Ceres Accelerator
for Sustainable Capital Markets

June 3, 2022

Martin J. Gruenberg, Acting Chair
Federal Deposit Insurance Corporation
550 17th Street, NW
Washington, DC 20429
Via Email to comments@fdic.gov

Re: RIN 3064–ZA32 – Request for Comment on Statement of Principles for Climate-Related Financial Risk Management for Large Financial Institutions

Dear Acting Chair Gruenberg,

It is a pleasure to submit comments on behalf of Ceres and the Ceres Accelerator for Sustainable Capital Markets. Ceres is a nonprofit organization with over 30-years of experience working on climate change. The Ceres Accelerator works to transform the practices and policies that govern capital markets in order to reduce the worst financial impacts of the climate crisis. It spurs capital market influencers to act on climate change as a systemic financial risk—driving the large-scale behavior and systems change needed to achieve a just and sustainable future and a net zero emissions economy.

Ceres works with leading global investors and companies. Our Investor Network is currently over 220 investors that collectively manage over $60 trillion in assets. Ceres is a founding partner of the Net Zero Asset Managers Initiative and the Paris Aligned Investor Initiative, which includes investors focused on sustainable investments within their portfolios and other assets. Our Company Network includes approximately 60 of the largest global companies with whom we work on an in-depth basis on climate strategy and disclosure, among other issues.

We congratulate the Federal Deposit Insurance Corporation (FDIC) for designing this Statement of Principles for Climate-Related Financial Risk Management for Large Financial Institutions (Principles or Climate Principles). We also commend the FDIC for the preliminary research the agency has initiated on climate-related financial risk, its establishment of the interdisciplinary Climate Working Group, and the recent interagency

Notice of Proposed Rulemaking (NPR) to update the Community Reinvestment Act (CRA) regulations, which includes climate resiliency considerations. We also recognize that the OCC issued substantially similar guidance for comment in December 2021. There would be great benefit in the FDIC, OCC, and Fed working together on consistent climate principles. Issuance of uniform, binding guidance by the three banking agencies could avoid regulatory inconsistency, send a strong signal to the banking industry, and ease compliance costs for regulated entities.

Below, we provide our comments to the questions posed in the Climate Principles. We have also included an attachment containing operational and tactical recommendations previously submitted to the FDIC meant to further support your vital work on climate and the investments required to address the FSOC report recommendations (please see Attachment 1). Because this memo was submitted in December 2021, we note that the FDIC has already taken some of these suggested actions.

Applicability

1. What additional factors, for example asset size, location, and business model, should inform financial institutions' adoption of these principles?

We agree with the FDIC that all banks, regardless of size, may have material exposures to climate-related financial risks. Furthermore, although these Principles closely track the FDIC's existing management for large banks, they target only those banks with over $100 billion in total consolidated assets (i.e., the largest financial institutions).

While this may be a reasonable starting point, all financial institutions face climate-related financial risks, not just those over $100 billion in assets. The FDIC's rule requiring certain insured depository institutions to submit resolution plans has a threshold for banks with over $50 billion in total assets due to the understanding that the failure of such institutions would have serious adverse effects on financial stability in the United States.[1] Additionally, regional banks may experience higher rates of failure and closures due to lower diversification and geographical concentration. Ceres hopes the FDIC will utilize the $50 billion threshold, as these institutions already employ sophisticated risk management

[1] *See* 12 C.F.R. § 360.10.

practices and should thus be capable of incorporating climate-related financial risks into their risk frameworks.

Ceres believes that climate change risk permeates all aspects of the capital markets, similar to cyber security risks and the coronavirus pandemic, posing grave threats to banks of all sizes and business models. Moreover this risk is only increasing in terms of frequency and severity. According to NOAA, in 2021 there were 20 separate weather and climate disaster events where losses exceeded $1 billion. Furthermore, these climate disasters killed 688 people and cost the United States more than $145 billion last year.

These acute and progressive physical risks have the potential to seriously disrupt the bank market as well as the communities they serve. For example, more than 40 percent of Americans live in counties hit by climate disasters in 2021 and more than 80 percent of Americans experienced a heat wave. Climate impacts are already manifesting in the largest state economies. In just the last few years, California has experienced recording-breaking wildfires, in both number and size, that have taken hundreds of lives, bankrupted the state's largest utility, left millions regularly without power and brought home insurability into question. Florida is facing rapidly rising sea levels and now-routine flooding that are eroding coastal property values and wiping out freshwater supplies.

