COMMODITY FUTURES TRADING COMMISSION

TECHNOLOGY ADVISORY COMMITTEE MEETING

12:31 p.m. to 4:13 p.m. EST

Monday, January 8, 2024

Three Lafayette Centre

1155 21st Street Northwest

Washington, D.C. 20581

A P P E A R A N C E S

COMMISSIONERS

Commissioner Christy Goldsmith Romero

Commissioner Kristin N. Johnson

Commissioner Summer K. Mersinger

TECHNOLOGY ADVISORY COMMITTEE (TAC) MEMBERS

Carole House, Terranet Ventures Inc., TAC Chair

Ari Redbord, TRM Labs, TAC Vice Chair

Nikos Andrikogiannopoulos, Metrika

Dan Awrey, Cornell Law School

Christian Catalini, Lightspark

Todd Conklin, U.S. Department of the Treasury

Jonah Crane, Klaros Group

Sunil Cutinho, CME Group

Cantrell Dumas, Better Markets, Inc.

Timothy Gallagher, Nardello & Co.

Michael Greenwald, Amazon Web Services

Dan Guido, Trail of Bits

Jennifer Ilkiw, ICE Futures U.S.

Ben Milne, Brale

A P P E A R A N C E S (CONTINUED)

John Palmer, Cboe Global Markets, Inc.

Joe Saluzzi, Themis Trading LLC

Michael Shaulov, Fireblocks

E. Gün Sirer, Ava Labs

Justin Slaughter, Paradigm

Todd Smith, National Futures Association

Steve Suppan, Institute for Agriculture and Trade Policy

Corey Then, Circle

Nicol Turner Lee, Center for Technology Innovation, The Brookings Institution

Jeffery Zhang, University of Michigan Law School

COMMODITY FUTURES TRADING COMMISSION STAFF

Andrew Rodgers, Trial Attorney, Division of Enforcement, CFTC, Alternate Designated Federal Officer

Lauren Bennett, Trial Attorney, Division of Enforcement, CFTC, Alternate Designated Federal Officer

A G E N D A

A G E N D A (CONTINUED)

A G E N D A (CONTINUED)

P R O C E E D I N G S

(12:31 p.m.)

MR. RODGERS: Good morning. As the TAC Alternate Designated Federal Officer, it is my pleasure to call this meeting to order.

Before we begin this morning's discussion, I would like to turn to Commissioner Christy Goldsmith Romero, the TAC sponsor, for the welcome and opening remarks. Commissioners Johnson and Mersinger will then give brief opening remarks as well.

COMMISSIONER GOLDSMITH ROMERO: Thank you. I welcome the CFTC's Technology Advisory Committee.

Technology can be transformative for people and markets if designed and deployed responsibly, and debate on issues of emerging technology is enhanced by the Commission's engagement with a broad and diverse group of technology experts who serve on the TAC.

As the TAC sponsor, I'm grateful for your service and for the leadership of TAC Chair Carole House, Vice Chair Ari Redbord, and Chairs of the

TAC Subcommittees. I also want to thank Tony Biagioli, Drew Rodgers, Lauren Bennett, Scott Lee, Yevgeny Shrago, Zach Coplan, and others at the CFTC.

In every meeting, TAC has examined responsible artificial intelligence. AI has long been used in financial services and markets, and the latest buzz is over generative AI, which could be a consequential tool to aid humans in breakthroughs in areas of big problems like health care and climate change, cybersecurity, and fraud detection, just to name a few. The potential impact of generative AI on financial markets cannot be fully known, but that does not mean that regulators cannot start to consider guardrails to ensure that AI innovation is responsible.

As a foundational matter, regulators should consider how best to establish accountability on the humans and organizations designing and deploying AI in markets. Governance requirements on those making decisions to deploy AI in financial markets are important to consider and can protect

against someone blindly deploying a tool or model with an outcome that causes harm.

Accountability requires transparency, not a black box. Transparency in the design and initial deployment of AI systems or AI models is critical, as is the case after the AI system or model is deployed. It's important for humans to be able to detect possible negative outcomes in deployed AI models or systems before they cause harm.

Given the unique complexity of AI, it is important for regulators to consider implementing best practice standards. NIST leads with its AI risk management framework, a framework that allows for innovation that is responsible and is designed to ensure the trustworthiness of AI.

I would ask the TAC Subcommittee on Emerging and Evolving Technologies to consider, as part of its ongoing work, whether to recommend that the CFTC impose best practice standards for AI, such as NIST's risk management framework for regulated entities. TAC will continue to coordinate with the Biden Administration in examining responsible AI.

We are honored today to welcome Elizabeth Kelly, Special Assistant to the President for Economic Policy in the White House, to speak about the Executive Order on AI. President Biden is setting the U.S. on a path to lead the world in fostering the promises of AI while protecting against potential perils with the EO's focus on the safety, security, and trustworthiness of AI.

We will also hear today from Professor Michael Wellman, Chair of Computer Science and Engineering at the University of Michigan, who earned his Ph.D. in Artificial Intelligence from MIT in 1988 and has spent his career as an AI researcher. Professor Wellman testified before the Senate on the potential use of AI for market manipulation, even if not intended, and what he calls the AI loophole, which is potential gaps in regulations that are focused on humans having intent. Those who place AI into regulated financial services have responsibilities to follow existing laws. If there are gaps in our laws, it is appropriate to consider ways to close those gaps. Senators Mark Warner and

John Kennedy recently introduced a bipartisan bill that would amend the SEC's regulatory authority by ensuring accountability, addressing intent, and providing for treble damages. The CFTC might need comparable authority, and I would urge the Subcommittee on Emerging and Evolving Technologies to take up this issue as part of their ongoing work.

Turning to cyber resilience, I'm very pleased that the Commission proposed its first rule for banks and brokers on cyber resilience, the development of which I had the privilege of leading over the last year. The federal government must also promote its own cyber resilience, and today we welcome Mitch Herckis, Director for Federal Cybersecurity, Office of the Federal CIO, White House. His work focuses on a Zero Trust paradigm, which is no easy feat, but is necessary for cyber resilience. I look forward to hearing about his work, which is something that the TAC Subcommittee on Cybersecurity can consider as part of its work.

And last, but certainly not least, Carole

House and Dan Awrey, co-chairs of the Subcommittee on Digital Assets and Blockchain Technology will present the Subcommittee's draft report on Decentralized Finance.

From the time that I have arrived at the CFTC I've talked about the importance of promoting innovation that is responsible and studying emerging issues around digital assets to prevent harmful unintended consequences, particularly to retail customers, market integrity, and financial stability, and this report is the result of one such study.

DeFi is more than $50 billion in total locked value. That's a lot of customer assets. I'm grateful for Carole's and Dan's leadership and for the Subcommittee members' work to study the promises of DeFi while being realistic about what it is today, as well as the risks the Subcommittee sought to present a balanced and straightforward examination of DeFi. The composition of the Subcommittee, with its broad and diverse views, helps bring that balance.

I hope this report will be used by policymakers and regulators as they consider DeFi going forward, and also by the industry itself. I'm grateful for the hard work that the Subcommittee made to develop findings and recommendations. Given that DeFi remains at the center of cyber hacks and illicit finance, I am particularly grateful for the recommended action related to anti money laundering and countering the financing of terrorism.

Today, TAC members will vote on releasing the report.

I really appreciate each of our speakers and the TAC members' willingness to share your technology expertise and viewpoints. As always, I encourage a broad discussion and a diversity of views today and going forward. Thank you.

MR. RODGERS: Thank you, Commissioner Goldsmith Romero. We will now have opening remarks from Commissioner Johnson.

COMMISSIONER JOHNSON: Thank you. Good morning. Thanks so much to Commissioner Goldsmith

Romero, her staff, and ADFOs for TAC, and the Technology Advisory Committee members for joining us for this first meeting of 2024.

Today is a special day, if you'll allow me.

(Opens her jacket to show her University of Michigan T-shirt.)

COMMISSIONER JOHNSON: Last year, around this time, I delivered a keynote address at the inaugural Digital Assets at Duke Conference, that's Duke University. For the first 3 minutes, I punctuated every sentence with two words, "Go Blue." In my limited time, I will not repeat "Go Blue" as often as I did during that speech, but I will share the following.

Later tonight, a team of exceptional athletes, who are part of a unique legacy, will take the field wearing maize and blue uniforms and a distinctive winged helmet. It was nearly 150 years ago, 1879, when the Michigan Wolverines began competing in intercollegiate football. Over their storied history, Michigan has won, has the most all time wins in college football -- 1,004, if all goes

well tonight.

We can learn a great deal from the incomparable, indefatigable, unstoppable athletes who comprise the Michigan football team. There are lessons about hard work, dedication, touchdowns, interceptions, and playing through the heat of the summer conditioning camps to the bitter cold and snow that can fall in the Big House by the end of the regular season, we can learn to tackle difficult problems and hopefully, like the Michigan football team later tonight, we can declare ourselves victors.

So today, I'd like to take some of that learning as TAC tackles two of the most difficult issues facing governments and financial markets around the world. We need to shore up our cyber defenses and questions that accompany the integration of artificial intelligence in our society.

Allow me to share a quick thought about each of these. I'll start with cyber resilience because of the Commission's pending rule in this space.

Increasingly, cyberattacks threaten the most critical infrastructure resources in our nation, from electrical grids to energy pipelines to servers that enable air traffic control or Internet resources that facilitate significant financial transfers. Governments and businesses rank cyber threats among the most critical operational risks and cybersecurity and cyber resilience as key to preventing or mitigating disruption of critical government and financial services.

Consequently, cyber resilience is top of mind for me, and many of us here at the Commission. I'm grateful that it's part of your agenda for today. For over a decade, I've presented as an expert and published on these issues and was happy to support the Operational Resilience Proposed Rulemaking that the Commission undertook last month. It frames cybersecurity as a critical component of resiliency for our market participants.

The systemic nature of this problem, as well as the increasing centrality of technology in our markets and economy, is such that it is incumbent

upon us to explore multiple approaches. Some may focus on governance, others on regulatory policy, while others consider and identify vulnerabilities in software and hardware.

Our recently proposed cyber rule addresses a number of these concerns.

I supported the Operational Resilience Proposed Rulemaking the Commission adopted last month, which frames, in addition to these issues, third party service provider relationships and business continuity and disaster recovery programs as critical components. The proposal is exceptionally well done, and I applaud the staff for their years of work ahead of the rulemaking to move the NPRM forward. I applaud the Chair for his leadership in advancing the rule and my fellow Commissioners Goldsmith Romero, Mersinger, and Pham, for supporting the rule.

However, the proposed rule is piecemeal in its efforts to establish standards across the Commission's registered entities. It focuses on a narrow segment of our markets, futures commission

merchants, swap dealers, and major swap participants, as overseen by our market participants division.

While the Commission is drawing on its experience establishing safeguard requirements for registered entities. It does not address gaps in the regulation that are rather important to our market infrastructure. Namely, as I mentioned during the recent open meeting, it's critical that we consider the application of a parallel set of regulations in the context of DCOs.

As I noted in my statement supporting the proposed rule, these registered entities are similarly serviced by critical third-party service providers and similarly the targets of cyberattacks, and also present equally concerning issues regarding disruption by unforeseen disasters. Each market infrastructure is subject to its own set of core principles on system safeguards, business continuity programs, and outsourcing programs under Parts 37, 39 and 49 of the CFR, which may be similar but different in

various respects.

I note that it is important that we think carefully about DCOs, in particular as we reflect on events around this time last year related to a third-party service provider attack.

In February of 2023, ION Group experienced a cyberattack that impacted trading and clearing of exchange traded derivatives by ION customers globally. The cyber incident had an outsized impact on our markets and affected a wide range of our registered entities and market functions such as trading, processing and clearing. As the ION incident demonstrates, cyber incidents have systemic risk implications.

I'll say finally and quite quickly a few words about artificial intelligence, likely echoing what Commissioner Goldsmith Romero mentioned, so I'll keep it rather quick. We all know that AI presents a rather critical set of questions for our markets. Over the last few years, I've had the pleasure of supporting the Administrative Conference of the United States, ACUS, in a series of projects

focused on AI.

Chair Benham encouraged me to serve among other principals as the CFTC's member for ACUS. ACUS' work on AI is leading the regulatory discussion globally regarding standards related to the adoption and integration of AI. I'm very excited to be part of that body of federal regulators engaged in thinking carefully about the application, in particular of Supervisory Technology, or SupTech, in our markets.

Specifically, the CFTC has on staff surveillance analysts, forensic economists and futures trading investigators, each of whom investigate and identify potential violations. Increasingly, we rely on cloud-based architecture and forms of artificial technology in the context of our surveillance. It's important that our Office of Technology Innovation and across the Commission, we are keeping pace with changes in technology.

With more time, I would share some reflections on an issue that I'm certain one of your members,

Nicol Turner Lee, is deeply thoughtful about, and that is bias.

As we think carefully about AI and the integration of AI in our financial markets, infrastructure and regulation, it's critical that we think about the potential for bias and discrimination and underlying data to be amplified through the use of generative AI.

I'm very much looking forward over the course of today's meetings to hear from Mitch Herckis, as well as Elizabeth Kelly, and very importantly, a super guest of honor today from the University of Michigan, Michael Wellman.

I thank you so much for your time allowing me to join the meeting. I apologize that I might sneak out. I have a little one who is sick upstairs in my office, so I have to make my way to the pediatrician, but I will join you all online for the continuing of the meeting. Thanks so much.

MR. RODGERS: Thank you, Commissioner Johnson, and good luck tonight to your Wolverines.

Commissioner Mersinger.

COMMISSIONER MERSINGER: Good afternoon, and I apologize that I'm not there in person today, but it looks like you have a great agenda before you, so I'll keep my remarks short.

Thanks to Commissioner Goldsmith Romero for calling this meeting, and thanks to all the members of the Technology Advisory Committee and the Subcommittees, presenters, and all the CFTC staff responsible for today's meeting. I know it takes a lot of effort to put these meetings together and I greatly appreciate everyone's work in doing so.

Considering the CFTC's vast data resources, advancements in cybersecurity, and artificial intelligence will continue to shape the means of accomplishing the agency's mission, these developments will also have important impacts on our registrants and registered entities. With the rapid progression of technology, the role of decentralized finance, and its alignment with an existing regulatory landscape, we'll have to carefully consider all that's involved.

I'm looking forward to today's discussion on

these critical topics and developments. And with that, again, I just wanted to say thank you to everyone and I'm definitely looking forward to today's discussion.

MR. RODGERS: Thank you Commissioner Mersinger, and thank you all for your opening remarks.

Before beginning our first segment, there are just a few logistical items that I've been asked to mention to the committee members. Please make sure your microphone is on when you speak. This meeting is being simultaneously webcast and it is important that your microphone is on, so that the webcast audience can hear you. If you would like to be recognized during this discussion, please change the position of your place card in front of you so that it is vertical on the table, and raise your hand and we will recognize you and give you the floor.

If you are participating virtually and would like to be recognized during the discussion for a question or comment or need technical assistance,

please message me within the Zoom chat. I will alert the TAC Chair, Carole House, that you would like to speak during the discussion period that follows the prepared remarks and presentation.

Please identify yourself before beginning to speak and signal when you are done speaking. Please speak directly into your phone or microphone for optimal audio quality on the webcast, and please unmute your Zoom video before you speak and mute both your video and your microphone after you speak. Please only turn your camera on when you are engaging in discussion.

If you are disconnected from Zoom, please close your browser and enter Zoom again using the link previously provided for today's meeting.

Before we begin, we'd like to do a roll call of members participating virtually so we have your attendance on the record. After I say your name, please indicate that you are present and then mute your line.

So, starting with Nikos Andrikogiannopoulos.

MR. ANDRIKOGIANNOPOULOS: Present.

MR. RODGERS: Christian Catalini.
MR. CATALINI: Present.
MR. RODGERS: Todd Conklin.
MR. CONKLIN: Present.
MR. RODGERS: Sunil Cutinho.
MR. CUTINHO: Present.
MR. RODGERS: Jill Gunter.
(No response.)
MR. RODGERS: Jennifer Ilkiw.
MS. ILKIW: Present.
MR. RODGERS: Ben Milne.
MR. MILNE: Present.
MR. RODGERS: John Palmer.
MR. PALMER: Present.
MR. RODGERS: Michael Shaulov.
MR. SHAULOV: Present.
MR. RODGERS: Steve Suppan.
MR. SUPPAN: Present.
MR. RODGERS: Adam Zarazinski.
(No response.)
MR. RODGERS: Dan Guido.
MR. GUIDO: Present.

MR. RODGERS: And Gün Sirer.

MR. SIRER: Present.

MR. RODGERS: With that, I'll turn things over to TAC Chair, Carole House.

CHAIR HOUSE: Andrew, thank you so much. I appreciate you and the CFTC team. I'm thrilled to be back here with all of you, this amazing committee, and to see two guest speakers who are former White House colleagues. I'm really excited to hear from them.

So, since our last convening, a lot has happened in the space of emerging technology policy development, implementation, and risks that we've seen. We've seen the White House continue to build on years of work focused on artificial intelligence, and now we've seen the culmination of it in the issuance of a comprehensive Executive Order focused on ensuring responsible developments in AI. Future digital economies will rely on the use of AI, and it will generate many higher order technological and economic commercial developments.

