabled.

Figure 1. Unemployment is near historic lows



Source: Bureau of Labor Statistics.

Figure 2. Improvement in unemployment is broadly shared



Source: Bureau of Labor Statistics.

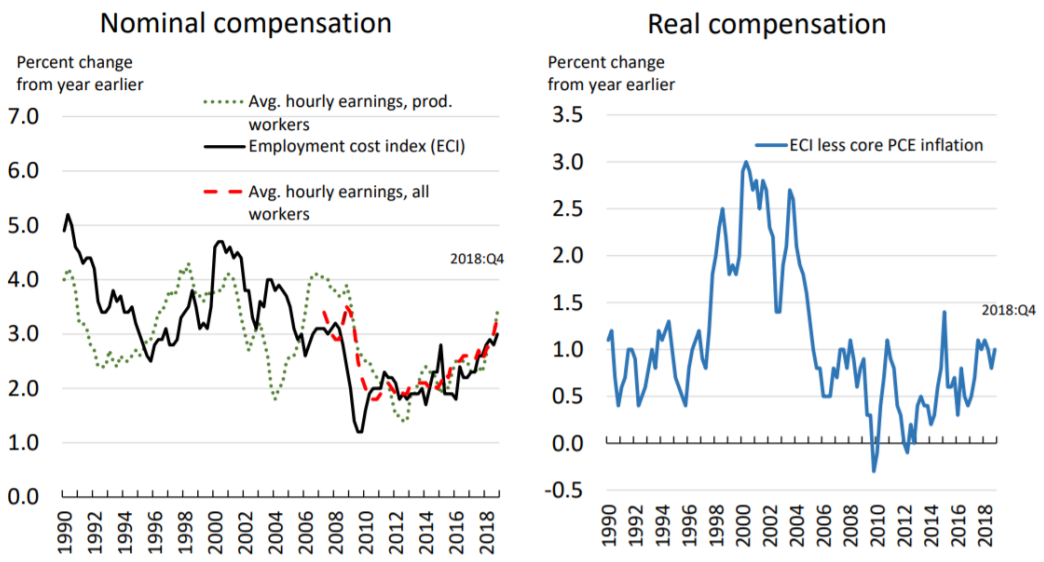
And while the unemployment rate for African Americans and Hispanics remains above the rates for whites and Asians, the disparities have narrowed appreciably as the economic expansion has continued.

Nearly all job market indicators are better than a few years ago, and many are at their most favorable levels in decades.

After lagging earlier in the expansion, wages and overall compensation--pay plus benefits--are now growing faster than a few years ago (figure 3).

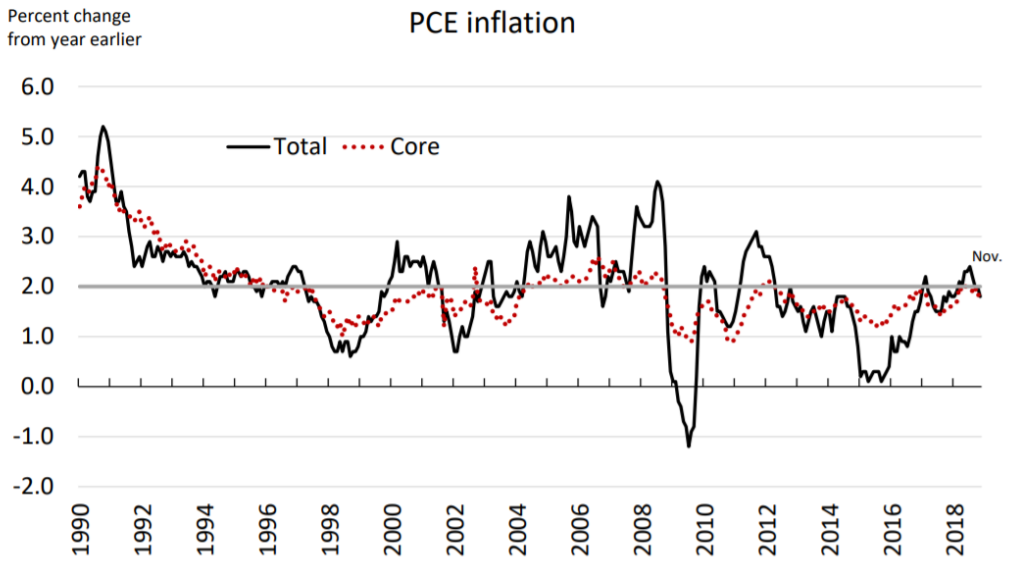
It is especially encouraging that the labor force participation rate of people in their prime working years, ages 25 to 54, has been rising for the past three years.

Figure 3. Wage growth has picked up, but it is still moderate



Source: Bureau of Labor Statistics.

Figure 4. Inflation is running near target



Source: Bureau of Economic Analysis.

More plentiful jobs and rising wages are drawing more people into the workforce and encouraging others who might have left to stay. In addition, business-sector productivity growth, which had been disappointing during the expansion, moved up in the first three quarters of 2018.

Rising productivity allows wages to increase without adding to inflation pressures. Sustained productivity growth is a necessary ingredient for longer-run improvements in living standards. The price stability side of our mandate is also in a good place.

After remaining below our target for several years, inflation by our preferred measure averaged roughly 2 percent last year (figure 4).

Inflation has softened a bit since then, largely reflecting the recent drop in oil prices.

Futures markets and other indicators suggest that oil prices are unlikely to fall further, and if this proves correct, oil's drag on overall inflation will subside.

Consistent with that view, core inflation, which excludes volatile food and energy prices and often provides a better signal of where inflation is heading, is currently running just a touch below our 2 percent objective.

Signs of upward pressure on inflation appear muted despite the strong labor market.

While the data I have discussed so far give a favorable picture of the economy, it is also important to acknowledge that not everyone has shared in the benefits of the expansion to the same extent, and that too many households still struggle to make ends meet.

In addition, over the past few months we have seen some crosscurrents and conflicting signals about the near-term outlook.

For instance, growth has slowed in some major economies, particularly China and Europe.

Uncertainty is elevated around some unresolved government policy issues, including Brexit and ongoing trade negotiations.

And financial conditions have tightened since last fall.