Climate risk is an existential threat and, as recently stated by the thoughtful and comprehensive October 2021 Financial Stability Oversight Council (FSOC) Report on Climate-related Financial Risk, is one that poses an emerging and increasing threat to U.S. financial stability. As such, we recommend that these principles be adopted by all U.S. banks irrespective of asset size, location, or business model.

Tailoring

2. How could future guidance assist a financial institution in developing its climate-related financial risk management practices commensurate to its size, complexity, risk profile, and scope of operations?

The FDIC has designed these Principles to target the largest financial institutions, although it acknowledges that "all financial institutions, regardless of size, may have material exposures to climate-related financial risks." In general, Ceres recommends that, as financial institutions and the FDIC become more adept at incorporating climate-related financial risk management practices, the FDIC lower this threshold to include more than the

largest banks over time as these standards evolve. However, we acknowledge that smaller banks, community banks, and credit unions have different capabilities than the largest banks. The FDIC should therefore tailor its approach to accommodate for those size, complexity, risk profile, and scope of operations differences.

To this end, Ceres suggests the FDIC implement an assessment program similar to the Federal Financial Institutions Examination Council's (FFIEC) Cybersecurity Assessment Tool (CAT), which was launched to assist banks and examiners determine a bank's risk profile and level of cybersecurity preparedness.[2] The FDIC should develop a similar assessment tool for climate-related financial risk, providing resources to help banks understand supervisory expectations, how climate risks relate to traditional financial risks, and assess and manage those risks. Like the CAT, this could include a pilot program at smaller institutions to enable state and federal regulators to assess how these institutions manage and mitigate climate risks. Based on this program, the FDIC should publish its observations, including findings regarding inherent climate-related financial risks and institution preparedness.

Moreover, Ceres recommends that the FDIC consider using the data it collects from this program to develop a self-assessment tool to assist smaller institutions in evaluating those risks and their risk management capabilities. To reflect evolving science and scenario analysis with a focus on risk management, collaboration, and resilience, the FDIC should continue to update and publish new data it and the other financial regulators obtain and/or analyze. This would allow the FDIC to tailor its guidance for smaller institutions, and enable those institutions to develop climate-related risk management practices without presenting an undue burden.

Similarly, the FDIC should consider updating its examination manuals to account for climate-related financial risks, and/or issue an examination manual dedicated to the identification and management of climate risks based on established risk factors that are very familiar to financial institutions and examiners. While in the process of amending or issuing a new manual, the FDIC could start by issuing a new booklet, publishing a policy statement, or addressing the topic in the periodically published Supervisory Insights or

[2] *See* Attachment 1, Appendix A.

FDIC Quarterly. Likewise, the FDIC should continue to include climate risk as a risk that may affect financial institutions or the Deposit Insurance Fund in its annual Risk Review. These updates as well as the FDIC's interactions with examiners should be based on financial institution size and business line.

Ceres also recommends that future guidance assist banks in factoring the climate change-related transition, physical, and reputational risks of their borrowers into their capital, loan pricing and credit allocation decisions. We believe it is important that large banks do so on a sector-by-sector basis, with consideration given to the unique transition risks (including legal and reputational) and physical risks inherent in each industry sector and client vertical. We note that some large banks have already developed climate-related financial risk management practices in line with this guidance. For example, in December 2021 Citi CEO Jane Fraser stated that Citi will start asking its clients to measure emissions and that a borrower's climate impact will factor into lending and capital allocation decisions. In fact, the January Citi TCFD report addresses some of these issues. Likewise, banks must develop the ability to assess if climate-related transition and physical risks will cause certain assets (including trading book assets) to become so illiquid that they are effectively "stranded." Future guidance should assist banks in developing plans to unwind such assets, or set aside more capital against these potential "stranded assets."

Further, FDIC should provide guidance as to how climate-related financial risks relate to the CAMELS framework. Climate risk could be treated as a cross-cutting risk that manifests through these well-recognized and established types of risk. Capital and asset quality could be significantly affected by both transition and physical risks, particularly where an institution has geographical or sector concentrations vulnerable to these risks. Management's ability to adequately assess, plan for, and mitigate these risks, including through access to appropriate and timely data to measure the bank's exposure, could be factored into the management component. Earnings and liquidity could also be implicated where a bank has made significant amounts of loans to sectors that are heavily reliant on fossil fuels and the bank (and its customers) has failed to adequately plan for transition or the bank's loans are supported by collateral increasingly at risk from severe weather events and rising sea levels.