I'm excited to hear from the White House

shortly on its vision, as well as an expert on AI and finance, as well as really excited for the Subcommittee's work on emerging technology. Examining the complex issues that are present related to AI in the financial sector.

The Executive Order prioritizes efforts on transparency, content, authenticity and cybersecurity and privacy. These issues are all especially important in driving competitive and democratic uses of AI, and all of which also have significant implications for regulated activities in finance, as well as regulators who are seeking to leverage AI and ensure against its exploitation of consumers and markets.

The issues, especially of transparency and explainability, are key and fundamental to accountability, issues that we've heard the Commissioners, and especially Commissioner Goldsmith Romero, highlight as a key issue in her convening of the Technology Advisory Committee and giving us direction on areas that would be of special use to the Commission. And all these

issues of accountability are critical to all emerging technologies, not just to AI. It includes digital assets in cybersecurity.

We've seen continued cyberattacks, including data breaches and ransomware, targeting major financial institutions, managed service providers and IT services, healthcare, retail, municipalities, including libraries, water systems and transit systems. It's clear that the work of the TAC Subcommittee on Cybersecurity remains critical, and also why the Commission is pursuing operational resilience and cybersecurity requirements for its regulated institutions.

So, I'm for one, thrilled to hear from the White House and the ongoing efforts underway to drive IT modernization and cybersecurity across the federal government, which may hold some really interesting lessons for the TAC here to consider as we examine best practices and recommendations for the Commission and policymakers.

Finally, in crypto, since our last meeting, we've seen some of the largest enforcement actions

and penalties in corporate history. We've also seen lots of legislation requested, introduced and debated, as well as historic uses of authorities aimed at combating digital asset activity of primary money laundering concern, issues of digital assets remain critical to address.

Today marks the culmination of many months of work for the Subcommittee on Digital Assets and Blockchain Technology, where we will discuss a landmark, comprehensive report that we've drafted altogether by the Subcommittee on a recommended approach to decentralized finance.

So all of these issues, whether focused on driving investment in innovative technologies, safeguarding our financial system from exploitation by bad actors, or defending against threats targeting our critical infrastructure, point to initiatives that require cross public and private sector collaboration. Neither side can do it on their own. The government cannot subsidize or enforce these sectors into compliance on their own, or drive responsible development on its own, and

industry forces need direction and guardrails to ensure the technological advancement is not unchecked without regard for the needs and rights of citizens and societies.

We've seen in both AI and DeFi, various stakeholders at different times call for pauses of development of these technologies and deployment of the tech. While the intent of these sentiments, I think is very well placed, the feasibility of them, I feel is questionable. And I do feel that it begs the question of how much more impactful might, instead of asking for a pause, but instead for a surge and sprint on development of the responsible technology building blocks and reg tech to help ensure accountability of these emerging techs might be in fact more impactful in driving our policy objectives.

So, partnerships with responsible actors across academia, industry, and governments across the international, federal and state local stages are necessary. Today here at the TAC, we will continue in pursuit of that vision of partnership

with great thanks again to the Commission, to Commissioners Johnson and Mersinger for joining us, and to Commissioner Goldsmith Romero for her leadership in convening us.

So now, it is my pleasure to introduce our first speaker regarding artificial intelligence, Elizabeth Kelly, Special Assistant to the President for Economic Policy at the White House, at National Economic Council, who will speak regarding the White House's Executive Order on the safe, secure, and trustworthy development and use of artificial intelligence.

MS. KELLY: Great. Thank you, Carole. It's a delight to be here today and to see so many friends both in the room and on Zoom. I'm here today to discuss the President's Executive Order on artificial intelligence, how we got here, and what's ahead.

So, I think it's fair to say that 2023 was the year of AI. You only have to look at stock market returns. Generative AI burst into the public awareness thanks to an astonishingly rapid advance

in its ability to create text, images, audio and video, and a consumer AI app, we all know which one was the fastest growing app of all time, gaining 100 million users in just two months.

Now, financial services companies have been using other classes of AI for many years, including to inform activities like lending and fraud detection. And, indeed, generative AI is just one example of a broad category of AI technologies. For example, machine learning, which has been common in industry for a long time, uses computational systems trained to make statistical predictions of many sorts.

We know that AI technologies, including generative AI, are poised to have enormous impact across the economy, including in financial services and everything we've seen thus far is really just the beginning. The President has said many times that AI carries enormous potential benefits as well as enormous risks, and it's vital that we mitigate the latter while working to capture the former.

I just want to spend a couple of minutes on

some of the benefits that AI could offer as we think about how to address critical challenges of our era.

It can aid drug discovery, letting us design new cures for intractable diseases in quicker time. It could help us address climate change and environmental risks, such as by predicting weather patterns or disaster events, devising new methods for carbon capture and storage, optimizing data center cooling, helping lower emissions from air travel, and improving microclimate forecasting in ways that can better enable renewable energy.

And it's already doing so much to make our lives easier, safer, and more convenient. It's helping speed up application processing or underwriting loan applicants once considered unviable. It's helping make cars safer. Hospital staff are using AI to extract data from patient’s medical records populated elsewhere, saving clinicians time, helping improve communications, and reducing clinician burnout.

And we all know from our personal lives that

it's behind countless online experiences that we enjoy every day, and perhaps some we enjoy a little bit less.

Of course, this is only one side of the story. AI also carries huge risks. It's exacerbating existing risks, such as threats to discrimination and threats to individual privacy. Even when AI enables faster underwriting, it can embed discrimination in lending decisions without appropriate mitigations. It can both make cars safer but also lull drivers into dangerous complacency. And even as it makes our online lives easier, it enables companies to collect even more data about us and to use that data for a wide range of purposes, oftentimes without our consent and against our interests.

And AI introduces novel risks altogether, such as some of its risks to National Security, to elections of democratic functioning, and to civil and human rights. Just as AI can aid drug discovery, it can also help design biothreats that are worse than those occurring in the natural world

and enable surveillance that violates privacy or that even undermines human rights, while empowering malign actors to threaten the integrity of critical sources of information.

As I've said, what we've seen today is just the beginning, and that's why the administration is working, and has been working decisively to mitigate AI's risks, even as we work to capture its extraordinary potential benefits. As Carole said, this has been an ongoing process, and the EO is just a continuation of all the work that has come before.

The administration's first step was articulating the principles and overarching standards that should guide responsible AI development and use. We started with the AI Bill of Rights, which articulates bedrock principles for ensuring that AI systems are safe, effective and transparent, and prioritize civil rights, equity and privacy protections.

A few months later, the National Institute of Standard Technology published the AI Risk

Management Framework to guide AI developers and deployers in evaluating and managing AI's risks. Building on these shared principles, the Biden Administration then worked to ensure that developers of frontier models are putting in place essential guardrails.

This summer, the White House received voluntary commitments from 15 leading developers, including Anthropic, Google, Meta, Microsoft, and OpenAI, to promote the safe, transparent, and secure development of AI technology. These commitments include rigorous and transparent testing and assessment of product safety, safeguards to ensure that systems are secure against cyber and other National Security threats, and new mechanisms to promote trust and reduce social harms, including labeling content altered or generated by AI, preventing bias and discrimination, and shielding children from harm.

Building on all of these steps, we were proud this October to issue a landmark Executive Order to ensure that America leads the way towards

responsible AI innovation. Leading with substance is the phrase we're fond of using. The order follows the President's directive to use every lever at the government's disposal to manage AI's risks and harness its benefits.

Now, I won't go through all of the Executive Order. For those of you who've seen, it's admittedly lengthy, I think 88 pages, if you put it on legal paper. But I want to give you some of the highlights.

In keeping with the work that we've done before, the EO is structured around eight fundamental principles. These principles are protect safety and security, promote innovation and competition, protect workers, ensure equity and civil rights, protect privacy, protect consumers, improve the government's use of AI, and advance U.S. global leadership on AI.

Let's start with safety and security. Here, the EO directs sweeping action to protect Americans. It directs the Department of Commerce to develop guidelines and standards for testing the

safety of AI models. And it requires developers of the most powerful AI models, those not presently at market. You could think of like a GPT-5, to share their safety test results and other critical information with the US government.

It also directs further measures to address AI's most dangerous risks, including its ability to help design dangerous biological materials and its threats to critical infrastructure and information integrity. It also directs guidance for clearly labeling and watermarking AI-generated content, and actually requires the federal government to lead by example in adopting these practices for its own content.

The second principle is around promoting innovation and competition. Now, America already leads the world in innovation, and nowhere is that more true than in AI, and the Executive Order seeks to maintain this lead and to ensure robust, competitive ecosystem. For example, the EO directs the National Science Foundation to launch $140,000,000 pilot of the National AI Research

Resource, or NAIRR. The NAIRR will provide federally supported computing power, data, and other resources to AI researchers, catalyzing innovation and promoting competition by democratizing access to these scarce resources, which are so important for LLM development.

And we've called on Congress to allocate more money to enable the NAIRR to be fully scaled, as opposed to the pilot we're starting in the EO.

The EO also takes a number of other steps to try and promote a more robust and competitive ecosystem where smaller players, academics, entrepreneurs, are able to compete. It includes grants and technical assistance to support startups and small businesses, commercializing AI breakthroughs, and assistance to small businesses that are seeking to deploy AI technologies. It directs Department of Commerce to help small businesses and startups access semiconductors and it encourages the Federal Trade Commission to exercise its authorities to promote competition and requires every federal agency to consider

competition in both procurement and regulation of AI. This is a continuation of the directive in the President's competition Executive Order, encouraging all agencies to consider competition and its regulation more broadly.

And we actually go a step further in guidance issued by the Office of Management and Budget, which directs each agency and its procurement of AI to consider whether or not the potential awardee is blocking competition through self-preferencing or lack of interoperability or other things that are not good for the ecosystem.

The last piece I'll touch on in this section is that the EO includes measures to make sure that we have the workforce to continue to lead on AI. In addition to greater government support for technical AI training, it directs the modernization and streamlining of visa criteria, interviews, and reviews so that we can expand the number of highly skilled immigrants and non-immigrants with expertise in critical areas to study, stay, and work in the United States.

The third principle is protecting workers. President Biden is fond of saying that he is the most pro-union, pro-worker president in American history. So it's no surprise that the EO directs a range of actions to address risks involving job disruption or displacement from AI, as well as recognizing and taking steps to address AI's effects on job quality, including worker health, safety, privacy, civil rights, and freedom to organize.

One of the most significant actions is a direction of the Department of Labor to develop principles and best practices for employers to mitigate AI's harms and maximize AI's benefits for workers, including by making sure that workers have a voice in how AI is deployed in the workplace. This could include things like labor standards, data collection, workplace equity and health, freedom to organize risk of job disruption. This process is ongoing, so I encourage all of you to participate.

But I'd note, that we're making sure there's

teeth attached to these best practices, through a directive by the Executive Order for each federal agency to look at its grants and see how it can attach these conditions to AI-related grants.

The Executive Order also takes steps to advance civil rights. This is a core principle in the AI blueprint. And a couple of things that I would call out: one, making sure the Department of Justice is developing best practices and recommendations regarding AI safe, responsible, and equitable use across the justice system and requiring agencies to pursue a range of actions to ensure AI's equitable deployment and public benefits administration and throughout various sectors of the economy.

For example, the Department of Housing and Urban Development will be issuing guidance on the implications of certain uses of AI under the Fair Housing Act, including marketing. And the Department of Labor will be issuing guidance for federal contractors on the nondiscriminatory use of AI in hiring. We know that sorting of resumes,

prioritizing of applicants is somewhere where AI has often been prioritized, oftentimes with discriminatory effects, which is why we think this guidance is so important.

The fifth principle, for those of you counting at home, is protecting privacy. AI exacerbates the already serious risk that exists to Americans' privacy in two ways. One, it makes it easier to extract, re-identify, infer, and link together data about people in a way that is more damaging to privacy. And two, it heightens the incentives for collecting data, given its reliance on data for trading models.

I think it's noteworthy that in his rollout of the Executive Order, the President reiterated his call for Congress to pass bipartisan privacy legislation. And last fall, the CFPB and FTC took meaningful action to use the full extent of their authorities to protect Americans' privacy.

The EO builds on this work by mandating evaluation of how agencies collect and use commercially available information from data

brokers, and it directs stronger federal privacy guidance. It also prioritizes federal support for privacy preserving techniques and privacy enhancing technologies.

The sixth principle the EO is focused on protecting consumers. This is touching every area of our lives, and hence consumers in many different ways. A couple of things to emphasize are, one, as we think about healthcare, we know this is an area where AI has, to use the phrase, both tremendous promise and potential, but we think it's incredibly important the Department of Health and Human Services, as directed by the EO, take steps to ensure that AI deployed in healthcare environments are safe, secure, and trustworthy, requiring pre-deployment testing and evaluation, as well as creating a safety center so that issues that do arise post-deployment are quickly reported and addressed.

The Department of Education will also be taking steps to ensure safe, responsible, and nondiscriminatory deployment of AI in classrooms

and schools. Again, this is an area we can see huge benefits, personalized learning for students, enabling a better classroom experience.

It comes with potential downsides, too.

I also want to touch on what the EO says about government's own use of AI. We know that AI can help government deliver better results for the American people. It can expand agencies' capacity to regulate, govern, and disperse benefits and cut costs and enhance the security of government systems. Indeed, on AI.gov you can find a spreadsheet with 700 different uses of how the federal government is presently using AI, and we think there's even more that AI can be deployed to do to better serve the American people.

That's why the AI Executive Order and the accompanying M-memo issued by the Office of Management and Budget are really making sure that the U.S. government leads by example. It starts a whole of government talent surge to make sure that we're using accepted hiring authorities: the Presidential Innovation Fellows Program, USDS and

other levers, to get more AI talent into government, and that we're upskilling our existing employees by providing training for employees of all levels.

It also takes steps to reduce barriers to the responsible use of AI. For example, trying to address barriers related to IT infrastructure, inadequate data and sharing of data, cybersecurity procurement process all the things that we know can slow how government works. We want agencies to be able to acquire specified AI products and services faster, more cheaply, and more efficiently through more rapid and efficient contracting.

But I think it's worth noting that the OMB M-memo makes the differentiation between those use cases that are not rights and safety impacting, for example, autocorrect, when we each all text and government uses that could impact rights and safety. These are things like, related to the functioning of critical infrastructure like dams or electrical grids, emissions of hazardous materials. On the right side, if we're thinking about uses

related to law enforcement, employment, government benefits.

In each of these higher risk contexts, the government takes steps to place additional guardrails. So, for example, before an agency was able to use AI in a government benefits decision, for example, it would need to have AI impact assessments, real world testing, independent evaluations with ongoing monitoring, public notification and consultation, and assessments, and mitigation around disparate impact and ensuring we're using representative data.

We're really trying to lead by example in the government's use of AI and hope that the federal government will encourage other actors to follow suit.

Two more things that I'd highlight as we think about the federal government's own use of AI. One I talked about, which is our commitment to promoting competition in our procurement of AI technology, which I think is really remarkable language that speaks to this President's continued

commitment to competition.

The second is the commitment that we make to consulting with federal employees and unions when AI is deployed in the workplace, something we hope all employers will do. The goal is to focus resources and attentions on concrete harms without imposing undue barriers to AI innovation.

The last principle is to advance U.S. global leadership on AI. Now, we've obviously been actively engaged in a number of fora; the UN, the G-7, engagement with Europe, everything else, but I think, in general, we've seen a remarkable amount of global alignment as shown by the fact that in one week we had the UK Safety Summit, the rollout of the U.S. Executive Order and OMB Memo, and the issuance of the G-7 Principles for Responsible AI and Code of Conduct, that they hoped other countries, other companies would follow.

If you look at those principles and code of conduct, you'll see a lot of similarities with the voluntary commitments that we received from companies last July, really speaking to the U.S.

leadership role on AI governance and our continued commitment to leading with substance.

I just want to close by talking briefly about AI's use in the financial services sector and what's ahead. We've talked about how AI can have significant impacts on how lenders allocate credit and the risks of bias and discrimination in lending. It's part of why the Executive Order directs HUD to release guidance for housing lenders on avoiding unlawful discrimination in the use of AI to advertise housing loans.

But on the other hand, we're seeing some promising use cases where AI can help mitigate the risk of discrimination and bias and offer ways to remove them from decision-making. For example, the Federal Housing Finance Agency is encouraging its regulated entities to use AI to underwrite its models for bias and disparities and then explore automated processes as ways to mitigate them.

A second area to consider is fraud. Now, AI has long been used for fraud detection in financial services, helping banks compliance teams detect

patterns in vast data sets that lead to fraudulent transactions or illicit financial activities, and recent advances in generative AI are enabling banks to improve how they communicate with customers to combat fraud.

At the same time, we know that AI heightens the risks of fraud, creating new risks for the integrity of information and increasing malign actors' ability to impersonate customers' voices, steal information or break into their accounts. Scammers are now using voice cloning to impersonate relatives to try and convince someone to send money or get around voice verification systems and gain access to accounts. No longer is your voice your password if it can be cloned by an AI system.