While most of the incoming domestic economic data have been solid, some surveys of business and consumer sentiment have moved lower.

Unexpectedly weak retail sales data for December also give reason for caution.

To read more:
https://www.bis.org/review/r190301a.pdf

Basel Committee discusses policy and supervisory initiatives and approves implementation reports

The Basel Committee on Banking Supervision met in Basel on 27-28 February to discuss a range of policy and supervisory issues, and to take stock of its members' implementation of post-crisis reforms.

At its meeting, the Committee:

- took note of the implementation status of margin requirements for non-centrally cleared derivatives. The Committee will publish in March a joint statement with the International Organization of Securities Commissions to clarify certain implementation aspects of the margin requirements framework;

- reiterated its support for reforms of interest rate benchmarks and approved a work plan to look at the interactions with supervisory requirements;

- agreed to publish high-level supervisory expectations related to crypto-assets in light of the high degree of risks associated with such exposures. These expectations will be published in March;

- discussed the use of different practices among jurisdictions to proportionately apply the Basel Committee's global minimum prudential standards, and agreed to publish a summary of these practices in March;

- reviewed the assessment reports on the implementation of the Net Stable Funding Ratio and large exposures standards in Brazil and India. Publication of these reports is expected in the coming months; and

- reviewed the follow-up reports and actions by member jurisdictions on the implementation of certain Basel III standards. These will be published in March.

The Committee also discussed its work programme for evaluating the impact of its post-crisis reforms.

The programme includes planned evaluations related to cross-cutting policy issues, the countercyclical capital buffer framework and the global systemically important banks framework.

Committee members also discussed issues related to sovereign risk.

The next meeting of the Basel Committee is tentatively scheduled for 19-20 June 2019.

CCP resilience, recovery and resolution: completing the journey towards resilient derivatives markets

Deutsche Bundesbank, European Central Bank and the Federal Reserve Bank of Chicago Conference on CCP Risk Management, Frankfurt
Remarks by Dietrich Domanski, Secretary General, Financial Stability Board

Ladies and gentlemen, it is good to be here today. The Deutsche Bundesbank, European Central Bank and the Federal Reserve Bank of Chicago have shown real leadership in convening this conference.

Today's agenda shows that we have come a long way in reforming derivatives markets.

Almost ten years ago, at the Pittsburgh Summit in September 2009, G20 Leaders declared that all standardised over-the-counter (OTC) derivative contracts should be traded on exchanges or electronic trading platforms, where appropriate, and cleared through central counterparties.

The declaration made central clearing an essential element of the reforms to reduce the complex and opaque web of exposures that existed between derivatives counterparties.

Since then, we have put in place a framework to fundamentally reform derivatives markets.

This includes measures related to central clearing, but also policies to enhance the transparency and resilience of markets for non-centrally cleared derivatives, through trade reporting and margin requirements.

Yet derivatives markets reform is only one key area of post-crisis regulatory efforts.

There is also significant progress in making the banking system more resilient; implementation of too-big-to-fail reforms is advancing, including via the establishment of effective resolution regimes for banks; and those aspects of non-bank financial intermediation that contributed to the financial crisis have declined significantly and generally no longer pose financial stability risks.

But, as today's conference shows, important issues still lie ahead.

What I would like to do in my remarks is to put CCP-related reforms into perspective – by looking back at what we have accomplished, and discuss what remains to be done from the perspective of the FSB; and by relating CCP-related policy measures to progress in other areas.

What we have accomplished?

CCPs have become central to the global financial system

Let me begin with a few simple numbers that illustrate how central CCPs have become for the financial system.

In 2009, the clearing level was around 24% for interest rate derivatives and just 5% for credit derivatives.

By June 2018 these levels had risen to approximately 62% for interest rate derivatives and 37% for credit derivatives.

Today, 90% of new OTC single currency interest rate derivatives are now centrally cleared in the US.

This impressive shift has been accompanied by the enhancement of legislative or regulatory frameworks to promote central clearing.

Such frameworks, including comprehensive standards for determining when OTC derivatives should be required to be centrally cleared, are now in place in 18 FSB jurisdictions.

Our latest annual report shows a continued broadening of the range of asset classes that are centrally cleared.

Policy measures to promote central clearing are working. Last year, the FSB, Basel Committee on Banking Supervision (BCBS), Committee on Payments and Market Infrastructures (CPMI) and the International Organization of Securities Commissions (IOSCO) published the results of its evaluation of the incentives to centrally clear OTC derivatives.

The report found that the reforms – particularly capital requirements, clearing mandates and margin requirements for non-centrally cleared derivatives – are achieving the goal of promoting central clearing, especially for the most systemic market participants.

However, the report also found that beyond the systemic core of the derivatives network of CCPs, dealers/clearing service providers and larger, more active clients, the incentives are less strong.

Significant work has been devoted to CCP resilience, recovery and resolvability

The shift to central clearing has made CCPs both larger and more systemic.

Cognizant of their even more central role in the financial system, authorities have made significant efforts to ensure that CCPs are safe and sound.

The CPMI-IOSCO Principles for Financial Market Infrastructures (PFMI) are a milestone in this regard.

In July 2017, the FSB working with CPMI, IOSCO and the BCBS completed a workplan on CCP resilience, recovery and resolvability.

The three reports coming out of the workplan provide guidance on a broad range of issues:

• CPMI and IOSCO set out further guidance on the PFMI regarding resilience of CCPs, in particular on governance, credit and liquidity stress testing, coverage, margin, and a CCP's contributions of its financial resources to losses.

• CPMI and IOSCO also updated their 2014 guidance on recovery for financial market infrastructures to provide clarifications in a number of areas including the operationalisation of recovery plans and non-default related losses.

• And the FSB published guidance on how to implement its Key Attributes in resolution arrangements for CCPs.

To read more:
http://www.fsb.org/wp-content/uploads/S270219.pdf

Statement by Gabriel Bernardino, Chair of the Joint Committee of the European Supervisory Authorities

ECON scrutiny hearing on PRIIPs 20 February 2019 Brussels

JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

Honourable Chair and Members of the Parliament,

It is my pleasure to address you today in my role as Chair of the Joint Committee of the European Supervisory Authorities (ESAs) for 2019.