Additionally, current approaches to climate risk modelling by large banks, treat climate risk in a manner analogous to credit risk. By this we mean that climate risk is quantified using sophisticated models, and capital or risk limits are adjusted to account for this risk. For banks without these capabilities, or where the cost of implementation would be prohibitive, we suggest that future FDIC guidance treat climate risk in a more prescriptive manner similar to its operational risk guidance on cybersecurity. This approach could involve requiring in-scope banks to assess underwriting of climate-sensitive industries, and in some cases recommending the complete withdrawal of lending activity from high GHG-emitting sectors where the assessed risk threatens a bank's safety and soundness.

Finally, Ceres recommends that future guidance for banks and bank holding companies involved in the trading and marketing of non-renewable commodities (including physical energy commodities and physical energy commodity derivatives) include a requirement to disclose the impact of climate-related risk drivers (including operational risk) around these products and services.

General

3. What challenges do financial institutions face in incorporating these draft principles into their risk management systems? How should the FDIC further engage with financial institutions to understand those challenges?

Ceres maintains an active and regular dialogue with U.S. banks of varying asset size, location, and business model. Moreover, most of the U.S.-based G-SIBs are members of Ceres' Company Network. Based on our interactions, many of the largest banks currently use some form of climate-risk scenario analysis and/or climate-risk stress testing to evaluate the transition and physical risks associated with their lending portfolios. The main challenges they face in incorporating these principles into their risk management systems are technical in nature.

For example, even with considerable client engagement, they face difficulty in obtaining borrower-specific climate data (for example, GHG emissions), and are therefore reliant on third-party data to provide index information. In some cases, they are unsure of which climate scenarios are most relevant for their business model, or the most relevant scenarios do not provide sufficient detail in some areas critical to financial institutions.

Ceres also recommends that the FDIC be clear that having a transition plan is a crucial part of a bank's risk management system, and provide guidance as to how these plans should be formed. When making loans, financial institutions should request data from counterparties, including governance policies, physical and transition risks, and Scopes 1, 2, and 3 GHG emissions. Obtaining this data will become easier if the SEC's proposed climate disclosure rule for public companies comes into effect, as it will allow all financial institutions to gain more comprehensive and consistent information from their clients.

4. Would regulations or guidelines prescribing particular risk management practices be helpful to financial institutions as they adjust to doing business in a changing climate?

Although the FDIC's current consultation seeks to promote a principles-based approach to improving risk management and supervisory practices related to climate-driven financial risk, we would encourage FDIC to consider making some or all of these prescriptive and enforcing them as mandatory requirements as opposed to voluntary best practices.

We believe the FDIC should use its authority under Section 39 of the Federal Deposit Insurance Act, specifically 12 U.S.C. § 1831p-1, to finalize this guidance and issue the final document as binding safety and soundness supervisory guidelines. Such binding regulations or guidelines would be beneficial as they would assist financial institutions in understanding what the FDIC and examiners are looking for. It would also make clear that climate-related risks are a safety and soundness concern, and would give the FDIC a legal basis for requiring banks to make necessary changes and bring enforcement actions for noncompliance. After these guidelines are finalized, the FDIC should continue to create more in-depth requirements.

It is important to note that the European Central Bank, the Bank of England, and other foreign financial regulatory agencies are already taking these steps.[3] The FDIC should make use of the data these prudential authorities and their regulated entities have already collected and analyzed, including scenario analyses and stress tests.

[3] Central banks that are beginning to regulate climate-related financial risk and/or plan mandatory scenario analyses include the European Central Bank, England, France, Australia, the Netherlands, Japan, Singapore, and Canada.

Current Risk Management Practices

5. What specific tools or strategies have financial institutions used to successfully incorporate climate-related financial risks into their risk management frameworks?

Many financial institutions have identified specific tools and/or strategies in at least some detail in their general reporting, integrating climate risk into existing risk types and systems rather than treating it as a separate risk. When banks are unable to quantify risks, they have reverted to describing the risks in qualitative terms, which we would consider a minimum threshold for climate risk management.

6. How do financial institutions determine when climate-related financial risks are material and warrant greater than routine attention by the board and management?