It's part of why the EO directs Commerce to develop guidance for clearly labeling and watermarking AI-generated content, and why we're working as an administration to help develop promising technical solutions to detect AI-generated content and in the case of voice cloning scams, terminate a phone call early or actually

warn the receiver while the call is in progress.

As in every other industry, we're seeing AI be used for financial services firms' back office and compliance functions, automating all sorts of manual tasks, data management, production of compliance documents, you name it. As someone who once ran a compliance program for a FinTech startup, I can imagine the efficiencies and benefits from that. At the same time, there's certainly privacy risks. We want to make sure that if it's being used for chat bots, you're not giving inaccurate information to a customer they might rely on.

And interestingly, we found it can even have job satisfaction impacts. One company deployed AI to handle the more sort of basic customer requests and found that its call center representatives actually had decreased happiness with their jobs and left their jobs sooner because they were stuck dealing with the naughtiest and thorniest issues without any of the positive feedback from being able to resolve simpler customer issues.

The last thing I'll touch on is around financial stability, and this is something where Commissioner Goldsmith Romero, Chair Gensler, Director Chopra have all spoken extensively. We know that algorithmic trading is one trend that risks introducing greater volatility into financial markets. But in addition, AI introduces risk to financial institutions' core infrastructure and capacity to operate by exacerbating cybersecurity risks. We also know that deep fakes could be used for market manipulation.

In May, we saw stocks wobble briefly after a fake image of a purported explosion near the Pentagon went viral, before officials very quickly clarified that the photo was a fake. This speaks to the importance of really advanced contact authentication and broader adoption of such tools.

I hope my comments have given you a bit of a sense of how the Biden-Harris Administration is approaching AI and what we aim to do with the Executive Order. For those of you looking for some bedtime reading, there's another 88 pages of

waiting if you'd want more detail.

But for now, I'll conclude it and turn it over to all the other esteemed speakers. And thank you so much for your time today.

(Applause.)

CHAIR HOUSE: Thank you so much, Elizabeth. At this time, I would like to open the floor to questions and comments from TAC members. Go ahead, Nicol. Thank you.

MS. TURNER LEE: Well, thank you so much, Elizabeth, for that presentation. We're very excited about what the Biden Harris White House has done in this area and I love the analogy used today in terms of building blocks because they all seem to complement one another.

One question I have, and I'm thinking about Congress's activities prior to recess, has been really this wave of legislation that is either running in parallel or in different areas than what the White House is doing, I think we're seeing more sectoral regulatory guidance from Congress.

So I have two questions. One, I'm curious of

the role of Congress in sort of solidifying the legacy of the activities that the White House has initiated and where you see that going.

And then, two, the other question I have is consumer agency. So, as the building blocks have evolved, there's been a lot of focus on technical cadence and I'm just curious how we'll sort of solidify some of these priorities among everyday people, like my mother, who will be curious to know where she fits into the ecosystem.

So just, again, the second question is more so what is the White House thinking about in terms of giving people more agency around how they decide to participate in an AI-driven world? And will we see the White House sort of think through in this next wave, more disclosures in the same way that we at the TAC are thinking about how do we raise awareness among the people who are getting their hands dirty in this stuff versus the larger structures that are mitigating those risks? Thank you.

MS. KELLY: So, on the first question, this is

an Executive Order. We were using the full extent of the authority that the President has, but there's certainly a lot that will be left to independent agencies, which the President would not direct, and a lot that will be left to Congress because it's not possible to reach through regulation.

For example, we need comprehensive privacy legislation, as the President called for. If you were to create a licensing regime, require certain disclosures, any number of those things would require legislation and that's why we're so excited by the progress that we're seeing on the Hill, the enthusiasm around the insight forums that Leader Schumer has hosted and hope to continue to see that drumbeat.

On your question about sort of how do we encourage more consumer agency? I think a lot of this is making sure that consumers know what they're interacting with. So, I think, the watermarking of content is another key thing. You're seeing actions from the FTC and others to

inform consumers when they're working with AI.

We're hoping to increase AI literacy, both through education programs with Department of Ed, NSF. And I also think that a lot of the responsibility will fall on the companies who were building on the Anthropic, OpenAI, other LLMs, and make sure that they are being honest with their customers when AI is deployed and not deployed. So a lot more to come, but I appreciate the question.

CHAIR HOUSE: Thank you for those insights on how the EO's initiatives will be affecting the general public. Michael?

MR. GREENWALD: Thank you. Carole.

Elizabeth, thank you so much for the presentation.

Each agency will have a Chief Artificial Intelligence Officer. How do you see best practices between each of these new Chief Artificial Intelligence Officers working together to collaborate on what's working, what's not? And then, how do you think the EO will incentivize outside talent to come into these agencies, rather

than drawing from within, but also getting outside talent in bringing that competitive spirit that the EO really calls for?

MS. KELLY: So on the first question, the EO sets up a number of mechanisms to ensure that we have continued coordination and sharing of best practices. One is the regular convening of an AI Council, which the White House Chief of Staff's Office is actually convening and each Cabinet Secretary is participating in, which speaks to the priority that we're putting on this.

In addition, for the Chief AI officers, they likewise have a regular convening led by OMB and OSTP to make sure that they are sharing all of the best practices and we're not getting stuck in government silos.

Remind me of your other question.

MR. GREENWALD: Incentivizing outside of government talent, because I'm assuming some of the new Chief Artificial Intelligence Officers will come from within, but how do you get incentivized new talent coming in also?

MS. KELLY: So there's a whole push within the Executive Order and the OMB Memo to really have a talent surge and bring government to a higher level. I think that there are a couple different ways that we're doing this. One is through leveraging accepted hiring authorities, USDS, PIF programs that create a community of scientists, computer engineers, all those types of folks.

And in addition, we've actually been very pleasantly surprised by the huge number of applications that we've received through AI.gov. I think people recognize the U.S. is leading on this topic and that by coming into government, they have an opportunity to set the standards. They're going to govern this technology for many years.

CHAIR HOUSE: Thank you so much. Really great insights and interesting considerations for regulators that are considering their own capability and capacity enhancement. So thank you for that question, Michael, and your response, Elizabeth.

Commissioner Goldsmith Romero, I believe you

have a question.

COMMISSIONER GOLDSMITH ROMERO: Yeah, so first of all, thank you so much. Elizabeth is looking at me going, you're going to put me on the hot seat with a question.

So first, it's an incredible honor to have you come speak to the TAC as we have this Subcommittee on Emerging and Evolving Technologies, trying to figure out recommendations for the Commission to consider and other regulators. Obviously, data becomes really important, and so access to data becomes very important for AI. And I think this raises important questions about who owns data or who charges for access to data.

And so, I don't know if the EO's competition provisions go to that, if there's other provisions but this important issue of access to data becomes really important because that's what goes into these AI models and other systems.

MS. KELLY: So I think there's two different components to that. One is sort of what is consumers' rights to their data and ability to

protect it so that it is not being used in ways that they wouldn't want. And that speaks to the call for comprehensive privacy legislation with its implications for data minimization and other things could be key for the AI ecosystem. The actions taken by the CFPB and the FTC, and some of the steps that we're taking in the EO around deploying and improving privacy enhancing technology and privacy preserving techniques.

There's also the question of entrepreneurs and startups access to data. We know that it's incredibly expensive to build large language models because of the cost of semiconductors, the cost of cloud computing, and the cost of that data. And so, part of what the NAIRR does is actually provide access to data to academics, to entrepreneurs, to try and ensure that we're not just seeing a handful of companies be able to leverage their data in ways that crowd out others.

CHAIR HOUSE: Thank you so much. So we have our two final questions, one from Corey and then from Justin.

MR. THEN: Thanks for the great work, Elizabeth, and the whole team. My question is kind of a derivative of Mike's, which is, how did the administration think about calls to create an independent agency that essentially handles just AI, or even more broadly, to handle technology, emerging technology?

MS. KELLY: So I would say that's really a question for Congress. There are certainly limits to what we can do with our executive authority, but we think that we've crafted a good solution leveraging the tools and expertise that all of our federal government partners have.

MR. THEN: I think you're right about it being a question for Congress. But was there discussion about this broader debate?

MS. KELLY: I think that whenever there is a new technology, there is always a conversation about what is the right way to regulate it. Is it a new agency? But I think we're very much focused on how do we use our existing tools consistent with the President's directive.

CHAIR HOUSE: Thank you so much, Corey.

Justin.

MR. SLAUGHTER: It's a privilege to talk to you about this Elizabeth, I know a lot of time went into this EO, and I have myself spent, I'm sure, a fraction of the time you spent developing it, reading it.

So I wanted to ask briefly about one phrase that's not in the EO, which is open source. I know there's been a lot of discussion about, of course, the need to support small developers. Your EO explicitly states you're supportive of competition, of helping small developers and academics build large language models and AIs, where so often only large companies have the resource deal with it.

At the same time, I know there is anxiety about releasing the open source data that underlies these AIs into the general public for fear that could be misused.

How is the White House thinking about the idea of supporting open source in AI versus the risk in doing so?

MS. KELLY: So you're right, Justin, the phrase open source does not appear in the Executive Order.

The phrase that does appear is “foundational models for which the model weights are widely available,” which is a type of open source, and it directs the Department of Commerce, specifically NTIA, to author a report looking at open source and determining sort of benefits, risks. Where is the ecosystem? Because we know that it is so quickly evolving and want to make sure that government is smart on the issue in moving cautiously.

There was a terrific kickoff, and there will be a request for comment forthcoming and I would encourage everyone to participate in that. I would also say that the EO very intentionally is focused on disclosure around large language models, where it recognizes this is evolving and we are not trying to stifle the technology.

And we're similarly focused on only the very most Frontier models, the models that are not even in market. So we can ensure that there continues

to be the rapid pace innovation that we've enjoyed.

CHAIR HOUSE: Thank you so much. I think a really incisive question, given that security and accountability involving open source software is relevant to all three subcommittees that we have, whether it's AI, Digital Assets, or Cybersecurity. So we're going to take a very quick break and reconvene at 1:35 folks. Thank you.

(Break.)

VICE CHAIR REDBORD: Thank you so much to Elizabeth and so much more going on today. Next, we'll build on our discussion from prior meetings regarding cybersecurity ensuring cyber resilience in financial markets. Our presenter is Mitch Herckis, Branch Director for Federal Cybersecurity in the Office of the Federal Chief Information Officer at the White House.

Mitch, I'm going to hand it over to you.

MR. HERCKIS: All right, thanks so much.

So a little bit about where I sit, beyond that, our office has wide responsibility to coordinate federal IT and cybersecurity policy

development, IT budget formulation and incident response on behalf of the OMB director. But also, cybersecurity is a team sport, and that's how the White House plays it. So we work across the entirety of it.

As an example, my boss, Chris DeRusha, who's the Federal Chief Information Security Officer, also wears the hat as the Deputy National Cyber Director for Federal Cybersecurity within the Office of the National Cyber Director. We're constantly working across the White House with the National Security Council, as well as our partners at CISA, at NIST, and beyond. And, of course, with the private sector.

The innovations in this space, just like we were talking about with AI, are moving quickly, and we need everyone to be working together to reduce risk.

Here, today, I'm hoping to talk a little bit about our Zero Trust journey in the federal government and how we got where we are today and that journey that we're on. It will, hopefully,

will kind of impart some of the key issues that private sector and the public sector are facing when it comes to this.

Effectively, the pace and sophistication of the threats have continued to evolve, as has how we use computers. So traditional security professional approaches that had happened for decades around how we secured networks, essentially were perimeter defenses, and we'd put up, essentially, walls and bolt on additional things, and build new ways of checking people when they came into a large perimeter.

However, today, we can't just keep bad things at bay by putting walls around a network. For one, most things are put in the cloud these days or they are accessed via IoT devices by other computers. And, of course, there's rapid increases in remote work as well.

We all saw that during COVID that not even the government is immune from having people have to come in all the time, right?

So we have to allow for people to work

remotely, whether it be via a mobile device, whether it be sitting at their desk at home. We have to understand that people will be accessing things from around the world, and that data, that is government data and government systems, may not be in a centralized location.

All that means is that the conventional perimeter defense is simply not sufficient. And when we want to protect critical systems and critical data, our adversaries know that as well and that means they will always have their opportunity to get a foot in the door if they see us trying to defend things in that manner.

Today's threats from cyberspace are really dynamic. They are some of the most serious challenges the United States faces in the 21st century. The administration has acknowledged this from the outset, and that is why they released Executive Order 1428, Improving the Nation's Cybersecurity early on in the administration.

This, as you probably are aware, was on the heels of several cybersecurity events. The

SolarWinds event was probably the most impactful for the federal government and was a supply chain attack on the SolarWinds company. There was also, though, several external events, such as ones impacting Windows Exchange Servers, and of course, the Colonial Pipeline event, which was a ransomware attack that shut down a significant, major critical infrastructure provider.

All of these kind of brought a lot of saliency to the issues, and in May of its first year, the administration really started moving this forward, and that served as our roadmap ever since.

Now the Executive Order talks about Zero Trust, but Zero Trust is really a loose term and it's more of a philosophy really, where a great deal of different actions can fit. With our Zero Trust Strategy, which we released about January thereafter in ’22, we defined what markers we expected agencies to take to defend their digital infrastructure from modern threats, essentially.

So we defined what Zero Trust meant to the federal government, which is essentially that no

actor, no system, network or service operating outside or within the security perimeter is implicitly trusted. Instead, we need to verify anything and everything, attempting to establish a form of access and that starts from really this assumption that individual users are fallible and they will make mistakes, and those mistakes allow for others to take advantage of them.

It also assumes that frameworks, even the best frameworks in the world, while useful, are ultimately also fallible and incomplete.

We appreciate our friends who build frameworks, both in the public sector and private sector, but we need to assume there's always going to be short changes on those structures. So we need to be able to verify those outcomes, do so continuously, and not assume anything can be fully trusted.

Zero Trust as a concept has been around for a while, but it's really been the last decade that those elements have really taken hold and the technology has been there to widely implement it.

There's no one plug-and-play solution here, is another thing I'd like to mention.

There's a lot of elements that you need to bring, but you can't buy Zero Trust. It's a continuous improvement. It's a journey that we've all been on. From our standpoint we want to make sure it has certain elements to start with, and I'll kind of go through what those are.

Essentially M-22-09, our federal Zero Trust Strategy created a baseline for agencies. It said we need to adopt certain elements that will put you on this path, this long-term path towards Zero Trust. That includes things like phishing resistant multifactor authentication, encryption of data, endpoint detection, response logging, vulnerability disclosure programs, manual expert testing of application security, and many more things, frankly.

We were aiming for security measures and targeting security measures that have been proven to significantly reduce risk in key areas and take the onus off individuals.

I mentioned phishing resistant multifactor authentication. It's a great example of this. We know that a simple name and password is not enough. People reuse credentials across their public and private lives, their business lives and their personal lives, those credentials can be compromised, reused, cracked, and that happens often.

And while having some sort of second factor, like a text message being pushed to your phone or a push notification or something sent to your email address, is extraordinarily better than just a username and password, even those are highly susceptible to what's called social engineering, which is someone reaching out, pretending to be from your company's tech desk or whatever, and they can ask for certain things to manipulate you into giving up or pressing that push button and approving, so on and so forth.

By taking it and moving it to a physical device, whether it be a YubiKey that you plug into your computer, whether it's using your thumbprint

on your computer keyboard or your computer being able to scan your face and recognize you, those are much harder for a threat actor to get remotely.

So the goal here is to reduce the burden.

And many times that means also a better digital experience, frankly, for the user as well. Not having to remember passwords as often, being able to know that you can access things in certain ways.

We also are trying to focus on other evidence-based ways to improve security, like vulnerability disclosure programs. For those that don't know, a vulnerability disclosure program allows for an ethical hacker or someone in the world who's good at these things, to essentially identify vulnerabilities within a system and notify the owner of the system and you having a simple process or a process to reduce the risk from those when those are found.

By requiring these across agencies, we are able to ensure those are being in-taken properly and then resolved and remediated quickly.

One agency, for instance, noted that in less than five months, its voluntary disclosure program received 330 vulnerability reports, 180 of which were critical findings. Those sort of things allow us to make sure the good guys are aware of it, frankly, before the bad guys are, and take care of those issues.

So at this point, agencies have been on the Zero Trust journey for two years.

About one year ago, I was saying the stories like those that I just mentioned showed that there were green shoots. Now I feel pretty confident saying that there's been significant cultural and technological shifts and they're very much cementing change in security across the federal government. And while the actions laid out in our Federal Zero Trust Strategy were always aggressive and bold, we've come extraordinarily far in ensuring those key measures are in place across the federal government.

So to kind of explain where we are today, I want to explain where we're coming from. When we

issued the memo, federal agencies were all required to provide us with implementation plans that essentially said through fiscal year '24, this is how we are going to get to these baseline elements.

All 24 CFO Act agencies provide plans as well as 46 non-CFO Act agencies, and ourselves along with CISA reviewed all of those. We held sessions with agencies to discuss them, engage on a one-on-one basis, and basically ensure that they were, from the get-go, on the right path forward when it comes to Zero Trust.