I would like to thank the Chair and the Members of the ECON committee for the opportunity to provide an update on the ESAs' work in relation to the delegated acts for the key information documents (KID) for packaged retail and insurance-based investment products (PRIIPs).

First of all, I would like to underline the importance of the KID in increasing the transparency and comparability of investment products through the issue of a standardised short form disclosure document.

We are committed to supporting an effective and convergent implementation of these rules as a variety of different national approaches to the KID will not help PRIIP manufacturers, distributors, or most importantly, consumers, particularly in the context of cross-border business.

We are also committed to reviewing the existing rules, where this is needed, so they can apply equally well to all different types of PRIIPs.

It is normal with rules as complex as these to refine and adjust them based on practical experience with what works well and what less well.

We are aware that stakeholders have raised strong concerns regarding some aspects of the current rules.

We have been examining these issues and considering what to do. In some cases, we have published Questions and Answers to clarify technical points. However, we decided in the autumn of last year that the best course of action on some issues was to propose targeted amendments to the PRIIPs Delegated Regulation.

We launched a public consultation in November last year, which focused on changes to the performance scenarios.

These have been the part of the KID that have raised the most critical issues.

We also proposed changes in the consultation to avoid a duplication of disclosures between PRIIPs and UCITS, which we were concerned risked undermining the aims of these disclosures.

I would like to summarise briefly some of the main themes that emerged from this public consultation:

- There is a consensus amongst stakeholders that the current performance scenarios in the KID should not be taken as best estimate forecasts, yet there is a risk that consumers read them that way. Stakeholders also expressed concerns that the current economic environment leads to scenarios that may not sufficiently reflect market expectations that future returns are going to be lower, at least in some markets;

- The proposals that the ESAs made to strengthen the warnings in the KID were generally supported. However, it was stated that there are no "quick-fixes" that can be made to the performance scenario methodology and, therefore, it was suggested that the ESAs should undertake a comprehensive analysis of alternative approaches;

- For certain types of PRIIPs, such as actively managed funds, both industry and consumer associations are of the view that the most relevant information for the consumer is the PRIIP's past performance;

- While the ESAs' public consultation focused on performance scenarios, a number of respondents, many from the asset management sector, also highlighted the importance of reviewing aspects of the cost disclosures.

When deciding on our final recommendations, we carefully considered this feedback. We also took into account the expected decision by the co-legislators to defer the application of the KID to UCITS by two years to the end of 2021.

Given this, we concluded, as published in early February, that it was not appropriate to propose narrowly targeted amendments at this stage.

However, we consider that immediate supervisory steps are needed to reduce the risk that the meaning of the current performance scenario figures is misinterpreted or there is undue reliance on them.

We have therefore issued a joint ESA Supervisory Statement to promote consistent approaches and improve the protection of retail investors prior to the conclusion of a fuller review.

In the statement, the ESAs recommend PRIIP manufacturers to include a warning in the KID to ensure that retail investors are fully aware of the limitations of the figures provided.

In our February publication, we also said we would launch a more comprehensive review of the PRIIPs Delegated Regulation this year, and set out the main areas of the rules that we intended to address.

I would like to highlight a number of these aspects now:

- We intend to cover issues related to performance as well as costs disclosure. This will include assessing whether the transaction cost methodology and reduction in yield approach should be adjusted. We will also draw on our analysis of KIDs during the work started last year to report on an annual basis on the costs and past performance of investment products;

- We will focus our work on possible amendments to the PRIIPs Delegated Regulation. However, where our work indicates changes to the PRIIPs Level 1 Regulation are needed to achieve the optimal outcomes at Level 2, we would intend to recommend such changes also;

- Given the very wide scope of the Regulation, and to ensure the KID works equally well for all products, we think that some further differentiation in approach for different types of PRIIPs may be needed, while still adhering to the aim of comparability between substitutable products;

- We intend to carry out consumer testing, including both the existing KID and alternatives.

The important thing is to keep a firm view on the original aims of the Regulation – giving consumers better and easier to understand information – and to avoid endangering this aim further during the upcoming review process.

In this regard we welcome input from Members of Parliament on how to improve the transparency and comparability of the KID, to make it work better for the consumers it has been designed for.

Finally, we welcome the confirmation that amendments to the PRIIPs Regulation will be made this year regarding the issue of the duplication of

disclosures between PRIIPs and UCITS; some minor consequential adjustments to align the PRIIPs Delegated Regulation with the new deadline will also be needed.

We now have the time to ensure the PRIIPs KID can work for all products, including UCITS. This will enhance the ability for consumers to compare between investment products and ensure a level-playing field for providers.

EIOPA CALLS UPON NATIONAL SUPERVISORY AUTHORITIES TO MINIMISE THE DETRIMENT TO INSURANCE POLICYHOLDERS AND BENIFICIARIES IN CASE OF A NO WITHDRAWAL AGREEMENT BETWEEN THE UNITED KINGDOM AND THE EUROPEAN UNION

- The Recommendations provide guidance on the treatment of UK insurance undertakings and distributors with regard to cross-border services in the European Union after the withdrawal of the United Kingdom from the European Union without a withdrawal agreement.

- The objective of the Recommendations is to minimise the detriment to policyholders with such cross-border insurance contracts.

- The Recommendations addressed to National Competent Authorities (NCAs) are to foster supervisory convergence and to ensure consistent supervisory practices.

- Policyholders residing in the European Union other than the United Kingdom (EU27) with insurance contracts from UK insurance undertakings may face uncertainty after the withdrawal of the United Kingdom, in case their undertakings have not taken measures to ensure the continuity of their insurance services in the EU27.

The European Insurance and Occupational Pensions Authority (EIOPA) has issued Recommendations for the insurance sector in light of the United Kingdom (UK) withdrawing from the European Union without a withdrawal agreement.

The Recommendations addressed to National Competent Authorities (NCAs) provide guidance on the treatment of UK insurance undertakings and distributors with regard to cross-border services in the European Union after the withdrawal of the United Kingdom from the European Union without a withdrawal agreement.

The Recommendations will apply as of the date following that on which the European Union's acquis ceases to apply to and in the United Kingdom.