Now there's a large diversity among our agency partners from large federated agencies that are international in scope. Some shoot satellites into outer space, some are focused, small offices of a few dozen people. For that reason, each of those plans looked quite different and how we approach those plans looked quite different.

Our job really, was and is, to look through the issues impacting the agencies and bring them in as partners in discussing these key issues and bring in minds from industry and the private sector

to help them solve these problems.

We've expended a huge amount of our time, frankly, at OMB working directly with these agencies on their implementation plans, as well as working with them to continue forward on the technical and operational assistance.

We held numerous educational events along the way as well as kind of communities to push these things forward. For instance, we established Zero Trust-focused communities of action centering around key priorities within our Federal Zero Trust Strategy. We've completed two cohorts on phishing resistant multifactor authentication, which brought together agencies who wanted to do pilots on these issues, made sure that they were able to build and expand and mature, getting some help from each other, as well as from technical experts outside of their agencies.

We've also been doing this around DNS security encryption and growing it in other areas of Zero Trust as well.

We're also making sure, which is important in

government, that these are funded activities.

We released in FY '22 a Joint Cybersecurity Priorities Memo across both the Director of the Office Management Budget as well as the National Cyber Director, and what it laid out was essentially where agencies should be investing when it comes to cybersecurity. That's M-22-16 for those playing the home game there.

And essentially saying where they should be pushing additional resources to meet and align with this new Zero Trust framework.

We were able to also use those data points to essentially push and promote additional budget resources where necessary, along with their implementation plans. And, frankly, we did the same thing in FY '25, releasing a M-memo. Again, this year to basically ensure that as they continue down this Zero Trust Strategy journey, they're closing gaps that they may not close by the end of FY '24, as well as they continue to follow this Zero Trust maturity model that CISA has put out moving into the future.

And essentially, by using those techniques, we've been able to increase the focus in spending from $10 billion in cybersecurity in FY ‘22 to $11.2 billion in FY ‘23, and then to put forward 12.7 billion into the President's budget for FY ‘24. That's essentially a 13 percent increase year over year and 27 percent increase over two years.

Congress has also been an ally in this, frankly, in removing barriers to deploying these technologies.

Far too often, old legacy systems essentially can serve as blockers to the most modern cybersecurity technologies, like multifactor authentication, encryption, and other modern protections. Through the American Rescue Plan, a billion dollars was allocated to the Technology Modernization Fund to address urgent IT modernization challenges, $500 million of that has been targeted towards cybersecurity investments.

It's allowed us to do things like accelerate multifactor authentication at the Social Security Administration, USAID, and improve USDA's threat

monitoring detection response, as well as help them fundamentally change their network to a more robust and Zero Trust framed system. And frankly, the Department of Education has also used it to improve security and data privacy for 100 million students and borrowers.

These deployments take time, but at this point we're able to see a lot of real results. A very recent example of that is how sophisticated log-in techniques have helped agencies quickly identify anomalous behavior, or nefarious behavior, frankly, and be able to resolve it. One instance of that that received some news is around the State Department. They were able to detect anomalous activity related to a threat actor that was leveraging Microsoft's own environment to access the State Department environment effectively. Using log-in techniques.

State was able to detect and flag a highly sophisticated event for Microsoft, alert them, help us spot similar behavior at another agency, and ultimately allow Microsoft to shut it down and warn

its other customers beyond the U.S. government.

So following the issuance of the Executive Order, we never thought this was going to be an easy journey, but we've been able to really make a substantial difference and we know this because we've been measuring success in new ways.

We are able, OMB, along with our colleagues at CISA, to collect vast amounts of FISMA data from agencies to oversee their implementations. We've aligned this since FY '22, made significant changes to those metrics to align them with the Executive Order and Zero Trust, and that's helped us essentially measure these trends and these baselines.

We've been automating those metrics as well to allow the technologies to send us this information. So frankly, our cybersecurity professionals can focus their efforts on stopping the bad guys rather than reporting to us.

It also takes out a lot of the subjectivity. We make sure apples-to-apples machine information is coming into us.

We've also been using it for transparency, frankly, as well. One year ago, we released a tool on Performance.gov, which allows the public and Congress to track our progress. We're going to continue to update these metrics. We actually also are ruthless about getting rid of metrics that, frankly, we don't feel are meeting those needs anymore, and we are able to use them also to drive impactful security outcomes.

Right now we're in budget season. We bring that information to bear to figure out where resources are needed.

We are also aligning with the National Cyber Strategy, which was released last March. It is furthering our work around modernizing the federal defenses. There is an implementation plan along with that, and that is continuance of the work that was started with that Executive Order.

One other item that is in the Executive Order that I want to mention before we go and open up questions here, all of us can appreciate that our environment is only as secure as the underpinnings

of it, of the software that it is based on.

Software that's secure by design is ultimately a major goal of this administration. And one of the things we've been working on, and it's in Section 4 of the Executive Order, is essentially taking action to rapidly improve the security integrity of the software supply chain.

Part of that implementation, we're in the process of finalizing a common form for secure software attestation. This requires that software producers, whose software is leveraged by the federal government, attest to certain minimum standards of secure software development. It's a very new process for everyone involved. There's no equivalent out there right now. So we've been heavily engaged with industry to make sure we're doing this the right way and everyone understands what's necessary to do this right.

It's a crawl, walk, run approach from our standpoint. We want to make sure we are doing this in a way that allows the federal government to leverage the best software available, but also the

most secure software available.

In the end, we think getting this right is critical, and it's going to help reduce risk to the federal environment and build a better, more secure marketplace as a whole. So with that, I appreciate everyone's listening to our journey on this and I look forward to hearing a bit about where you all stand on this.

But in the end, I think the steps we're taking, we hope is helpful to industry, helpful to agencies, and kind of lifts all boats in the end.

VICE CHAIR REDBORD: Mitch, thank you so much for the presentation and for working to harden our cyber defenses. Justin, is your placard up?

MR. SLAUGHTER: That's an artifact, but I'm happy to ask a question. I feel like someone else should get --

VICE CHAIR REDBORD: It was so early, the placard up.

MR. SLAUGHTER: I was so quick.

VICE CHAIR REDBORD: Let's go with you, and then to Chair House.

MR. SLAUGHTER: Here's my basic question. This is all amazing, and I'm really grateful, Mitch, for your work on this, obviously.

I've asked this question before. The biggest problem with cyber, of course, is that if cybersecurity were a soccer match, we'd have a score of, like, 271-to-270. It's so much easier to attack than to defend.

How much of the hardening should itself be white hat-focused efforts to find vulnerabilities where they occur, or alternatively, be aimed at finding the nooks and cranny vulnerabilities of adversaries, rather than purely defending our own defenses?

MR. HERCKIS: So I sit on the side that focuses on defense, so I'm probably a little bit biased, but I will say that there has to be a focus from our side on there will always be individuals who are looking for a way in.

There's a wide diversity of threats out there from folks who are just kind of interested in playing around to nation states who are, frankly,

not, unlike in some other areas, they're not deterred by how much they need to expend to get in. Right?

So we need to be doing all things. We need to be assuming that they can get in and continuously moving forward and learning from the private sector and frankly, working with the private sector to make sure everyone's getting better.

On the offensive side, I can't really speak to that, per se, but I would say that we can't give up one for the other in any way. I think on the defensive side, we need to keep going, reducing risk and ensuring that we're doing the right things. So there's no one silver bullet here, unfortunately. It's a continuous effort and journey.

You know that's not a fun answer, but it's the reality of the situation.

VICE CHAIR REDBORD: Carole, this is an area where you've had a lot of focus.

CHAIR HOUSE: Yes. Thank you so much, Mitch. It’s great to see you and I’m excited to hear what

my old office at OMB continues to drive. It's wonderful to hear.

Speaking of that old office, you guys sit in a really interesting spot. Sort of functioning as kind of a pseudo-regulator for federal agencies, and given that we're here convened by the CFTC, I feel like I'm curious, knowing that we have a subcommittee on cybersecurity, which many people here are members of, including our co-chairs, one online and one here, Timothy Gallagher and Dan Guido.

I'm curious if there are some specific recommendations that you might have for them as they consider, any regulator has to think about what requirements are implemented via risk-based approaches and requirements, and which are more prescriptive. And some of the measures that the White House has driven for agencies are risk-based and some are more prescriptive, where presumably you guys have seen specific best practices that just need to be implemented across all agencies.

I'm curious, knowing that the CFTC currently

has ongoing rulemaking related to resilience and cybersecurity, how do you feel that -- are there any recommendations that you would have to them, as they consider in their regulations? How things like Zero Trust translate into a risk-based approach versus prescriptive requirements that they then have to oversee and enforce against?

And then a second question that I'm going to sneak in, also relates to open source software security, which was hinted at and was brought up as a question on the prior panel. That issue has been a huge consideration for the government, whether being a culprit in some of the breaches that we've seen facing agencies and also initiatives that you guys have been driving to implement greater security practices.

What thoughts do you have about how the Commission should consider open source security as a part of cybersecurity requirements for their regulated institutions?

MR. HERCKIS: So I'll start with the risk and prescriptive side of things.

We have a lot of great frameworks within government for securing systems and those are only as good as applied, right? When the rubber hits the road, you have to make sure you're also thinking through all the other elements and not just checking the boxes.

And so, from our standpoint, a lot of what we tried to do with our Federal Zero Trust Strategy was look for things that were easy to see, visible security outcomes, I think is a good way of putting it. And also kind of looking at the threat environment, frankly, and saying, here are the ways that tend to be the tactics, techniques, and procedures that seem to be most significant and really placing some chips there, I think, is maybe a good way of putting it.

So if you take a look at our Federal Zero Trust Strategy, you'll see there's a heavy emphasis on identity and how people approach, as I mentioned, phishing resistant multifactor authentication, data encryption. Those are significant ways where you can largely reduce risk.

We tried to aim for some of the things that we know work. You can see as evident in very simple ways that they're in place in some places. HTTPS is another way. There are a number of ways where there are evidence-based ways of telling that you have made a discernible difference, and we know for a fact, that it will make a significant difference in creating additional friction and means of deterrence, essentially.

So that's what we're focused on. Ours as essentially this first two-and-a-half, three-year sprint to get agencies into this Zero Trust structure.

Everyone's starting in different places, so where they had to within those agencies invest their resources was a little bit different. But understanding that there are these areas like endpoint detection response, encryption, multifactor, that make significant differences was where we put a lot of our kind of interest.

When it comes to open source security, it's a big problem and it's not just one that will be

solved in a vacuum. We're really working across the administration to try and find ways where we can invest in open source security as a whole, it's going to be something that the public sector and private sector are going to have to work on together.

In our approaches, we've taken varied approaches of working with the private sector to try and raise our approach there but it's an ongoing discussion, so there's not too much I can share there and where we're going with it.

VICE CHAIR REDBORD: Thank you so much. Commissioner Goldsmith Romero.

COMMISSIONER GOLDSMITH ROMERO: Thank you, Mitch. That was terrific. Mitch and I've talked about this before, and it just is an area that continues to be important but also a challenge.

And so, I had two thoughts.

One is I wanted to thank you for your remarks, and I really appreciate you talking about public and private sector working together. I mean, when I think about the CFTC, I think about critical

infrastructure. We're talking about agriculture, we're talking about energy, we're talking about supply chains.

And so, I think it's critically important that we have this ongoing dialogue and I remember Todd Conklin, in our first meeting, talking about sharing of information and trying to reduce the level of confidentiality so that it can be shared.

So, I think that part is worth emphasizing.

And then I had a second point, which is really a question, which is, as a federal employee, for more than two decades, I've watched sort of the requirements be put on federal employees about, I mean, we went RSA tokens and then another way, and then maybe RSA tokens are back and all of that.

How should government agencies kind of work with their employees to best get them to implement these measures so that we don't have a point of weakness, particularly when we're in, especially most agencies are in a hybrid environment, and so we've got people at home or wherever.

But one of the, I think, critical points has

to be, if we implement these measures, being able to make sure that our staff are following them.

MR. HERCKIS: Yeah, I would say what we need to do is really focus on that end user. Right? It's not just about security in the end. It's about finding ways to make it so that the security is easy for individuals or seamless or so behind the scenes that they don't even know it's there.

If you make the security onerous, people will find ways around it. That's just an unfortunate reality of humans. People want to get their jobs done, and people are going to find ways to do it.

What we try and do is ensure that it takes into account things like the digital experience of the individual user. So if we can move towards a passwordless environment that really recognizes through other techniques who the person is, where they are located, and based on those facts, perhaps they're on a government-issued laptop and their certs are on there, and they've used biometrics to log into that device. Maybe then they're allowed access to more files, whereas if they were logging

in remote via web portal, they may have far less access.

Those sort of decisions can be made in real time, frankly, and that helps us allow users to have the right access to the right information while reducing drag in most cases.

Unfortunately, historically, it's been let's raise the bar on everything all the time. And by changing how we do that and kind of right-sizing things for the risk, and also making sure that we can have the right security behind the scenes that's kind of doing the work for them, essentially, and continuously doing that verification, it makes it far easier, frankly.

VICE CHAIR REDBORD: Thank you so much. I'll take our last question, comment from Corey.

MR. THEN: Thanks so much, Mitch. Great presentation.

I'm wondering how quantum computing sort of fits into or has affected the work that you're doing. That's one.

The other one that I had, the Commissioner

brought up on information sharing, but I was once told by a cyber expert that they think about it almost like a neighborhood where somebody might be attacking JPMorgan and Deutsche Bank and Citi don't understand it or kind of know what's going on. And so, I'd just be curious whether the government plays a role in those types of situations or has a role to play with regard to information sharing.

MR. HERCKIS: Yeah. In regards to the first question, quantum computing is something that is out in the future a little ways at least. No one can tell you exactly when quantum computing will come online and have real significant impacts for cybersecurity, but we know it will happen eventually, and therefore, we're not resting and waiting for that moment to happen.

What we're focused on now is what we can do now is really focus on the fact that we can start looking into quantum resistant cryptography now, which will be able to resist quantum computers' unique way of solving problems. And we're looking now to get an inventory of what systems need to

move to post-quantum cryptography and then try and start prioritizing based on risk, upgrading and modernizing those systems to meet this risk that's out there in the future.

We'll be shortly, in the near future, reporting to Congress on that journey but that inventory is in place and we're continuing forward.

So when it comes to working together, I mentioned it's a team sport, it’s not just the administration, it is the private sector. And frankly, by working together, it's a nice area that everyone wins by sharing information and trying to get to the point where we can ensure that if we understand in one place how a certain threat actor is gaining access or a new vulnerability, known as a zero day, perhaps is being exploited, everyone gains from reducing that risk.

So the more information that's out there and shared, the better we can do.

Now, it's not an easy process to do that well and to tier risk, but there are good tools out there, and CISA is doing a great job of building

that community and driving awareness when there's significant risks.

So information sharing is critical. We're always trying to get better as a community in doing it, and I'm very happy with the way that our administration is leading the way on that.

VICE CHAIR REDBORD: Mitch, thank you so much for joining us today for the presentation and for the engagement.

We are now going to circle back to artificial intelligence for our second presentation on that topic, Professor Michael Wellman, the Lynn A. Conway Professor of Computer Science and Engineering at the University of Michigan will present regarding AI and financial regulation.

Professor Wellman, thank you for joining us on what Commissioner Johnson reminded us as a very important day for the University of Michigan.

PROFESSOR WELLMAN: Thank you very much for inviting me. It's really a pleasure to be here to talk about one of my favorite subjects, which is artificial intelligence and especially how it

affects financial markets and the financial system.

This has for some time been a research focus of mine. It's lately become an area that more and more people are interested in. Next slide, please.

And, in fact, understand the implications of AI on whatever field that you're in. No matter what you are doing, it has occurred to people that, hey, let me understand how AI is going to affect that, and that's a very sensible thing to be concerned about and to be thinking about. Next slide, please.

I want to though, say a few words about why I think X equals financial markets is special, and it probably is not going to be too hard to convince this audience that it's of a particular interest, that obviously that finance is a key financial sector. It's especially fragile, as we saw around 2008. It's built out of information and expectations, and moreover, it's already very highly infiltrated by AI.

And that's been somewhat long standing. There are some reasons for that that predate the most

recent developments in AI. I'm not going to go into it in any kind of detail, but just the fact that computers are fast, market mechanisms have very nice interfaces that are standardized, and we can build programs to basically operate through them. Computers are very good at taking in lots of information from a lot of different places all at once. And, of course, the stakes involved have attracted a lot of investment and effort.

One thing that I think bears even also some emphasis is that as all these areas of government and of society are thinking about how are we going to deal with artificial intelligence, how are we going to potentially regulate artificial intelligence, there's a possibility that finance can take the lead.

And one of the reasons is because there's a lot of existing regulatory infrastructure, and I'm saying this sitting in the CFTC, that is much more established, sophisticated, well-oiled compared to regulatory infrastructures in a lot of other domains.

So there's a potential for you, to basically provide case studies and lessons for a lot of other sectors as they start to deal with AI, as well. Next slide, please.

Now, when I first started studying the implications of AI, one of the first questions is why should it even matter if it's an AI or if it's a person doing trading? And it's really obvious that when you can get to levels of speed and precision that are way above human reaction speeds, some things could change and it leads to, it changes the timescale that events can happen way faster than the economy really moves. All kinds of strategies that were not possible at human timescales can become possible with computer timescales. It enables taking humans out of the loop.

In fact, it necessitates taking humans out of the loop because response times of people are not fast enough to operate.

So these are some of the reasons that AI has taken hold and has led to qualitatively new

behaviors or potential compared to in financial markets in particular.

Another is that once you build an algorithm to operate in some market, you could replicate it and have it go all around. That's another thing about AI, is that you can replicate it and scale it very fast. Next slide, please.

But the newest wave of AI, which I'll include generative AI, as well as things a little bit older, things like deep reinforcement learning, have yet further qualitative implications. I would argue for how we think about the effects of AI and finance.

One, in deep reinforcement learning, that's the technology for generating strategies, generating policies, generating ways of acting in the world. So what that enables us to do is to develop trading strategies, even taking the humans out of the loop of the development of the strategies themselves. Just using the data and our models to learn how to strategize, that's relatively new.

Second, with generative AI, things like large language models, is it opens up the language channel. I mentioned that one of the reasons that AI got our early foothold in financial markets was because they had these nice interfaces of very restricted. You submit orders of these certain types and have these fields that everyone knows, don't have to worry about language.

Well, now, even in areas where you do need language as an entry, AIs are potentially going to get in the door.

And this also, I think, will require some rethinking of new kinds of, as Commissioner Goldsmith Romero mentioned earlier, new kinds of scams that depend on putting things out in language are now possible.

So both of these effects can increase the scope of AI, as well as the autonomy of AI, because especially the language channel, if you can interact in language without being supervised by a person, that you can put your AI in new places. Next slide, please.

So my group, for the last 15 years or so, has really focused on finance as the domain. We wanted to understand the implications of algorithmic trading as that started to become a thing.

Systematically different, not trying to categorize with a broad brush as algorithms, are they good or bad, but rather try to understand which things are good and which things are bad and try to distinguish between them. I think that's the same thing we have to do with the new AI.

Our approach combines agent-based simulation with game theoretic reasoning, especially when you're talking about understanding hypothetical situations involving new capabilities or maybe new regulations. You can't just look at the data because the data does not reflect the new thing that you're thinking may come soon. So we want to try to get ahead of it.

I'm not going to go through all the various areas that we've studied, but there have been many, various issues around different kinds of strategies in the ecosystem of financial trading; including

market manipulation which I will talk about today, as well as we've studied various issues about the financial system beyond markets including things like banking regulation and new kinds of payment mechanisms, and so on. Okay, next slide, please.

A few years back, I wrote a paper with a colleague from the finance area of the Ross School of Business, Uday Rajan, that tried to recognize the fact that the technology will generally be faster in its evolution than laws and regulatory regimes. How can we think about that? Next slide, please.

We came up with a framework we called the ARB-BOT, which was basically imagining you have this general capability for arbitrage. Thinking of most algorithmic trading strategies can be viewed as arbitrage in some way, whether it be strict arbitrage or statistical arbitrage of some kind or another. And there's a spectrum from the most passive, just gathering information, noticing when there's an opportunity for profit and trading that's generally benign. You would think of it

often as helpful. It's not necessarily beneficial, but it often is.

But thinking about how that can often lead to additional strategies that you would regard as more aggressive and maybe potentially more dangerous for markets. So there's a thing about once you get really good at arbitrage, you want those situations to be present more, and if you could intervene in the world to make those situations present more, you can both make more profits and potentially distort the environment and make it worse.

And that is one part of what market manipulation is about, and particularly the technique of spoofing is basically instigating movements that lead to that.

You can be concerned about even more aggressive schemes where you have adversaries that are trying to subvert the economy or subvert a system, and those get into more of the cyber issues. I think at some point, the AI issues and the cyber issues kind of converge and they become the same issues that we deal with. Okay, next

slide, please.

So let me say a little bit more about market manipulation. You're all familiar with the regulation of manipulation. There are definitions in federal law from the SEC and from Dodd-Frank, among other places. A lot of these regulations depend on the notion of intent. Maybe the next animation, please.

Which, actually can be quite hard to establish for human beings as well, but it also presents a potential loophole. It's one example where regulations that are designed under the reasonable assumption that decisions are made by human beings may no longer be the right regulations and right rules when decisions can be made by computers and I think this is just one example of the kind of AI loopholes that we should be looking for all over the place.

And we study this in particular through an area called benchmark manipulation, using some statistic about market variables that can be used in contracts or derivatives, or as well as in

reference measures, the ability of computers to manipulate those, and I'll talk about that study in a moment. Next slide, please.

But manipulation, in general, there's been a lot of talk about how AI can maybe help to combat manipulation, basically using machine learning to build detectors. So, AI can be used on the part of an adversary, of manipulating, of attacking markets, but also can be used to defend them, for example, by developing detectors.

Now, this is challenging for many reasons, including the lack of widespread labeled data that has lots of examples of what would be a manipulative activity versus others. There's ways of dealing with that, I'm not going to go into, but even if you could do that, there'd be this additional issue, which is adversarial learning. Next slide, please.

Whenever you have a machine learning approach to try to detect adverse behavior, attack behavior, you get into a kind of arms race, which is called adversarial learning.

So in this case, we have basically this race between a detector and a manipulator. The detector looks at behavior, classifies it as being manipulative or not. The would-be manipulator is trying to manipulate, but is also trying to evade detection.

The problem is that the way this kind of machine learning works, is that any advance in detection immediately could be exploited by a manipulator to evade the detection. If any of you have seen technology called generative adversarial networks, that's a lot of how generative AI works. It works by basically improving, by having an interplay among two machine learning efforts.

And because we have this kind of, I called it an arms race. Whenever you have something that you could call an arms race, the ear should perk up. It's maybe not good. It has an indeterminate outcome.

This is really no different than detecting fake news, and evading detection of fake news in the same manipulation, is really just a kind of

that. So next slide, please.

We decided to do a little case study where we built a very simple spoofing algorithm and we also have a market making algorithm, which is considered to be a benign trading algorithm. And we built a detector that could tell the difference between them. Both of these algorithms put in orders and cancel orders, and they change orders all the time and it was very easy to detect given how we coded it.

But then we have the spoofer try to modify its strategy to evade the detection, basically to look more like a market-maker. Basically, put more orders in on both sides and do things that would basically obfuscate the spoofing activity. Next slide, please.

And so, this is just a little bit of an illustration. We went through several cycles of this. You evade, then you build a new detector that tries to detect the new evasive action against the market making. And you can see just visually that what I'm showing here is the spoofers order

stream. Here it's starting to look more like market making in terms of just a high level pattern. And in this case, the effect of doing that did evade the detection, but it also degraded the manipulation.

You could view that as a kind of a good outcome. We forced it to weaken itself by basically diluting its behavior. Now, I don't necessarily take great solace from this, because we can't really be sure that maybe we weren't smart enough in how we were doing the evading, and there could be other ways to do that. And like I said, I think in general, these are indeterminate outcomes, these kind of cat and mouse, predator/prey dynamics, which you'll always have whenever you try to do that.

So, I guess I'm saying I'm all in on trying to use AI as much as possible for reg tech and for doing that, but let's not put all of our eggs in the basket of relying on machine learning to solve it. We have to rely on things like cryptography, watermarking, and other kinds of things to also be

in our arsenal as well. Next slide, please.

So I mentioned benchmark manipulation.

So one of our most recent studies was we looked at the issue of manipulating benchmarks and doing that automatically via machine learning.

So the benchmark we use is VWAP, which a study by Duffie and Dworczak some years ago, a few years back, argued theoretically that it's the most robust, that it's least manipulable example of a market benchmark statistically within a class that they studied.

So we built an agent-based simulation where we had some background, benign traders, some with a market-maker, some without a market-maker, and then we threw in a manipulator. Next slide.

So the manipulator here, its total profit is the profit it makes from the market which here is V, plus we assume that it has some contracts that use the benchmark as part of the terms in the contract. So its total profit will be what they make in the market plus what they make over their benchmark tide contracts.

We did a hand-coded manipulator, we call it here ZIM, as well as we took two different reinforcement learning approaches to try to learn a manipulator and they're two qualitatively different ways of doing it. I'm not going to go into the details, but next slide.

But just real roughly, the scheme is we have an RL algorithm. It interacts with the market, the market shows, gives it some state information that is the observable features of the market, what trades have happened, what orders it can see, and so on. Next.

The RL algorithm tries some actions and then it gets some feedback. Next slide.

Which are called a reward here.

And so, you could learn a trading strategy this way by seeing how what happened if the update of the market improved your situation or hurt your situation compared to how it was before based on your actions and RL is kind of a very complicated credit assignment place that tries to drive an overall strategy based on that kind of feedback.

So to add the benchmark, we just give it another component of the reward signal based on the contract holdings.

So notice the developer of the AI is not saying go manipulate this market, it's just saying go make some profits. Now just include the benchmark contract holdings in my reward signal.

And what we find, and I'll go through the results relatively quickly, is that it was successful. So next slide, please.

I'll kind of go through the details of the experiment, but next slide. So here we see that the point on the left says ZI. That's no manipulation. So the market profit and the total profit are the same because it doesn't have any contract holdings that it's aiming at.

Here, the other three strategies, the ZIM is the manually-coded manipulator and the DQN and DDPG are the two RL manipulators. Advance the animation, please.

So you can see they have a higher total profit. So they got more profit than the no

manipulation case. And next animation.

But notice that they have lower market profit.

So they sacrificed, they did worse in the market, but that was okay because they were making it on the contract. Next slide.

So that graph I just showed you is now here, the graph on the left. Just rescaled. So you see these are relatively narrow. That example was with a market-maker. The market-maker stabilizes things and makes it harder to manipulate. But it didn't make it impossible to manipulate, so it learned to manipulate even with the market-maker. Without the market-maker, the slide on the right, it just goes crazy and it makes crazy amounts of additional profit. Next slide.

Just to point out the background traders here, they actually do a little bit better when the manipulators are there, it's not necessarily very large or significant, but they do a little bit better. Why is that?

Well, if there's a party there that's willing to lose money in the market, the other participants

in the market can actually pick up some of that profit for themselves.

So they're not going to be the one policing against this.

Who is the loser? The losers are the counterparties to the benchmark contracts. They're not in the model, but they're the big losers. Also, there's perhaps some less information in the prices and the benchmark anymore because that's been degraded because of the subversion here. Okay, next slide.

We can just go through it, I think, why don't we go since I know we're short on time, just all the way to the last slide. Well, so actually go back one. Thank you.

So just to recap what I said about manipulation, we can capture it in an agent-based model. We have this adversarial learning situation, basically an arms race between detection and evasion, which we don't know what the outcome is going to be, and we can also automatically learn to manipulate. These are sort of new things to

worry about.

So the AI implication here is that we should be prepared to deal with some super manipulators.

Okay, now let's move all the way to the end, if we can, because I know I'm really out of time.

I was going to talk about some of our, if we had time, recent work on just generally trying to evaluate AI, but let me lead with this.

So I think that understanding AI and X is obviously occupying the minds of a lot of parts of our society right now, justifiably. The case for finance is especially compelling.

I had the privilege of testifying before the Senate Banking Committee last September, and what I told them is a lot of what I told you. So go forward, please.

Worry about super manipulators. I talked about the AI loopholes. I talked about opening the language channel.

And one thing I haven't mentioned yet today is that maybe another kind of concern is to the extent that whoever has the best information will have the

best AI, we may need to worry about concentration of ownership of large bodies of nonpublic information that have sort of strategic value. It's always had some strategic value. Maybe it has new strategic value. How it could be exploited in financial markets, I think is a somewhat untested question and deserves some more thought.

The last thing I'll mention is that I was really happy to learn recently about the legislation that Senator Warner, with Senator Kennedy, put, the FAIRR Act, the Financial AI Risk Reduction Act, that explicitly tries to close that loophole that I talked about today.

Thank you very much.

(Applause.)

VICE CHAIR REDBORD: Professor, thank you so much for the presentation. Really, really, extraordinary.

Do folks have questions on the TAC? Yes, sir.

MR. SALUZZI: Professor, thank you.

A question for you, which is coming from my side of the markets, which is the equity markets.

We've got something called the Consolidated Audit Trail, which was put in place -- it was conceived in 2012, and it was finally put in place in 2022. Millions and millions of dollars, massive delays in it. It was an SEC approval, and then FINRA finally got the contract.

Is it outdated already?

Because from what he just told me, it sounds like that system can't compete with AI and all sorts of manipulators that are probably when we conceived the Consolidated Audit Trail, data and algorithms are a lot different than they are today. So is it already out of date?

POFFESSOR WELLMAN: Thank you, Joe, for the question.

It's an interesting question. I guess maybe the way I would spin it is that imagine where we would be without the Consolidated Audit Trail and trying to deal with some of these issues. So I mentioned the general non-availability of a lot of labeled data.

And, of course, another big issue is that a

lot of the data is very fragmented. So if you're a body for a particular exchange doing regulation, you only see what's happening in your exchange. The Consolidated Audit Trail does give at least, FINRA, some cross-exchange visibility into what's happening, and especially with a lot of these kind of manipulations that will involve cross-market arbitrage. You'll need at least that.

Now, do we know how to use it in the best possible way yet? No, I think that's going to be one of these hustle things that has to be done.

VICE CHAIR REDBORD: Thank you so much for that. Corey, is yours up?

MR. THEN: Also a remnant, but let me just make a comment.

Great presentation. I really appreciated something that you put up there on potentially having to change legal standards, in particular with intentionality once you have this [unclear] up and running. That was eye opening for me. So thanks.

VICE CHAIR REDBORD: Thank you so much.

Nicol, and then Michael.

MS. TURNER LEE: I'm right next to you.

Thank you for the presentation. Really interesting, and as a researcher, refreshed my memory on things that I did not like to study when I was in graduate school. So I give that all to you. But I have a couple of questions.

My colleague, Todd, and I are on the Emerging Subcommittee, which is going to be looking at AI along with many of our colleagues here.

So a couple of things. One thing that we were chatting about most recently was the extent to which there's manipulation between machine-to-machine, right? So we're seeing a lot more attacks that are happening that may not be a new model being developed by someone externally, but the machine picking up language along the way, and it's sort of designing and redesigning itself to be able to become smarter.

So I'd love to hear more about that.

And then, also this idea of watermarking in financial services, I did participate in one of the

AI Insights forums, which was hosted by Senator Schumer, and we're seeing a lot of that on the copyright side. I'm curious to hear your opinion on watermarking on the financial services side, particularly when we're trying to get to [unclear] about content that's generated on trading or other vehicles institutionally that we should be concerned about.

PROFESSOR WELLMAN: Let me pick up the second one. First, in part because I'm not a technical expert on the crypto underlying watermarking and to how well it will ultimately work and under what is the scope, but I think it's got to be taken as far as it can go.

Because like I said, I think the machine learning-only approaches are not going to be sufficient and I think getting the requirements out that a party has to exert this effort to indicate when it's the bot who is responsible for the action and to tie and to keep that together. So I think it's just got to be pushed as far as it can go.

The question about the bots manipulating the

bots, I mean, ultimately it's all AI, and a thing about manipulation is that you can't study it in isolation because it depends on who's manipulable.

So when we do these studies, if you have an algorithm that is not looking at certain information, they're immune from being manipulated about that information. So it's only to the extent that anyone is looking at information that using that misleading, about that information can have that effect.

So ultimately, there is a natural self-defense that these bots will have against being manipulated. Some of these early, very simplified approaches to sentiment analysis and other things were very easily affected. I think there was an allusion earlier today about glitch in markets because somebody put out a photo on bombing and that's only because there's automatic things that are looking for those that are going to have those effects.

So there's some natural incentive for parties to learn how to not get misled, but I think there's

always going to be some irreducible vulnerability to being misled that will require policing and enforcement.

MS. TURNER LEE: Madam Chairwoman, can I do a follow-up question?

VICE CHAIR REDBORD: Sure.

MS. TURNER LEE: I'm sorry, Mr. Chairman.

VICE CHAIR REDBORD: You're good. Yes, of course. Go for it.

MS. TURNER LEE: I just had one other follow-up question on that.

So with regards to best practices for industry, given that you would want -- you know, we heard from the White House, they're sort of trying to get into this technical space, right? Where they can get companies to have a little bit more responsibility on the technology side.

Is it your opinion then that there should be better disclosure when companies are trying to sort of look at some of these practices that you're suggesting in terms of being able to scam or super manipulators?

As we know, a lot of tech companies say things like, we're using AI to fight AI, but we're not really sure what's under the hood.

So I'm just curious, from your perspective, from a policy perspective, should there be more best practices, more shared learnings, more disclosure around the use of AI in the financial markets?

PROFESSOR WELLMAN: Yeah, I would say absolutely, yes.

Now, of course, whenever those requirements are going to come up, there's going to be objections that they're intrusive, that they're going to make me reveal trade secrets and other kinds of things. So there's going to be some interesting navigating for how to disclose the things that clearly need to be disclosed and how to make the requirements as least burdensome and least intrusive as you can get away with them being.