In case the United Kingdom withdraws from the European Union without ratification of the withdrawal agreement, on 30 March 2019 the United Kingdom becomes a third country and UK insurance undertakings and

distributors lose their right to conduct business across the EU27 Member States by way of freedom of establishment and freedom to provide services.

In principle, insurance contracts concluded before that date by UK insurance undertakings in the EU27 are valid after that date.

However, the insurance undertakings would not anymore be authorised to carry out insurance activities with regard to these cross-border insurance contracts.

On 21 December 2017, EIOPA issued an Opinion, calling on the NCAs to ensure that insurance undertakings with affected cross-border business develop realistic contingency plans setting out measures to prevent insurance activity without authorisation and ensuring service continuity after the United Kingdom's withdrawal and the implementation of those measures.

Many UK insurance undertakings, in particular with large cross-border business in the EU27, have already taken action and are implementing contingency measures.

However, there is a residual amount of insurance business in the EU27 for which UK insurance undertakings have not taken appropriate measures - as of November 2018, 124 UK insurance undertakings, representing about 0.16% of the total insurance business in the EU27.

The Recommendations provide guidance on the supervisory treatment of residual insurance business with the objective to minimise the detriment to policyholders with such cross-border insurance contracts.

NCAs should ensure an orderly run-off of the insurance business, including the appropriate supervision.

UK insurance undertakings without authorisation should not conclude new insurance contracts.

Furthermore, the Recommendations provide guidance on the application of relevant legal provisions with regard to cross-border insurance of UK insurance undertakings.

The nine Recommendations are ranging from the authorisation of third country-branches, the lapse of authorisation, the cooperation between the national competent authorities, the communication to policyholders and beneficiaries to distribution activities.

In particular, the following three Recommendations are to be highlighted:

- Orderly run-off: Without prejudice to policyholder rights to exercise an option or right in an existing insurance contract to realise their pension benefits, the NCAs should prevent that UK undertakings conclude new insurance contracts or establish, renew, extend, increase or resume insurance cover under the existing insurance contracts in their jurisdiction as long as they are not authorised for such insurance activities under Union law.

- Portfolio transfer: Provided that it was initiated before the withdrawal date, the NCAs should allow the finalisation of portfolio transfer from UK insurance undertakings to EU27 insurance undertakings.

- Change in the habitual residence or establishment of the policyholder: If a policyholder with habitual residence or, in the case of a legal person, place of establishment in the United Kingdom concluded a life insurance contract with a UK insurance undertaking and afterwards the policyholder changed its habitual residence of place of establishment to a EU27 Member State, the NCAs should take into account in the supervisory review that the insurance contract was concluded in the United Kingdom and the UK insurance undertaking did not provide cross-border services for the EU27 for this contract.

Enhanced cooperation between NCAs is necessary to address issues arising from unauthorized cross-border insurance.

EIOPA will facilitate the necessary cooperation through the establishment of cooperation platforms.

UK insurance undertakings should disclose the consequences for their rights and obligations to the policyholders and beneficiaries of contracts affected by the United Kingdom's withdrawal.

Guidance on the application of the legal framework for insurance intermediation regarding UK distributors after the withdrawal of the United Kingdom is also part of the Recommendations.

Gabriel Bernardino, Chairman of EIOPA, said: "Besides the fact that UK insurance undertakings have taken appropriate measures for most the cross-border insurance into the EU27, there is a residual amount of business that would become unauthorised when the United Kingdom leaves the European Union. To ensure the protection of policyholders and beneficiaries concerned national supervisors have to ensure consistent supervisory actions and to cooperate closely and effectively."

The Recommendations can be obtained at:
https://eiopa.europa.eu/Publications/Standards/EIOPA-BoS-19-040_Recommendation_Brexit_final.pdf

Recommendation 1 – General objective

In their treatment of cross-border business of UK insurance undertakings, competent authorities should aim to minimise the detriment to policyholders and beneficiaries, based on the applicable EU and national laws.

Recommendation 2 – Orderly run-off

Competent authorities should apply a legal framework or mechanism to facilitate the orderly run-off of business which became unauthorised or they should require the insurance undertakings to immediately take all necessary measures to become authorised under Union law.

Competent authorities should prevent that UK undertakings conclude new insurance contracts or establish, renew, extend, increase or resume insurance cover under the existing insurance contracts in their jurisdiction as long as they are not authorised for such insurance activities under Union law.

This is without prejudice to policyholder rights to exercise an option or right in an existing insurance contract to realise their pension benefits.

Competent authorities should make every effort to supervise the cross-border business of UK insurance undertakings in their jurisdictions.

The supervision should include conduct supervision and, in co-operation with the supervisory authorities in the UK, appropriate oversight of the relevant prudential aspects of the cross-border business, including the financial position of the UK undertaking.

The supervision should be risk-based and take into account proportionality.

Recommendation 3 – Authorisation of third-country branches

In accordance with Article 162 of the Solvency II Directive, UK insurance undertakings may seek authorisation to carry out cross-border business through a branch in a Member State and thus ensure that they can service cross-border business in that Member State.

In assessing whether the legal conditions for the authorisation of such a branch are fulfilled, competent authorities should apply the principle of proportionality and take into account that the UK insurance undertaking was subject to Solvency II requirements before the UK's withdrawal.

Where it would accelerate the authorisation procedure, competent authorities should consider restricting the authorisation of the branch to the run-off of existing business.

Recommendation 4 - Lapse of authorisation

Where the legal framework of a Member State includes provisions on the treatment of insurance undertakings after a lapse of their authorisation as referred to in Article 144(1)(a) of the Solvency II Directive, the competent authority should consider applying these provisions to UK insurance undertakings in their jurisdiction after the UK's withdrawal.

In that case, the competent authority should make every effort to ensure an effective enforcement of those provisions, in co-operation with the supervisory authorities in the UK.

Recommendation 5 – Portfolio transfers

Competent authorities should allow the finalisation of portfolio transfers from UK insurance undertakings to EU27 insurance undertakings, provided that it was initiated before the withdrawal date.

For that purpose, competent authorities should co-operate closely with the supervisory authorities in the UK taking into account the requirements of Article 39 of the Solvency II Directive and the provisions of Section 4.2.1. of the Decision of the Board of Supervisors on the collaboration of the insurance supervisory authorities of the Member States of the European Economic Area of 30 January 2017 (EIOPA-BoS17/014).

Competent authorities should deem a portfolio transfer to be initiated in case the UK supervisory authorities have notified them about the initiation of the portfolio transfer and the UK insurance undertaking has paid the regulatory transaction fee to the supervisory authority(s) in the UK and appointed an independent expert for the transfer.

Recommendation 6 – Change in the habitual residence or establishment of the policyholder

Where a policyholder with habitual residence or, in the case of a legal person, place of establishment in the UK concluded a life insurance contract with a UK insurance undertaking and afterwards the policyholder changed its habitual residence or place of establishment to a EU27 Member State, competent authorities should take into account in the supervisory review that the insurance contract was concluded in the UK and the UK insurance undertaking did not provide cross-border services for the EU27 for this contract.

Competent authorities should apply the same approach to non-life insurance contracts that do not relate to buildings or to buildings and their contents or to vehicles.

Recommendation 7 – Cooperation between competent authorities

Where a UK insurance undertaking has cross-border business in more than one Member State, the competent authorities of those Member States should co-operate with regard to supervising that business, in particular by exchanging the following information, taking into account the principle of proportionality:

(a) the nature and scale of the cross-border business in their jurisdiction;

(b) measures taken or planned by the undertaking to ensure an orderly run-off of the cross-border business;

(c) supervisory measures taken or, where appropriate, intended by the competent authority with regard to the undertaking;

(d) any conduct or solvency issues identified with regard to the undertaking.

Where deemed necessary, EIOPA may establish a cooperation platform for a specific undertaking with the participation of the competent authorities concerned.

Competent authorities should make every effort to participate in the platform.

Recommendation 8 – Communication to policyholders and beneficiaries

Competent authorities should inform UK insurance undertakings with crossborder business in their Member State of the requirement to disclose to the policyholders and beneficiaries of those contracts that are affected by the consequences of the UK's withdrawal, the consequences for the rights and obligations of policyholders and beneficiaries regarding those contracts.

Competent authorities should remove the UK insurance undertakings from the national register of insurance undertakings upon the withdrawal date and inform the public about the legal framework applicable to the cross-border business of UK insurance undertakings.

Recommendation 9 – Distribution activities

Competent authorities should ensure that UK intermediaries and entities which intend to continue or commence distribution activities to EU27 policyholders and for EU27 risks after the UK's withdrawal are established and registered in the EU27 in line with the relevant provisions of the IDD.

Competent authorities should ensure that intermediaries, which are legal persons and are established and registered in the Union, demonstrate an appropriate level of corporate substance, proportionate to the nature, scale and complexity of their business.

These intermediaries should not display the characteristics of an empty shell.

Moreover, the professional and organisational requirements of the IDD must be met on a continuous basis.

This is without prejudice to the right of the Member States to introduce special provisions in their national law for third country intermediaries, provided that equal treatment of intermediaries on the respective market is guaranteed.

When assessing whether a specific UK intermediary or entity is providing distribution activities in the EU, competent authorities should take into account that only the consistent and uniform application of the IDD can guarantee the same level of protection for consumers and ensure a level playing field in the Union.

Competent authorities should ensure that all intermediaries carrying out distribution activities which target EU27 policyholders and EU27 risks fall under the scope of the IDD.

For this purpose, competent authorities should assess any distribution model against the definition of distribution activity as provided for in the IDD.

Written testimony of CISA Director Christopher Krebs for a House Committee on Homeland Security hearing titled "Defending Our Democracy: Building Partnerships to Protect America's Elections"

Chairman Thompson, Ranking Member Rogers, and members of the Committee, thank you for the opportunity to testify regarding the U.S. Department of Homeland Security's (DHS) progress in reducing and mitigating risks to our Nation's election infrastructure.

DHS has worked to establish trust-based partnerships with state and local officials who administer our elections, and I look forward to sharing with you an update on our work during the 2018 midterm election cycle.

Leading up to the 2018 midterms, DHS worked hand in hand with federal partners, state and local election officials, and private sector vendors to provide them with information and capabilities to enable them to better defend their infrastructure. This partnership led to a successful model that we aim to continue and improve upon in the 2020 election cycle.

Since 2016, DHS's Cybersecurity and Infrastructure Security Agency (CISA) has led a voluntary partnership of Federal Government and election officials who regularly share cybersecurity risk information.

CISA has engaged directly with election officials—coordinating requests for assistance, risk mitigation, information sharing, and incident response.

To ensure a coordinated approach, CISA convened stakeholders from across the Federal Government through the Election Task Force.

The Department and the Election Assistance Commission (EAC) have convened federal government and election officials regularly to share cybersecurity risk information and to determine an effective means of assistance.

Since 2016, the Election Infrastructure Subsector (EIS) Government Coordinating Council (GCC) has worked to establish goals and objectives,

to develop plans for the EIS partnership, and to lay the groundwork for developing an EIS Sector-Specific Plan.

Participation in the council is entirely voluntary and does not change the fundamental role of state and local jurisdictions in overseeing elections.

DHS and the EAC have also worked with election vendors to launch an industry-led Sector Coordinating Council (SCC), a self-organized, self-run, and self-governed council with leadership designated by sector membership.

The SCC serves as the industry's principal entity for coordinating with the Federal Government on critical infrastructure security activities related to sector-specific strategies.

This collaboration is conducted under DHS's authority to provide a forum in which federal and private sector entities can jointly engage in a broad spectrum of activities to coordinate critical infrastructure security and resilience efforts which is used in each of the critical infrastructure sectors established under Presidential Policy Directive 21, Critical Infrastructure Security and Resilience. The SCC has helped DHS further its understanding of the systems, processes, and relationships particular to operation of the EIS.

Within the context of today's hearing, I will address our efforts in 2018 to help enhance the security of elections that are administered by jurisdictions around the country, along with our election related priorities through 2020.

While there was activity targeting our election infrastructure leading up to the midterms, this activity is similar to what we have seen previously and occurs on the Internet every day.