MS. TURNER LEE: Thank you.

VICE CHAIR REDBORD: Michael Greenwald.

MR. GREENWALD: Thank you. Thank you,

Professor, for the presentation.

When you look at how AI within finance allows us to reimagine the financial risk assessment, how do you see risk changing and defining risk differently given the applications that are currently at our disposal, and that will be at our disposal, given that really the yard line for risk continues to shift?

And so, how do we look and define and redefine and reimagine that risk assessment moving forward?

PROFESSOR WELLMAN: So, obviously, I think it's necessary to separate different categories of risks. Right? So there's the risks of petty theft and skimming of profits here and there, versus the risks of instability and subversion of markets, and probably those needs to be put in different categories.

I think you can try to deal with them, they're all important, but I think trying to define what are these adverse outcomes that you're trying to avoid is a part of that kind of risk. I think that because especially when you talk about catastrophic

events in the financial system, those are not something that there's lots of data about. By definition, they're rare and things like that.

But I think that's where it requires the kind of more imagination, hypothetical reasoning to define and quantify the risks of those.

VICE CHAIR REDBORD: Jonah, last question for Professor Wellman.

MR. CRANE: I'll try to be brief. Thank you, Professor, for the presentation.

I wanted to pick up on one of the points you made early in the talk where you said that the existing regulatory infrastructure and financial services may provide an opportunity to inform regulation in other sectors. It just strikes me that we're at a moment where the White House is putting out AI Bill of Rights and Executive Orders, involving a whole bunch of their agencies. There is sort of, what I'll call horizontal regulatory standards being developed for an AI, like the NIST Risk Management Framework. At the same time, the financial regulators have, for the most part, said,

basically our existing rules apply, whether you're using AI or not, without providing a ton of AI specific guidance.

So how do we marry up these various efforts?

So, for example, will the financial regulators say, okay, if you're following the NIST framework, that's good enough for us? Or maybe the NIST framework, over time needs to be informed. Maybe this is partly what you were suggesting, horizontal standards can be informed by more sector-specific efforts. But it just strikes me that there's a lot going on and it's a little bit hard for me at least to figure out sort of what is the standard that's going to be applicable in any given context.

How do we think about that?

It seems to me that at the very least, what we need is a lot of interagency work. A lot of sort of interdisciplinary work to make sure that these efforts are informing each other and we don't end up in a world where those two things work at cross purposes or inconsistent, so that I might be operating in one sector and have inconsistent

standards that apply if I'm trying to operate across multiple.

PROFESSOR WELLMAN: Well, I think it's also inevitable that mistakes will be made in the regulation of AI, both by omission and commission, and the key issue is to learn from the mistakes. Even the situation where it might be deemed that existing regulations already cover what we care about, well you're going to find out whether they do or not, and the extent that they do.

There may be the other sectors where they don't even have that regulation, right? And there's going to be other areas where they don't.

This is certainly in discussions about the fraud potential of AI. There's already, of course, lots of rules and regulations that prohibit fraud, but new modes may circumvent them, and I think we have to be watching for them.

VICE CHAIR REDBORD: Thank you so much. We are going to take a five-minute break and let's keep it to five minutes because we have a lot to get through in the next hour or so. Thank you

everybody.

(Break.)

VICE CHAIR REDBORD: We are going to get started.

CHAIR HOUSE: We are now ready to explore our final topic of the day, consideration of the report containing recommendations regarding decentralized finance from the Subcommittee on Digital Assets and Blockchain Technology.

I am extremely honored and proud of the work that the Subcommittee has done, and thrilled to have worked with my amazing Co-Chair Dan Awrey. I'm really excited about being able to share with all of you the key takeaways from the report that we've drafted and to get input and foster a really good, robust dialogue and discussion with all the members of the Technology Advisory Committee about the recommendations and the substance that are inside of the report.

So the plan for today is to have a robust discussion regarding that report and then ultimately a vote by the TAC regarding whether or

not to adopt it and its recommendations to the Commission.

Before we delve into specifics, Ari Redbord would like to provide a few introductory remarks.

VICE CHAIR REDBORD: Thank you so much. It's an honor to kick things off. Thank you to Commissioner Goldsmith Romero and the DeFi Subcommittee co-chairs, Carole House and Dan Awrey for your leadership.

About a year ago at this Committee's first meeting, I began my remarks, “The true promise of blockchain technology is DeFi. DeFi is financial services offered without a traditional financial intermediary delivered via a software program or smart contract, which uses distributed ledger technology and enables peer-to-peer transactions. DeFi enables an ecosystem of peer-to-peer-financial services untethered from many of the issues that plague our current system, and offers the promise of financial inclusion, peer-to-peer cross-border value transfer at the speed of the Internet.”

That is the promise. This extraordinary

report we're going to hear about today does not lose sight of that promise.

However, the report also acknowledges the credible risks to systemic market integrity, consumer protection, and those that I'm most focused on, illicit finance and National Security, posed by a financial system characterized by highly automated, disintermediated financial networks.

While over the last few years policymakers around the globe have constructed regulatory frameworks for crypto assets, the focus has almost exclusively been in the context of centralized exchanges, with regulators seeking information from siloed intermediaries the same way that information flows from banks to their regulators today.

Today's report from this committee is one of the most thorough and accessible explanations of the technical and regulatory opportunities and challenges as we build together in DeFi. The challenge for regulators and policymakers, as we move deeper into a more peer-to-peer, decentralized financial ecosystem, is how to ensure that lawful

users are able to transact in a secure and private manner, while at the same time mitigating various risks, including systemic market integrity and those associated with illicit actors who seek to take advantage of the promise of the technology for maligned activity.

According to the TAC, “The central message of this report is that both government and industry should take timely action to work together across regulatory and other strategic initiatives to better understand DeFi and advance its responsible and compliant development.”

I am looking forward to working with this committee, DeFi builders, and policymakers, on these efforts. Thank you so much.

MR. AWREY: Thank you, Chair Redbord, next slide, actually, please. Thanks.

I'd like to begin, Chair House and I would like to begin by acknowledging all of the members of the Subcommittee that worked on this report. It really was in many ways a model of what you want these discussions to look like, with people with

diverse expertise and views coming together. Hashing out differences and asking questions of each other, and our views, attempting to understand as best as we possibly could, given our mandate, what exactly is happening in the world, and devising a way of approaching its future developments and regulation.

And so, we just wanted to start by thanking everybody on the Subcommittee for their time and efforts and really an incredibly positive outlook in the approach to the drafting of this report. Next slide, please.

We're going to divide up responsibility for this. I'm going to talk about the first couple of sections here, really looking at our approach.

And as I'll talk about a little bit in a second, this is an approach that while we've developed specifically for the purposes of this task, is one that we think can also be applied to broader questions about the implications of new technologies and the assessment of regulatory threats and opportunities, and how to apply -- and

in some cases, evolve existing regulatory frameworks in response to those opportunities and threats.

I'm going to, then, turn it over to Chair House, who's going to talk about the specific recommendations in the report, and what we're urging both policymakers and industry to do going forward. Next slide, please.

Before getting into the report itself, I did want to make just a couple of observations about the general approach that we've taken.

One, was to lean in as a group towards problem solving, problem solving around building of DeFi ecosystems, but also problem-solving around tackling the various risks. This is something that is not uncontroversial within this room and in broader sort of discussions about DeFi. But ultimately, this market is big and it's growing and it's developing, and it poses risks now, and it will pose even bigger risks in the future.

Two, as I mentioned before, really, especially the first part of this report where we talk about

mapping these ecosystems, identifying the regulatory objectives that we want to achieve, and understanding what types of opportunities and risks are presented by new technology is something that we hope will find broader application across government, not just in the CFTC, but across the financial regulatory community more broadly.

Lastly, this report is just a first step.

We are not asking the agencies of government to turn the ship. We are asking them to spend some time charting a course and scanning the horizon for potential opportunities and risks. So whatever happens today really is only beginning of this process, and it's one that we urge policymakers to move ahead with, with speed and diligence. Next slide, please.

In terms of key takeaways, our first key is that, not surprisingly, the development of DeFi projects, enterprises, and ecosystems hold out a number of potential opportunities, many of them relating to longstanding issues with a conventional financial system, but also pose a number of risks.

And a key thing here is that these opportunities and risks are related to each other. The opportunities require scale. Scale requires trust. Trust requires effectively addressing the risks, both through industry mechanisms, but also effective regulation.

Second, the benefits and risks of DeFi depend greatly on what it is we're talking about.

Today, and in the report, we're going to present a definition of DeFi, but we're also going to talk about the various ways that decentralization can manifest itself across different types of projects, and ultimately, understanding the risks. Understanding the potential rewards requires that level of granularity in order to both build these systems to be safe and fair, but also to make sure that the attendant risks are properly mitigated.

Third, having said all that, one of the things that almost all DeFi projects, enterprises, and ecosystems share is that there are question marks surrounding who is ultimately responsible and

accountable for when things go wrong. This is almost inherent in the nature of DeFi, both because of code being subject to problems of incomplete contracting, because it's difficult to code robustly for changing circumstances, including new regulation. And ultimately, because some people will inevitably try to use the distinction between centralized and decentralized to engage in potentially welfare-destroying regulatory arbitrage.

Lastly, all of us are in this. This is a problem for industry, this is a problem for government. It's an opportunity for industry, and it's an opportunity for government. And one thing that we were eager to get across as a subcommittee was that only by working together across government and with industry actors are we going to realize these opportunities, and only by working together and across government and industry are we going to mitigate those risks. Next slide, please.

And I suppose next slide again.

First, definitionally, and I wanted to

highlight that we have provided a singular definition of DeFi, and then simultaneously observed that that singular definition in many respects is not particularly reminiscent or reflective of a lot of what's happening in the DeFi ecosystem now.

That is, decentralization is not a question of all or nothing. There are degrees, and those degrees have dimensions. And the Subcommittee identified five in particular that we think are important.

The first is access. Whether these networks are permissioned or not permissioned. In effect, whether there are gatekeepers that control entry to the use of the products and services that these networks provide. Whether development is decentralized, that is open source, for example, or whether it's in the hands of a smaller group of actors or a firm that's creating proprietary software.

Third, governance. Whether decisions are being made broadly or amongst a centralized group

of actors. And, again, immediately we can see that some decisions may be those that are based across a broad spectrum of different users. Others may be very, very concentrated, especially when things go wrong.

Fourth, whether these ecosystems have centralized balance sheets or decentralized balance sheets.

And lastly, we have a series of questions around operational centralization or decentralization, and to sort of indicate why that's important, let's go to the next slide.

When we look at what really defines decentralized finance, this is what we see. What we see is a tech stack where many different actors are contributing at different parts of the ecosystem in order to provide a specific product or service.

I'm not going to go into detail here in terms of each layer, the functions performed at each layer, or the key players. The key takeaway is that these layers exist in the context of

decentralized finance. They're often provided by different and independent actors who themselves may display different levels of centralization or decentralization.

Importantly here as well, once you throw the feature of composability into the mix, you can get networks-on-networks. And this represents an important part of the challenge of then attempting to govern what is relative to a conventional DCO or relative to a commodity futures merchant or another centralized actor. Kind of a different ballgame. And that ballgame is ultimately the one that the report is trying to urge the creation of rules around. Next slide, please.

In the context of writing the report and sort of developing this framework, we also thought it was important not to define decentralized finance, but to point to a number of features that decentralized systems have and to consider the implications of those features.

And the two that I would like to call out here in particular, are one, automation. We've already

heard today quite a bit about automation in the context of AI, and in many respects, these are inseparable topics from a regulatory perspective. Automation, though, brings with it questions around the completeness of the code that is undertaking the automation.

What happens when algorithms go rogue? And more generally, going back to one of the big themes of the report, who's ultimately responsible when those rogue lines of code actually harm investors, or destabilize the financial system, or undermine AML, KYC, or National Security?

Putting all of these things together, what becomes apparent quite quickly, is that all of centralization and decentralization exists on a spectrum and that makes the question of regulating decentralized finance not a single question but a much broader question about the types of risks that we ultimately encounter in different business models, and then questions about how to address those risks.

The other side of the equation, of all of

this, is that the diversity of risks is also mapped by the diversity of potential business models and opportunities for making finance better for everyone.

In the report, we map several potential and existing use cases here. We can talk more about that during the Q and A. We are really grateful at this point to the members of the Subcommittee who dedicated their time and effort to really educating us about what's happening already and what the ultimate goal is, or what the ultimate sort of endgame is for the development of some of these use cases. Next slide, please. And next slide again.

So, having mapped the state of technological change, so having mapped the thing, even if our definition of the thing is actually multidimensional. The next question for us is why are we all here? Why, as a subcommittee, have we been engaged by the CFTC to actually explore these technological developments?

And our touchstone here are these regulatory objectives. These objectives, I want to note their

source, but then also something that stands out about them.

First, this is a synthesis of existing regulatory mandates, not just for the CFTC or SEC, but for all federal financial regulatory agencies, along with statements that have been made by the White House, by the Treasury Department and other agencies about the things that this government cares about.

The second thing is that when you put all of them together, they do not map neatly at all onto the existing regulatory architecture of federal financial agencies. Some of these objectives relate to financial markets. Some relate to financial institutions, some relate to National Security. All of these things are the responsibility of many agencies in government, not just one, which is one of the reasons why we've been so full throated in our support for an all of government approach to surveying the opportunities and risks of decentralized finance.

Next slide, please.

So what are these opportunities?

I'm cognizant that we've been here for quite a bit of time and without snacks, to boot. So I will keep it brief.

All of us here at some point, somebody raised the specter of 2008 earlier today, I think it was Professor Wellman. All of us are aware of the deficiencies in conventional finance.

Some of these deficiencies relate to information silos. Some relate to too big to fail institutions. And one of the big, at least theoretical opportunities created by the rise of the technologies that we call decentralized finance, is the ability to smooth out some of those efficiencies. To create new and better ways of providing products and services that are technology-driven, that are data-driven, and if we can do so safely, if we can do so fairly, then to create business models that are not so highly correlated to fluctuations in business or financial cycles. Or at the very least, don't suffer from the same vulnerabilities as conventional financial

markets and institutions.

Now, of course, if you do that wrong, you've created the exact opposite problem, which is hugely correlated risks between centralized and decentralized finance with a prospect of cross-sectoral contagion, which I'll come to a little later on. Next slide, please.

Some of the other risks, or some of the other opportunities that we considered as a subcommittee, are a little less granular to financial regulation and a little more related to general issues of competitiveness in the financial system and real economy, to the U.S. approach towards technological innovation more generally. And I think what's fair to say, questions around the extent to which federal policymakers want to promote innovation and want to be involved in promoting innovation and that in turn bleeds over into questions of U.S. and global leadership in technology and finance.

At the heart of this, are questions that I think it's fair to say go beyond the paygrade of the Subcommittee, such as we have a paygrade, that

relate to how the U.S. wants to position itself in the midst of a period of technological change. Both in terms of whether it wants to be a leader in building the new infrastructure of the digital age, but also whether it wants to maintain its status within the global policy community that is already well-advanced in considering many of the risks and opportunities presented by decentralized finance. Next slide, please.

All of which, of course, takes us to the risks. And one of the things that I personally pride myself on in this report is how candid and how in-depth we went into the risks posed by decentralized finance. These risks are extremely diverse and context dependent, so I don't really think it's necessary to go into them all here.

But I did want to highlight, again, this is basically every risk in the financial book. This reflects the fact that decentralized finance is being used across conventional financial markets, institutions, and activities to find new ways of doing things.

There is nothing that decentralized finance doesn't raise in terms of questions around its effective regulation. That, again, underscores the enormity of the task that policymakers face in attempting to map these risks and find ways to effectively address them.

But in saying that, it's also clear that this is not a CFTC issue. This is an issue for everybody in the policy community, and everybody's going to have to work together on this. It is not the case that protecting consumers is just something for one agency. We spread this out across multiple agencies, and one of the things that's going to be necessary is bringing everybody together to the table.

So to talk about that in more detail and the ambitious, although we think well-advised plan moving forward, I'm going to turn it over to my Subcommittee Co-Chair, Carole.

CHAIR HOUSE: Thank you so much, Dan. Next slide, please. Great.

So first, we're going to kick-off with the

specific key issues that the Subcommittee was able to distill after having mapped and identified the key opportunities and risks related to DeFi, and we've done our best to define it -- and not define it, but attribute specific features and key issues related to decentralization and the spectrum that exists there. Next slide, please.

So both public and private sectors hold critical and unique roles and responsibilities to design and implement policy frameworks related to any type of activity, but especially in emerging tech and finance. So both sides, we feel, should devote effort to dissecting these key issues, determining the most tractable and the highest impact, and translating that into near-term and long-term priorities and action.

So for issues for policymakers.

Policymakers ultimately bear key responsibility for articulating, monitoring, and enforcing compliance with legal and regulatory obligations. As Dan mentioned, the report is only the beginning. There's a lot of work that we

recommend and that we highlight that policymakers are going to have to address, including since, as Dan mentioned, we pointed out what a lot of the risks are but much must be done to map and understand DeFi ecosystems, look at the specific risks and the nature and extent of them for each of those systems, and, ultimately, there's a lot of complexities and novel features that policymakers are going to have to address, which may demand that policymakers fundamentally rethink and reframe their current regulatory frameworks in certain instances, along with their approaches to supervision and enforcement.