This activity has not been attributed to nation-state actors and along with the Department of Justice (DOJ), we concluded that there is no evidence to date that any identified activities of a foreign government or foreign agent had a material impact on the integrity or security of election infrastructure or political or campaign infrastructure used in the 2018 midterm elections

Assessing the Threat

The Department regularly coordinates with the Intelligence Community and law enforcement partners on potential threats to the Homeland. Among non-federal partners, DHS has engaged with state and local officials, as well as relevant private sector entities, to assess the scale and

scope of malicious cyber activity potentially targeting the U.S. election infrastructure.

Election infrastructure includes the information and communications technology, capabilities, physical assets, and technologies that enable the registration and validation of voters; the casting, transmission, tabulation, and reporting of votes; and the certification, auditing, and verification of elections.

In addition to working directly with state and local officials over the past two years, we have partnered with trusted third parties to analyze relevant cyber data, including the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC), the National Association of Secretaries of State, and the National Association of State Election Directors.

DHS field personnel deployed around the country furthered information sharing and enhanced outreach.

Enhancing Security

During the 2018 midterms, CISA provided a coordinated response from DHS and its federal partners to plan for, prepare for, and mitigate risk to election infrastructure.

Working with election infrastructure stakeholders was essential to ensuring a more secure election.

CISA and our stakeholders increased awareness of potential vulnerabilities and provided capabilities to enhance the security of U.S. election infrastructure as well as that of our democratic allies.

Election officials across the country have a long-standing history of working both individually and collectively to reduce risks and ensure the integrity of their elections.

In partnering with these officials through both new and ongoing engagements, CISA will continue to work to provide value-added—yet voluntary—services to support their efforts to secure elections in the 2020 election cycle.

Improving Coordination with State, Local, Tribal, Territorial and Private Sector Partners

Increasingly, the nation's election infrastructure leverages information technology for efficiency and convenience, but also exposes systems to cybersecurity risks, just like in any other enterprise environment.

Just like with other sectors, CISA helps stakeholders in federal departments and agencies, state, local, tribal, and territorial (SLTT) governments, and the private sector to manage these cybersecurity risks.

Consistent with our long-standing partnerships with state and local governments, we have been working with election officials to share information about cybersecurity risks, and to provide voluntary resources and technical assistance.

CISA works with the EI-ISAC to provide threat and vulnerability information to state and local officials. Through funding by CISA, the Center for Internet Security created and continues to operate the EI-ISAC.

The EI-ISAC has representatives co-located with CISA's National Cybersecurity and Communications Integration Center (NCCIC) to enable regular collaboration and access to information and services for election officials.

Providing Technical Assistance and Sharing Information

Knowing what to do when a security incident happens—whether physical or cyber—before it happens, is critical. CISA supports election officials with incident response planning including participating in exercises and reviewing incident response playbooks.

Crisis communications is a core component of these efforts, ensuring officials are able to communicate transparently and authoritatively when an incident unfolds.

In some cases, we do this directly with state and local jurisdictions. In others, we partner with outside organizations.

We recognize that securing our nation's systems is a shared responsibility, and we are leveraging partnerships to advance that mission. CISA actively promotes a range of services including:

Cyber hygiene service for Internet-facing systems: Through this automated, remote scan, CISA provides a report identifying vulnerabilities and mitigation recommendations to improve the cybersecurity of systems connected to the Internet, such as online voter registration systems, election night reporting systems, and other Internet-connected election management systems.

Risk and vulnerability assessments: We have prioritized state and local election systems upon request, and increased the availability of risk and vulnerability assessments. These in-depth, on-site evaluations include a

system-wide understanding of vulnerabilities, focused on both internal and external systems. We provide a full report of vulnerabilities and recommended mitigations following the testing.

Incident response assistance: We encourage election officials to report suspected malicious cyber activity to NCCIC. Upon request, the NCCIC can provide assistance in identifying and remediating a cyber incident. Information reported to the NCCIC is also critical to the Federal Government's ability to broadly assess malicious attempts to infiltrate election systems. This technical information will also be shared with other state officials so they have the ability to defend their own systems from similar malicious activity.

Information sharing: CISA maintains numerous platforms and services to share relevant information on cyber incidents. Election officials may also receive information directly from the NCCIC. The NCCIC also works with the EI-ISAC, allowing election officials to connect with the EI-ISAC or their State Chief Information Officer to rapidly receive information they can use to protect their systems.

Best practices, cyber threat information, and technical indicators, some of which had been previously classified, have been shared with election officials in thousands of state and local jurisdictions. In all cases, the information sharing and use of such cybersecurity threat indicators, or information related to cybersecurity risks and incidents complies with applicable lawful restrictions on its collection and use and with DHS policies protective of privacy and civil liberties.

Classified information sharing: To most effectively share information with all of our partners—not just those with security clearances—DHS works with the intelligence community to rapidly declassify relevant intelligence or provide as much intelligence as possible at the lowest classification level possible. While DHS prioritizes declassifying information to the extent possible, DHS also provides classified information to cleared stakeholders, as appropriate. DHS has been working with state chief election officials and additional election staff in each state to provide them with security clearances.

Field-based cybersecurity advisors and protective security advisors: CISA has more than 130 cybersecurity and protective security personnel available to provide actionable information and connect election officials to a range of tools and resources to improve the cybersecurity preparedness of election systems; and to secure the physical site security of voting machine storage and polling places. These advisors are also available to assist with planning and incident management for both cyber and physical incidents.

Physical and protective security tools, training, and resources: CISA provides guidance and tools to improve the security of polling sites and other physical election infrastructure. This guidance can be found at www.dhs.gov/hometown-security. This guidance helps to train administrative and volunteer staff on identifying and reporting suspicious activities, active shooter scenarios, and what to do if they suspect an improvised explosive device.

Election Security Efforts Leading up to the 2018 Midterms

In the weeks leading up to the 2018 midterm elections, DHS officials supported a high degree of preparedness nationwide. DHS provided free technical cybersecurity assistance, continuous information sharing, and expertise to election offices and campaigns.

EI-ISAC threat alerts were shared with all 50 states, over 1,400 local and territorial election offices, 6 election associations, and 12 election venders.

In August 2018, DHS hosted a "Tabletop the Vote" exercise, a three-day, first-of-its-kind exercise to assist our federal partners, state and local election officials, and private sector vendors in identifying best practices and areas for improvement in cyber incident planning, preparedness, identification, response, and recovery.