So I'll take a note from Dan and just highlight a couple of key issues on those for policymakers that the Subcommittee had highlighted that I think are especially of interest for the Commission and for those of us here to discuss.

First is determining whether and how DeFi systems fall within the existing regulatory perimeter. That's the place that you start. You have to evaluate how, in the current universe of

DeFi ecosystems, it falls within the perimeter of existing legal and regulatory frameworks, which requires determining both subject matter and geographic jurisdiction for U.S. policymakers. That is not necessarily easy based on the construct of DeFi.

Assessing jurisdiction can be challenging. It requires a complex understanding of the actors, the activities, components of the systems, and identifying where key points of control and sufficient influence exist. Determining whether or not having one or multiple parties engaged in regulated function is sufficient to meet the threshold for being regulated and enforced, as well as highly dispersed business operations, can all make determining that jurisdiction very difficult.

This will also not only apply to financial regulation. The Subcommittee highlighted that, for example, it's possible that certain entities inside of DeFi systems may be covered under forthcoming regulations coming from the Cybersecurity and Infrastructure Security Agency regulations that

they're opposing for imposing cybersecurity incident reporting obligations on critical infrastructure operators. It's also possible that regulations that are currently being promulgated at the Department of Commerce, subjecting Know Your Customer, or KYC, obligations to infrastructure as a service operators, may also be subject to certain DeFi ecosystem and infrastructure operators.

These are questions, but especially given that many components of DeFi systems claim, and in some cases are not necessarily financial, other types of regulations may in fact be in play here.

Another key issue was looking at where and how the regulatory perimeter might be expanded.

Policymakers will have to identify where there needs to be an expansion of legal authorities or using already existing authorities to capture more parts of the DeFi ecosystem to mitigate relevant risks. Most existing regulatory frameworks target especially the application layer. That's what we're used to. That's the part that typically interfaces most with consumers. It's one where

identifying key players and responsible parties tends to be a bit easier and more readily identifiable.

But if the risks in a DeFi ecosystem are not sufficiently mitigated with imposing regulations at the application layer, policymakers must look elsewhere within DeFi ecosystems to locate and enforce controls consistent with policy objectives, and this may require a new envisioning of types of institutions and activities that should be subject to regulation.

Crafting the appropriate regulatory response will require an understanding of specific risks. The risks that we outlined do not point to or do not assess the probability or impact of all of them. We just highlight what could be the impact. But the risks are unique based on each system's design and features and attributes.

Permission systems and permissionless systems have different levels of risk for things like anti-money laundering and illicit finance, compared to operational resilience in the face of cyberattacks.

So the specific features for each unique system demand specific evaluation.

Allocating responsibility and accountability for compliance in a world of decentralized governance is a key issue consistent with the accountability objective that Commissioner Goldsmith Romero has highlighted for all of the Subcommittee's work, but especially for Digital Assets. It's one of the most challenging issues and also one of the most critical. It's needed to ensure responsibility and accountability for high-risk, highly sensitive activities. In particular, decentralization on end-automation, challenge the ability of policymakers to effectively target regulation and apply conventional regulatory strategies and levers in these ecosystems.

We also see that policymakers will have to address issues related to regulation involving software and the inherent First Amendment arguments that we've seen being raised in this space, as well as determining entities and personhood.

So there's a variety of other issues. The

last two that I'll underscore relates to ensuring DeFi lives up to critical policy objectives. Policymakers will continue to grapple, likely with the issue of scaling, practical application of regulation and enforcement to shape a sector into compliance early within its development.

Scaling the amount and timeliness of enforcement is already difficult for TradFi spaces, where you have lots of international partners that are regulating successfully. And in a world of DeFi, where the rest of the world has taken mostly no action, or certainly insufficient action to properly regulate even in areas where there have been for years, international standards related to regulation is going to be a serious issue.

Timeliness of enforcement is further complicated by complexities of DeFi models, identifying responsible entities, and continued growth of global reaching operations.

And then, finally, fostering a robust and constructive dialogue with industry. Currently, dialogue between policymakers and DeFi industry is

not always characterized positively and is often characterized by vitriol and defensiveness. In the most extreme instances, this does not characterize what we've seen in the Subcommittee, certainly -- but in the most extreme instances, you see opponents that offer little-to-no acknowledgment of the dangers of ignoring timely action on payment systems innovation happening worldwide or the benefits that the technologies could manifest if properly regulated and enforced.

On the other extreme, you have proponents that are voicing overly sanguine praise to an immature sector that has implemented haphazard designs at times that took no account for the kinds of controls that you need in place to defend consumers and systems.

So this presents a serious problem. So direct, deliberate, and prioritized engagement to foster robust and constructive dialogue between policymakers and industry is critical. Next slide, please.

The Subcommittee mapped out different

considerations that we hope that policymakers will account for in thinking about the appropriate regulatory response. It requires, when thinking about the tech stack and the different players that exist inside of the DeFi ecosystem, and where obligations should exist on putting -- whether it's controls on participation, whether it's reporting, whether it's monitoring activities or recordkeeping, thinking about where to impose the obligation.

It's important for policymakers to consider what is feasible, what is proportional based on the nature of the risk and understanding it thoroughly. What is the most useful to support regulators and law enforcement in achieving those policy objectives. And then, also how costly is that based on burden imposed and inefficiencies being minimized. Next slide.

And then, we also identified issues for industry as we talked about, this is not just a policymaker's obligation or responsibility to ensure responsible development in DeFi. Industry

has responsibility for promoting leadership and technical standard setting and infrastructure and solutions development. This is a primary mandate for industry and where the government can play a role in helping to convene and to help codify standards under agencies, like NIST.

But, ultimately, standards are not built in a vacuum. They are built upon industry coming together and coalescing around what are those best practices and standardized approaches that should be taken into account. So this is a place where industry should be taking leadership.

Incorporating regulatory considerations into an early stage, and also building dynamic regulatory compliance. If we can go to the next slide.

This really emphasizes the point that compliance is totally possible. I remember years ago when there were parts of industry that were claiming that it was impossible to build in compliance. And now we've seen many reg tech companies, including many members of the

Subcommittee, that have shown that that's not right, that there's ways to be able to monitor and leverage the information and capabilities in DeFi in order to ensure compliance and ensure more maturity inside of the space.

Again, I won't go through all of these the same way that Dan did earlier when going through our tech stack. But this particular iteration of this chart highlights different examples of technical features and controls. It doesn't have to be these. These are only meant to be illustrative.

But there are a lot of different mechanisms that can be built in at different layers of the stack that can help to mitigate against certain risks. Next slide.

And then, finally, we'll move on to our recommendations that the Subcommittee put together.

So we really created a framework, as Dan mentioned earlier, that works for approaching any issue. You start with understanding the issue, resource assessment, data gathering and mapping,

needing to ensure an understanding of what are the DeFi ecosystems. Who are the players? What are the functions that are ongoing? And assessing their own capability to address and understand these spaces. Whether it's building human resource talent, acquiring tools, ensuring training and ongoing capacity to monitor and understand the risk there.

Surveying the existing regulatory perimeter is our next recommendation. This requires a true, comprehensive understanding of all the regulatory touch points, from the federal to the state level, assessing our own perimeter against international approaches, and then mapping and understanding how the regulatory perimeter maps against risks and where there are gaps. Then looking next in the risk identification, assessment, and prioritization, where there's gaps needing to catalog and map who those players are that potentially could have access to the kind of information or be able to exert the kind of control and influence that you need in a system to impose

what's needed to mitigate the risks that were identified. Next slide.

And the closing portions of our recommendation point to identifying and evaluating the range of potential policy responses.

There's a lot of tools that regulators have available to them. Like I mentioned, it can be things like reporting obligations, control of access to certain systems, and participation in markets, reporting, and recordkeeping. There needs to be an inventory of all those authorities that exist to mitigate risks. And then going to Congress, where additional authorities are needed to be able to successfully mitigate those risks.

And then, finally, fostering greater engagement and collaboration with domestic and international standard setters, regulatory efforts, and DeFi builders.

So all of these point to and give very concrete, discrete actions for recommendation inside of the report on what we propose that policymakers undertake in order to successfully

understand the nature of all the risks presented by DeFi and to address them. Next slide.

And then in closing, we applied that framework. Next slide. Thank you.

We applied that recommendation to a specific issue, which Commissioner Goldsmith Romero also underscored in her opening remarks, the issue around illicit finance and anti-money laundering concerns related to DeFi. DeFi continues to be exploited by cybercriminals because of insufficient security controls, and then, also because of weaknesses in identity and anti-money laundering regime application across the DeFi institutions.

So it's those vulnerabilities in identity and being able to hold accountable bad actors that currently make DeFi attractive to illicit actors that is not inevitable. Again, we discussed earlier, compliance is possible. Identity can be built-in across these ecosystems. And so, we applied the framework that the Subcommittee had drafted earlier to identity and making recommendations about concrete, specific actions

that the U.S. government and policymakers could consider related to building the right infrastructure for identity in DeFi.

So that concludes our discussion of the report. Thank you guys so much for entertaining our discussion of the incredibly comprehensive work that the Subcommittee put together on this report.

I really do think it's the most comprehensive assessment of risks and opportunities that certainly I've seen. So I'm honored to have been a part of that work for the Subcommittee.

And at this time, I'd like to open the floor to questions, comments, and discussion from TAC members.

Todd, I know you might have had some comments about cybersecurity, we were talking a bit before the session.

(No response.)

CHAIR HOUSE: Would any of the Subcommittee members who participated in drafting the report like to make any comments or remarks about the report as we drafted it and the recommendations?

Yes. Jonah.

MR. CRANE: Thank you. I mostly want to thank you and Dan, Carole, for the tremendous work you guys did in pulling together lots of ideas from lots of people, many of which conflicted in various ways and pulling it all together in, you know, a piece that is really coherent.

And Dan, you used the word ambitious, and this is an incredibly ambitious report, trying to really remap the DeFi ecosystem in a way that I hadn't seen done before anywhere else.

There are lots of papers and lots of prior research done on this from government bodies and others, a lot of which you all, and we all reviewed in the process of putting this together, but sort of rethought it in a new way and really sort of broke it down. I think all the different dimensions of decentralization that you pulled into this and being able to think clearly about risks and opportunities and new use cases along all of those dimensions was really helpful and important.

There's just so much to chew on here. I hope

folks who read it and really digest it in that spirit. And so just kudos to you for taking on such an ambitious project, pulling together so much feedback and bringing it all together in a way that, like I said, really provides a lot of different frameworks for people to think about DeFi through. So thanks.

CHAIR HOUSE: Thank you so much, Jonah. Justin.

MR. SLAUGHTER: Thanks, everyone for this.

I just want to echo Jonah and say I think this is perhaps the most nuanced, thoughtful report I've seen so far on pretty much any subject in crypto, but especially DeFi. We're getting on almost four years since DeFi Summer, and I think this is the first time I've seen a document from the government that engages the views of everybody across the ecosystem, from people who are in the industry, to people who are investor advocates, to people who are pro-industry crypto, and skeptical of crypto and DeFi.

And this really represents a chance to get

some building blocks for policymakers to understand how to wrap their arms around this hard, novel question.

I also really want to thank you, and Dan, in particular for the idea of the spectrum of DeFi. Not everything that is said to be DeFi is DeFi. There's a lot that has been discussed that's DeFi in name only.

And I think this report really gets across ways for the industry to strive toward greater decentralization and toward fulfilling the promise of those opportunities while taking into account some of the risks that are attended to any new technology like DeFi. So I'm very grateful for the time and effort that was put into this. I think it's a real big step forward for everybody.

CHAIR HOUSE: Thank you so much, Justin, and for your contributions to the report as well.

I see Vice Chair Redbord, you had your flag up, and then we'll go to Dan Guido online.

VICE CHAIR REBORD: Just very, very quickly.

And thank you, Justin, for that really

extraordinary comment. I agree with all of it.

I think one thing that's really important in terms of the recommendation section in this report is it really is the beginning of a conversation and a conversation that specifically calls out DeFi builders. In other words, the industry, policymakers, and others with an interest and expertise in the space to really have a conversation about what the regulatory perimeter is today, how it can be expanded.

So I see this obviously as a very detailed, intricate report, the most ever, arguably, on the topic. However, really just still the opening of a much broader conversation.

So I will stop there. I think Dan has his hand up and we can sort of move along there.

CHAIR HOUSE: Thank you so much, Ari. Dan, and then, we'll move on to Steve.

MR. GUIDO: Thanks. I think the report is great. It's comprehensive. It's one of the better, if not the best one that I've seen.

I do just want to flag attention to one

specific part of it, which is the immense software security challenge that is present when developing things like DeFi. I think when people develop traditional software; we have a vulnerability mitigation approach. We take a best effort towards identifying vulnerabilities in that software and do our best to reduce the risk of those affecting the software in the future.

And if there are issues that are discovered, you do things like threat detection in order to figure out when things may have been hacked. You issue patches and software updates, and those techniques work great for traditional software, but they do not work great for DeFi. So a lot of people in the financial industry are familiar with that former sort of strategy.

But the strategy that's required to build software that is safe for DeFi reflects more of a safety critical approach, where you're developing software that needs to work once and never fail, or else it sinks your ship or more accurately, blows up your rocket to the moon. Right?

You wouldn't be able to launch a satellite into space with the same sort of software development approach that you write a typical web application or SAS technology service.

So I think that this is a major shift for people in the financial industry and for financial regulators, as well. It looks more like how NASA might want to oversee how we get to space than how the CFTC or other regulatory agencies have regulated financial institutions in the past. This is really safety critical software, and it necessitates a different approach.

So as we look at what the next steps are after this report, that is one area that I think is particularly treacherous, since it is such a large divergence from what is the typical standard for cybersecurity in other fields.

CHAIR HOUSE: Thank you so much, Dan. I really appreciate those insightful comments and that term, safety critical software. I think that really underscores the importance of when DeFi is engaging in incredibly sensitive and highly risky

activity. It demands the level of security that I know you focus on a lot in your day-to-day work and have long in your career. So thank you so much for those comments, Dan. I appreciate it. Steve.

MR. SAPPAN: Yeah, thank you for the presentation of the report. I had a few concerns that probably relate to my limitations as somebody who's largely worked on CFTC rules and not on DeFi.

One of them is going to be that your traditional financial entities and markets are going to take a look at this report, just as regulators are. And they're going to say, for example, will these DeFi platforms be required to comply with the CFTC's core principles? And if not, that's a competitive disadvantage for me. Right?

So I don't think there's any attention in the report to the issue of competition with traditional finance.

Another thing that concerned me was when I looked at how you built the definition, the working definition of DeFi, the part of the quote from the

Bank for International Settlements that was left off was, "-- and that has no safety net." Right?

The exchanges, the mega-banks, they have the Federal Reserve as the safety net.

And since you have all of the DeFi apps, or most of the DeFi apps, built onto one blockchain, that to me seems like a structural vulnerability. And if something goes awry with that blockchain, what then happens to the apps and to the customers that are using the apps. I mean, there would be no doubt that in the case of emergency that Congress would arrange some kind of bailout, but it would be very ad hoc and much more difficult to structure than the $29 trillion of emergency loans that the Federal Reserve arranged for the mega-banks and a few insurance companies.

So those are a couple of considerations. I don't want to continue to take up discussion space here, but I think there were some issues.

Oh, there was one last thing, in case I don't get to speak again. Throughout the report, DeFi is referred to as a nascent industry. And I don't

have any sense from the report about what use case is mature.

As I understand it, it's largely payment systems that are mature. But I don't know about the other use cases, if those are considered to be -- maybe those are just understood within the DeFi industry, what this kind of scaling and maturity is. But that might be something to add to the report prior to discussion with financial regulators who may not be familiar, as I am not, with DeFi. Thank you.

MR. AWREY: Thanks, Steve. Just to respond to a couple of those points before we go to Sunil.

And this may be just a question of language, your first question, which I think is extremely important, would a DeFi actor have to comply with the CFTC core principles? Is absolutely part of the mapping exercise that we think needs to take place.

We don't think conventional finance should be asking that question. We think the CFTC should be asking that question. We think government should

be asking that question, because it's hugely important.

And where this fits in or doesn't with existing regulatory frameworks is kind of the broader message here, that what DeFi calls something is kind of irrelevant in this process as compared to what it does. And unfortunately, the U.S. regulatory system is based on a whole bunch of labels, and all of those labels have conventional financial system connotations, and all of them have very path dependent regulatory structures. But technology changed, and whether the technology works or not is an open question.

But the fact that people are trying to do the functions technologically in a way that doesn't map onto traditional regulatory categories, is precisely the nature of the challenge that this report is trying to get at the heart of and why we think it's only the first step. Because if you think of the federal code alone, the amount of questions that need to be asked, in addition to CFTC core principles, is enormous.

And I don't mean to make light of that process, but you have a technological shock, and that's the process you have to undertake.

Part of the approach of this report is the world didn't stand still as some people might have wanted it to. And the world having revolved on its axis now means that we have to update our models of the way that the world works and the way that the law approaches the opportunities and challenges created by that.

So I think, actually, Steve, we may have just crossed paths in the night on that, because I think your question is an important question, and it's not just JPMorgan that should be answering it.

Second, on the safety net point, we do include the full quote in the actual report, just not on the slides. And I do think that this is also another important aspect of this. Right?

This is why we're talking about the dimensions of decentralization. Because in your world, where everything runs on one blockchain, right? I've just created the “Pudd’nhead Wilson” problem of,

I'll put all my eggs in one basket now, and now I have to watch that basket again.

And, as at least conceived in theory, the diversification argument, the heterogeneity argument for DeFi is that you're not ending up in that world. And I think that the Subcommittee, if I can speak for them, was cognizant that if we do end up in that world, that's not what the opportunities of DeFi were ultimately about. That's the opposite of that.

And then lastly, in terms of use cases, your point is well-taken. And I really do think one of the limits of the subcommittee process is that we don't have the firepower, really, to canvass the entire universe of DeFi projects and understand this at a systematic level. And we definitely encourage further work, whether it's part of the TAC, or broader and more inclusive groups within government and civil society, to continue to press at that question, because it's an incredibly important one.

CHAIR HOUSE: Thank you so much, Dan and

Steve, for, again, very insightful comments, and I appreciate, especially underscoring the issue of no recourse that is presented through features like automation and immutability in the system that make inserting changes that are needed to adapt with shocks and to address issues and risks in the system.

I know we gave a lot of voice to that in the report, so I appreciate you underscoring it as an issue. Sunil.

MR. CUTINHO: Can you hear Carole?

CHAIR HOUSE: Yes.

MR. CUTINHO: Okay. I think I was going to actually respond to Steve. I want to actually thank my fellow Subcommittee members, Carole and Dan, because we had a rigorous debate when we discussed risks. DeFi, we cannot call it an objective good all the time because there are instances, there are situations in markets, especially when exposures span more than an instant and they go beyond an instant. Let's say they last a day, week, year, or a month. A decentralized

system doesn't really hold up. It's not resilient and there is a footnote in the report that addresses that.

So, my comment is that it's very hard for us to use a single report and start carving it out and saying where it makes sense and where it doesn't. So I think the report is structured to introduce the topic, and then its recommendations are about studying it more deeply and figuring out the true vulnerabilities and situations in which it makes sense and situations where it doesn't make sense.

CHAIR HOUSE: Thank you so much, Sunil. To your comments now, as well as to your incredible input during the whole subcommittee process, I really appreciated everything that you brought to the report.

And I also, just wanted to especially underscore, you're right, I do think that it starts the process. The Subcommittee, we all put together at the end of the report in the recommendations, we didn't just put together specific actions for policymakers to take, but also key questions that

we feel need to be addressed by policymakers in that. So while it was certainly tough for all of us, it was lots of work to put together this report. The real tough work is ahead for policymakers and industry to figure out how to implement it.

Hopefully, our recommendations can help guide them as they think about how to approach the risks and policy objectives related to DeFi. Thank you so much, Sunil.

Are there any other comments from the floor?

Nicol.

MS. TURNER LEE: First and foremost, I want to thank the committee for a very thorough report, and one which I think will serve as a model for future reports coming out of this full advisory.

I just wanted to make a comment, which is more so, I do appreciate some of the flexibility that is embedded in the reports crafting. And I'm also appreciative of the call-out of the DeFi system as it relates to communities of color who are loosely connected to financial markets, particularly when

it comes to intermediaries.

And I would just be remiss by not suggesting in my comment, pretty much along those same lines of my colleague, that we encourage the CFTC to have more conversations around the alignment of those who are not necessarily fully engaged in financial markets due to race or discrimination, implicit or explicit. But how the DeFi industry, basically, has allowed for entry for entrepreneurs and others to actually be connected to those.

So I did acknowledge the conversations that you did have in the report around just better access to more affordable financial services.

And I would be remiss to not encourage this Commission and this committee to continue to explore how it relates to those who just have less formal connections to financial markets in ways where DeFi has benefited them and created greater access without intermediaries.

CHAIR HOUSE: Thank you so much, Nicol. I really appreciate that. And I know that that issue of inclusion and equitable outcomes is a huge part

of the work that you and Todd are driving in the Subcommittee for Emerging Technology. So I appreciate you referencing that for us.

I know we, in the Subcommittee for Digital Assets, we're excited to point to that as an issue that could be a potential opportunity in driving more inclusion, but also a potential risk if not accounted for properly. Because inclusion in a system that doesn't have proper controls for consumers and to ensure those equitable outcomes is not, in fact, a financial inclusion desirable outcome.

So thank you so much for that. I really appreciate that and your leadership. Thank you. Nicol. Any other comments from the floor?

Great, Joe, thank you.

MR. SALUZZI: And thank you for the great work.

I mean, it really was very comprehensive, and for somebody like me, who's a novice in the industry, it was a lot to learn there.

Question for you, both. Years ago, I was on a

subcommittee for the CFTC, and our task was to define high frequency trading. And I was on a subcommittee with, I think it was seven or eight other industry participants, and everybody had their own angle. Everybody had a say because their business was depending really on this definition, which I didn't really realize at the time.

They wanted to take this thing and move it forward to other committees and other things, and they would say, “Oh, look at the definition. Rely on the definition.”

So, I dissented. I made a public dissent on it because there was one word in there I didn't like. It was about a number of orders that were being placed.

So I'm wondering, the question I have, and there's a question here, was there that type of dissent in the committee anywhere? Was there a word anybody got hung up on? Was there a competing interest that people battled with?

MR. AWREY: It's a great question. I'm not sure there was a word, but I think there was

debates over approach and you can see that on the one hand, definitions help market participants understand what their obligations are.

Am I subject to this rule? Am I not subject to this rule?

So having a definition there becomes something, that a legally applicable tractable definition, is something that is desirable on the one hand.

On the other hand, if the thing underlying the definition is so diverse that to lump everything together into one definition and the legal path dependency that comes from that, then you're probably going to get a lot of square pegs being tried to put into a lot of round holes. I think that was the cut and thrust of our debate, a fair bit. It's ultimately why we have two definitions in there, in a sense.

One that is, I think, the aspirational definition of what decentralized finance hopes to achieve. The other one is a more granular definition looking at different dimensions. In

some sense they're in tension, in some sense having two definitions, I think, helps frame conversations like this about the meta-question of whether decentralized finance is something we want to regulate, or whether decentralized finance raises a whole bunch of issues that we want to regulate.

CHAIR HOUSE: Yeah, I appreciate that. Dan, of course, is totally spot on. And I also really appreciate the nature of that question, because the definitional issue was a core one, and I think that where ultimately the Subcommittee all agreed and came out was reflective of our intent to make sure that we provided some help to policymakers and to frame the discussion, but not provide an exact line.

The issue on the spectrum of decentralization, there are some that recognize that it could be very helpful for policymakers, and especially for industry calls to say, “This is the amount of decentralization that make you not regulated.” That is something that many in industry have called for and asked for clarity on.

And honestly, that is not a one size fits all approach, because each system is different in decentralization. All the different dimensions that we outlined ultimately make it impossible and impractical to come up with a very specific, consistent definition. But there was a lot of discussion that led up to that ultimate finding of like, “Well, this is the way that we have to approach it.”

So I think that issue, especially on how specific can we be? What is the right approach to take in creating that definition and providing something that's a helpful framework for both industry that's trying to figure out how to compliantly and securely create in this space and operate, as well as policymakers who are trying to think of, “Gosh, how do I impose obligations and identify responsible parties?”

That was as close as we could get in this current report, but it is meant to be sort of the beginning of a conversation and not something that translates into a legal definition.

Great question, Joe. Thank you. I see, Justin?

MR. SLAUGHTER: Yeah, I just want to echo that and say, Joe, thank you for your service on that HFT process seven, eight years ago. That was on my mind as we did this.

I'm not aware of a particular word we focused on. Instead, what I think actually happened is we recognized it's beyond our abilities and probably a power we don't want to wield trying to find what is decentralization for everybody. Instead, I think we didn't give a definition as much as we gave an approach, one that policymakers may reject, but at least begins the process of wrapping our arms around this.

And I didn't sense a lot of opposition to that because it's designed to be a flexible signal rather than to be a dictate from heaven.

CHAIR HOUSE: Thank you so much for that, Justin.

Any other comments from the floor or from online?

(No response.)

CHAIR HOUSE: Great. We have received a dissenting statement from TAC member Hilary Allen.

Now my Co-Chair of the Subcommittee, Dan Awrey, will now read that into the record to the extent that the TAC votes to adopt the report and submit it to the Commission, this dissenting statement will be provided along with the report.

MR. AWREY: Thank you, Chair House. My apologies to Hilary in advance, I'm sure I will not deliver this as articulately as she would have. And just in case anybody is watching, I'm going to open some quotations here. This is definitely not one academic stealing another academic's ideas.

“I apologize that I could not be there today. Unfortunately, the meeting conflicted with long standing travel plans. I am grateful to the committee leadership for sharing my statement today.

First of all, I would like to applaud the Subcommittee for their hard work on this report. I think the technical descriptions are both accurate

and accessible, and I believe that the report offers perhaps the best identifications and explanations of DeFi risks that I have seen.

In particular, I applaud the authors of the report for resisting the urge to demarcate a level of decentralization that would count as sufficiently decentralized for regulatory purposes. Any such demarcation would inevitably be tied to the state of technology and business models at this moment in time, and would thus provide many fertile avenues for regulatory arbitrage.

The report also does an excellent job of distinguishing between DeFi's present reality from its hyped potential.

Ultimately, however, I cannot support this report's recommendations. I'm concerned that the report stops short of engaging with why much of DeFi's hyped potential is in fact impossible, often because of the realities of economic incentives. At least if it's impossible without DeFi becoming so much like the existing financial system that all the added technological complexity is pointless, as

well as inviting all the new risks that the report articulates so well.

Given these realities, I question the report's recommendations that the CFTC and other regulators expend scarce resources in learning more about and developing bespoke regulatory approaches for something that is unlikely to deliver any new benefits.

To be clear, there are lots of structural problems in the existing financial system, but Permissionless Blockchain Technology is ill-suited to addressing them for many reasons that I've articulated in my new work, ‘Fintech and Techno-Solutionism,’ the report also does not consider where regulatory resources will be diverted from in order to discharge these recommendations.

I think it should be acknowledged that the interest rate changes have made venture funding harder to come by, and much of the venture capital interest that had been driving DeFi experimentation has now pivoted to AI. This reality of decreased commercial interest in DeFi underscores the

concerns that I have about expending scarce regulatory resources on DeFi.

In short, while the report recognizes that DeFi has not yet progressed very far down the spectrum of decentralization. The report should also reckon with the implausibility of it ever progressing far enough to justify large investments by regulators in mapping existing regulatory regimes to DeFi, let alone justifying developing accommodative, bespoke regulatory treatment-like waivers and sandboxes, that would effectively rollback regulations designed to protect the public from harm."

And I just wanted to personally thank Hilary for being such an engaged, if dissenting, voice on the committee. Her work always makes us test our own assumptions and the ways that we think about these issues.

So in absentia, I just wanted to thank her.

CHAIR HOUSE: Thank you so much, Dan. Great. Joe, is that just a legacy flag?

MR. SALUZZI: Yeah, I wish I would have heard

that before, actually. It's just making me think a little bit now, but thank you.

CHAIR HOUSE: Sure. Thanks so much, Joe.

I also would like to thank and appreciate Hilary's expertise, and she's done a lot of work and has a lot of understanding in this space.

In my own just reaction to it, I feel that it's important for regulators to have to address and understand this space. Especially one that has shown that it will continue to develop with or without government intervention, and the fact that it engages in what we've discussed as highly sensitive and high-risk activities.

And the amounts that Commissioner Goldsmith Romero pointed to earlier, these are not trivial or insignificant amounts or risks related to the kinds of harms that they can bring if the risks are left unchecked.

So my own view and position is that it is the mandate and responsibility of policymakers to set guardrails and North stars. And also, something that I think that agencies like the CFTC, have

taken a big leadership role in by setting forth principles and taking enforcement action in the space to show what they expect and demand of actors inside of DeFi ecosystems.

But thanks again to Hilary. Again, even with her dissent, her expertise is very well-noted and I know was cited in our report in a couple of places. Great. Then members, we have now discussed at length the Digital Assets and Blockchain Subcommittee's report and recommendations regarding decentralized finance to further consider these important issues.

Is there a motion from the body to adopt this report and recommendations and submit them to the Commission?

MR. THEN: I move.

CHAIR HOUSE: Thank you, Corey. Is there a second?

MR. CRANE: Second.

CHAIR HOUSE: Thank you, Jonah.

It has been moved and properly seconded that the TAC adopt the Digital Assets and Blockchain

Subcommittee's report and recommendations regarding decentralized finance in full and submit it to the Commission.

Is there any further discussion?

(No response.)

CHAIR HOUSE: Are there any further comments from TAC members on the phone or online?

(No response.)

CHAIR HOUSE: Then, committee members, are we ready for the vote?

(Ayes.)

CHAIR HOUSE: Thank you.

The motion on the floor is for the TAC to adopt the Digital Assets and Blockchain Technology Subcommittee's report and recommendations regarding decentralized finance and submit the report and recommendations to the Commission for consideration. As a point of order, a simple majority vote is necessary for the motion to pass. I will now turn it over to the Designated Federal Officer to conduct a roll call vote.

MR. RODGERS: Thank you, Chair House.

Committee members, when I call your name, please indicate your agreement with aye, disagreement with nay, or indicate abstain if you're abstaining from the vote. As a reminder, abstentions are not counted as a vote.

And I'm going to start by going around the folks that are here in-person, starting with Timothy Gallagher.

MR. GALLAGHER: Aye.

MR. RODGERS: Jonah Crane.

MR. CRANE: Aye.

MR. RODGERS: Todd Smith.

MR. SMITH: Aye.

MR. RODGERS: Nicol Turner Lee.

MS. TURNER LEE: Abstain.

MR. RODGERS: Corey Then.

MR. THEN: Aye.

MR. RODGERS: Joe Saluzzi.

MR. SALUZZI: Abstain.

MR. RODGERS: Michael Greenwald.

MR. GREENWALD: Abstain.

MR. RODGERS: And Jeffrey Zhang.

MR. ZHANG: Aye.
MR. RODGERS: Carole House.
CHAIR HOUSE: Aye.
MR. RODGERS: Dan Awrey.
MR. AWREY: Aye.
MR. RODGERS: And Ari Redbord.
VICE CHAIR REDBORD: Aye.
MR. RODGERS: So moving to the folks online, Nikos Andrikogiannopoulos.
MR. ANDRIKOGIANNOPOULOS: Aye.
MR. RODGERS: Todd Conklin, he may have dropped off. Sunil Coutinho.
MR. CUTINHO: Aye.
MR. RODGERS: Jennifer dropped off.
Ben Milne.
(No response.)
MR. RODGERS: John Palmer.
(No response.)
MR. RODGERS: Michael Shaulov.
MR. SHAULOV: Aye.
MR. RODGERS: Steve Suppan.
MR. SUPPAN: Abstain.

MR. RODGERS: Dan Guido.
MR. GUIDO: Abstain.
MR. RODGERS: And Gün Sirer.
MR. SIRER: Aye.
MR. SLAUGHTER: Some of us weren't called yet, I think.
MR. RODGERS: Okay, apologies. Yes. Folks have shifted around, so Justin Slaughter.
MR. SLAUGHTER: Aye.
MR. RODGERS: And is there anybody else online that I have not called?
MR. CATALINI: Yes, Christian Catalini? Aye.
MR. RODGERS: Oh, sorry. Christian Catalini. Thank you very much.
Okay, Chair, you have 14 yes votes, zero no votes, and five abstentions.
CHAIR HOUSE: The ayes have it and the motion carries. The Digital Assets and Blockchain Technology Subcommittee's report and recommendations regarding decentralized finance have been adopted by the TAC and will be submitted to the Commission for consideration.

MR. RODGERS: Thank you. It is now time for closing remarks from Commissioner Goldsmith Romero.

COMMISSIONER GOLDSMITH ROMERO: It's great to have everyone here today. These are very complex, challenging issues that are always informed by debate from a broad and diverse group of stakeholders and I appreciate all the dedication that I'm seeing from each of you who care passionately about these important issues. Particularly when it comes to customer protection and protecting our markets from things like illicit finance and financial instability.

So I'm grateful for everyone for their work and look forward to continued engagement on these issues.

I'm particularly grateful for everyone on the Subcommittee, you worked very hard. And to the Subcommittee here on Digital Assets and Blockchain for putting the work towards this report so that there is a foundational kind of understanding of DeFi as a first step that could help with further engagement in this area.

And so, with that I'll say thank you to everyone on the committee, as well as to our leaders.

Thank you so much, and I appreciate your work.

MR. RODGERS: Thank you, Commissioner. And thank you, Chair Carole House and the leaders of the committee. I want to thank everyone for attending our first TAC meeting of 2024. The meeting is adjourned.

(Whereupon, at 4:13 p.m. EST, the meeting was adjourned.)