Through tabletop simulation of a realistic incident scenario, exercise participants discussed and explored potential impacts to voter confidence, voting operations, and the integrity of elections. Partners for this exercise included 44 states and the District of Columbia; EAC; Department of Defense, including the Office of the Secretary of Defense, U.S. Cyber Command, and the National Security Agency; DOJ; Federal Bureau of Investigation; Office of the Director of National Intelligence; and National Institute of Standards and Technology (NIST).

Through the "Last Mile Initiative," DHS worked closely with state and local governments to outline critical cybersecurity actions that should be implemented at the county level. For political campaigns, DHS disseminated a cybersecurity best practices checklist to help candidates and their teams better secure their devices and systems.

On Election Day, DHS deployed field staff across the country to maintain situational awareness and connect election officials to appropriate incident response professionals, if needed. In many cases, these field staff were co-located with election officials in their own security operations centers.

DHS also hosted the National Cybersecurity Situational Awareness Room, an online portal for state and local election officials and vendors that

facilitates rapid sharing of information. It gives election officials virtual access to the 24/7 operational watch floor of the CISA NCCIC. This setup allowed DHS to monitor potential threats across multiple states at once and respond in a rapid fashion.

Our goal has been for the American people to enter the voting booth with the confidence that their vote counts and is counted correctly. I am proud to say that our efforts over the past two years have resulted in the most secure election in modern history.

No Evidence of Election Interference

The Secretary of Homeland Security and the Acting Attorney General have concluded that there is no evidence to date that any identified activities of a foreign government or foreign agent had a material impact on the integrity or security of election infrastructure or political or campaign infrastructure used in the 2018 midterm elections for the United States Congress.

The activity we did see was consistent with what we shared in the weeks leading up to the election. Russia, and other foreign countries, including China and Iran, conducted influence activities and messaging campaigns targeted at the United States to promote their strategic interests.

Election Security Efforts Moving Forward

Ensuring the security of our electoral process remains a vital national interest and one of our highest priorities at DHS.

In the run up to the 2020 election season, DHS will continue to prioritize elections by broadening the reach and depth of information sharing and assistance that we are providing to state and local election officials, and continuing to share information on threats and mitigation tactics.

DHS goals for the 2020 election cycle include improving the efficiency and effectiveness of election audits, continued incentivizing the patching of election systems, and working with the National Institute of Standards and Technology (NIST) and the states to develop cybersecurity profiles utilizing the NIST Cybersecurity Framework for Improving Critical Infrastructure. We will also continue to engage any political entity that wants our help. DHS offers these entities the same tools and resources that we offer to state and local election officials, including trainings, cyber hygiene support, information sharing, and other resources.

DHS has made tremendous strides and has been committed to working collaboratively with those on the front lines of administering our elections to secure election infrastructure from risks.

Just last week, DHS officials provided updates to the secretaries of state, state election directors, and members of the GCC and SCC on the full package of election security resources that are available from the Federal government, along with a roadmap on how to improve coordination across these entities.

DHS also worked with our Intelligence Community partners to provide a classified one day read-in for these individuals regarding the current threats facing our election infrastructure.

We will remain transparent as well as agile in combating and securing our physical and cyber infrastructure.

However, we recognize that there is a significant technology deficit across SLTT governments, and state and local election systems, in particular.

It will take significant and continual investment to ensure that election systems across the nation are upgraded and secure, with vulnerable systems retired. These efforts require a whole of government approach. The President and this Administration are committed to addressing these risks.

Our voting infrastructure is diverse, subject to local control, and has many checks and balances.

As the threat environment evolves, DHS will continue to work with federal agencies, state and local partners, and private sector entities to enhance our understanding of the threat; and to make essential physical and cybersecurity tools and resources available to the public and private sectors to increase security and resiliency.

Thank you for the opportunity to appear before the Committee today, and I look forward to your questions.

Note

Christopher Krebs serves as the first director of the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA). Mr. Krebs was originally sworn in on June 15, 2018 as the Under Secretary for the predecessor of CISA, the National Protection and Programs Directorate (NPPD). Mr. Krebs was nominated for that position by President Trump in February 2018.

Before serving as CISA Director, Mr. Krebs was appointed in August 2017 as the Assistant Secretary for Infrastructure Protection. In the absence of a permanent NPPD Under Secretary at the time, Mr. Krebs took on the role

of serving as the Senior Official Performing the Duties of the Under Secretary for NPPD until he was subsequently nominated as the Under Secretary and confirmed by the Senate the following year.

Mr. Krebs joined DHS in March 2017, first serving as Senior Counselor to the Secretary, where he advised DHS leadership on a range of cybersecurity, critical infrastructure, and national resilience issues. Prior to coming to DHS, he was a member of Microsoft's U.S. Government Affairs team as the Director for Cybersecurity Policy, where he led Microsoft's U.S. policy work on cybersecurity and technology issues.

Before Microsoft, Mr. Krebs advised industry and Federal, State, and local government customers on a range of cybersecurity and risk management issues. This is his second tour working at DHS, previously serving as the Senior Advisor to the Assistant Secretary for Infrastructure Protection and playing a formative role in a number of national and international risk management programs.

As Director, Mr. Krebs oversees CISA's efforts to defend civilian networks, secure federal facilities, manage systemic risk to National critical functions, and work with stakeholders to raise the security baseline of the Nation's cyber and physical infrastructure.

Mr. Krebs holds a bachelor's degree in environmental sciences from the University of Virginia and a J.D. from the Antonin Scalia Law School at George Mason University.

ESMA to recognise the UK Central Securities Depository in the event of a no deal Brexit

The European Securities and Markets Authority (ESMA) has announced that, in the event of a no-deal Brexit, the Central Securities Depository (CSD) established in the United Kingdom (UK) – Euroclear UK and Ireland Limited – will be recognised as a third country CSD to provide its services in the European Union (EU).

ESMA has adopted this recognition decision in order to allow the UK CSD to serve Irish securities and to avoid any negative impact on the Irish securities market.

ESMA has previously communicated that its Board of Supervisors supports continued access to the UK CSD.

Having assessed the application and the information submitted by the UK CSD, and consulted the relevant authorities in accordance with the Central Securities Depositories Regulation (CSDR), ESMA considers that the conditions for recognition under Articles 25 of CSDR are met by the UK CSD in case of a no-deal Brexit.

Therefore, it has adopted a decision to recognise the UK CSD as a third-country CSD under the CSDR.

The recognition decision would take effect on the date following Brexit date, under a no-deal Brexit scenario.

Notes

1. On 19 December 2018, ESMA published a public statement stating that it was ready to review UK CCPs' and the UK CSD's recognition applications for a no-deal Brexit scenario if the four recognition conditions under Article 25 of EMIR and Article 25 of CSDR were met, respectively.

2. On 18 February 2019, ESMA published a press release stating that it would recognise three central counterparties (CCPs) established in the UK – LCH Limited, ICE Clear Europe Limited and LME Clear Limited –to provide their services in the EU in the event of a no-deal Brexit.

3. ESMA's mission is to enhance investor protection and promote stable and orderly financial markets.

It achieves these objectives through four activities:

i. assessing risks to investors, markets and financial stability;
ii. completing a single rulebook for EU financial markets;
iii. promoting supervisory convergence; and
iv. directly supervising specific financial entities.

4. ESMA achieves its mission within the European System of Financial Supervision (ESFS) through active cooperation with the European Banking Authority (EBA), the European Insurance and Occupational Pensions Authority (EIOPA), the European Systemic Risk Board, and with national authorities with competencies in securities markets (NCAs).

On the global Impact of risk-off shocks and policy-put frameworks

BIS Working Papers No 772, by Ricardo J. Caballero and Gunes Kamber, Monetary and Economic Department, March 2019

BANK FOR INTERNATIONAL SETTLEMENTS

Summary

Focus

Big sell-offs in financial markets ("risk-off shocks") can trigger severe recessions if fiscal and monetary policymakers fail to respond appropriately.

After the Great Financial Crisis (GFC), central banks in advanced economies resorted to unconventional monetary tools such as asset purchases.

These measures successfully propped up the economy, but they have also been criticised for encouraging investors to buy riskier assets ("reach-for-yield behaviour").

As such, they have been seen as a sort of free "put option" or insurance policy for investors.

Contribution

We look at how financial markets around the world have reacted to risk-off shocks, and how the authorities have responded.

First, we focus on how risk-off shocks have affected the financial markets of advanced economies, comparing their effects before and after the GFC.

We then study the knock-on effects ("spillovers") from these shocks to emerging market economies (EMEs).

We explore how these effects were influenced by the monetary policy of advanced economies, as well as the economic condition of EMEs.
We pay particular attention to how the response of EMEs to these shocks has changed since the GFC.

Findings

We find that the unconventional monetary policies of the main advanced economies were highly effective, at a time when already low interest rates

would have hindered central banks from attempting to boost the economy through further policy rate cuts.

Without these policies, financial markets would have been more vulnerable to global sell-offs.

Most of the policy discussion has focused on the problems arising from the strong capital flows into EMEs that these policies encouraged. But we document a positive side to these policies.

They increased the resilience of the rest of the world against global risk-off shocks.

For EMEs in particular, this took the form of smaller credit spreads and a reduced tendency for long-term interest rates to rise sharply following such shocks.

To read more:
https://www.bis.org/publ/work772.pdf

When expectations meet the future

Sir Jon Cunliffe, Deputy Governor for Financial Stability of the Bank of England, at the London School of Economics.

The subject of this symposium is "The Next Great Crisis" by which I think we mean financial crisis.

One of the defining characteristics of humans is our ability to imagine the future, as I shall discuss later.

But though we can imagine the future, we cannot know it.

And I am a cautious central banker.

So I will not today give you my prediction for the origin, shape and extent of the next great crisis.

I am however prepared to make one prediction with confidence.

Whatever the trigger and the financial services and instruments most affected, the next crisis will have, somewhere at its centre, losses from an overextension of credit and an adjustment in asset prices.

And, for me, as Deputy Governor at the Bank of England responsible for Financial Stability, an equally if not more important question is not what will the next great financial crisis look like but whether the next and subsequent financial crises will actually be 'great'.

Will the correction of asset prices and the losses on credit be amplified by the financial system and cause the economic and social loss we saw 10 years ago?

Or, losses notwithstanding, will the system absorb them without material dislocation to the economy?

I can make the prediction that the next 'crisis' will have somewhere at its centre the overextension of credit and asset price adjustment because it is not a particularly bold one.

Since its invention in the temple organisation of bronze age Mesopotamia, interest bearing debt – or credit if you want to see it from the other side of the coin – has had the property of being able to grow beyond the ability, or sometimes the willingness, of the economy to repay it.

Debt contracts are essentially claims on the future and the future, when it arrives, does not always honour them.

The origin of debt and credit are fascinating but unclear.

It may have been an evolution of the reciprocal gift giving social obligations of early tribal societies.

The etymological evidence suggests rather an evolution from the system of fines and compensation for injuries prevalent in such societies.

It has also been suggested that the foundation of debt is the belief that man is born with debt to the heavens and creation and debt between members of society is an extension of this idea.

In economic terms, the early debt systems and the debts themselves, painstakingly recorded in the ledger systems of the temples of bronze age Mesopotamia, appear to be primarily about what we would now call working capital and overdraft facilities in agrarian societies that produced little economic surplus – credit to tide farmers over until the harvest or through bad harvests with the debt repaid in standardised units of agricultural produce.

To read more:
https://www.bis.org/review/r190312d.pdf

Disclaimer

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

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

This information:

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

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

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

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

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

- is in no way constitutive of an interpretative document;

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

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

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

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

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

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

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

You may visit:
www.members-of-the-board-association.com/HowToBecomeMember.html

2. Monthly Updates - Subscribe to receive (at no cost) Basel II / Basel III related alerts, opportunities, updates and our monthly newsletter:

http://forms.aweber.com/form/77/609193677.htm

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

You must follow the steps described at:
www.members-of-the-board-association.com/Distance_Learning_and_Certification.htm

www.basel-iii-association.com/Basel_III_Distance_Learning_Online_Certification.html

For instructor-led training, you may contact us. We can tailor all programs to your needs.