The FDIC should provide clear guidance on the minimum requirements to conduct a materiality assessment. In conducting these assessments, financial institutions should be required to report their results, including what data was used in the assessment to allow comparability across sectors, and an explanation of why information was determined material or not. Banks should also focus their assessments on financial opportunities as well as financial risks. Information banks should consider in making materiality assessment include context-specific metrics such as asset locations, local laws, and geographical information. Determination of whether such climate-related financial risks are material should mirror those determinations made in other risks assessments by a bank.

7. What time horizon do financial institutions consider relevant when identifying and assessing the materiality of climate-related financial risks?

Ceres research from 2019 shows that only one of nine banks studied is looking at a risk management time horizon longer than five years. Two others are looking longer term with respect to climate risk, but not for more conventional risks like credit risk or market risk. While there may have been some movement toward long-termism in the last two years, most banks are still focused on the one- to five-year time horizon. It is clear that to fully understand the climate risks banks face to their safety and soundness, they need to look at a longer time frame. In 2020, Ceres produced a report highlighting the risk due to transition risks of the largest banks. In 2021, we prepared an analysis of the physical risks of climate

change to banks. Both of these reports highlight the imperative to have a longer time frame in the analysis.

8. What, if any, specific products, practices, and strategies – for example, insurance or derivatives contracts or other capital market instruments – do financial institutions use to hedge, transfer, or mitigate climate-related financial risks?

Based on Ceres' interactions, many of the largest financial institutions have used, or have considered using both insurance and carbon offsets to mitigate climate-related financial risks.

Regarding the use of insurance contracts, we believe that the residential mortgage divisions of large banks are directly exposed to the risk of insurance price increases or coverage withdrawal. Specifically, with the recent increase in acute climate-related physical risk comes the specter of home insurance price increases or possible denial of coverage in certain areas. For example, AIG recently announced plans to leave the California market due to climate risks. There are significant risks in the insurance industry as noted in this recent analysis. The most recent NOAA data shows that the U.S. has experienced 20 separate billion dollar weather and climate disasters in 2021.

Ceres believes that the bank market's reliance on the availability of home insurance for its residential mortgage portfolio could lead to a climate-related gap in risk monitoring. As such, we recommend that banks study the potential impact of residential property insurance price increases or coverage withdrawal on the value, default rate, loss given default, and financing cost of residential mortgage portfolio holdings. Similarly, banks use insurance and derivatives to hedge climate-related risks at the loan and portfolio level, but this does not eliminate the systemic risk, as that risk is assumed by the firm to which the risk is transferred. With hedging also comes systemic risk concerns, especially where one firm is providing most of the climate risk protection. We recommend the FDIC discuss these risks in its next Risk Review and/or Supervisory Insights. There is also similar risk in other portions of banks portfolios.[4]

[4] Our 2020 report highlights the risk by various sectors.

With regards to the use of carbon offset credits (or other similar carbon trading schemes) as a risk mitigation strategy, Ceres recommends that the primary focus of banks should be on "absolute GHG reductions" through client engagement as opposed to "net GHG reductions" via financial engineering. As such GHG offset strategies should be used sparingly and only as a last resort. Ceres has produced a report, The Role of Natural Climate Solutions in Corporate Climate Commitments: A Brief for Investors, to help banks and other end-users understand best practices when using this risk mitigation tool.

Outside of insurance and offsets, financial institutions' relationships with their clients must be at the heart of any strategy for climate risk mitigation. Arguments that large financial institutions "bank the entire economy" and as a result have no pathway to reduce their climate risk miss the critical role of client engagement and transition. Business within a sector can gradually be shifted towards companies with a higher share of sustainable assets and/or robust transition plans. The recently released 2030 plans from a few of the largest banks take initial steps with some of their client sectors. While additional actions are needed, these are good initial steps.

For example, if a bank weighted its exposure to the utility sector heavily toward renewables and its exposure to the auto sector toward electric vehicles, Ceres analysis shows that some transition risk could be offset by the de-risking of green investments that would occur in a rapid transition scenario. Our analysis also shows the extent to which a bank's vulnerability to transition risk is extremely sensitive to the choice of clients in climate-relevant sectors. The availability of "investable opportunities" is an important factor in how easy it is to mitigate risk through sustainable finance. The current structure of the economy will mean that most banks, particularly the largest ones, will have a "long" exposure to the business-as-usual case and a "short" exposure to the transition scenario. However, proactive banks may be able to capture enough sustainable opportunities to adjust this balance in a way that manages their overall transition risk.

9. What, if any, climate-related financial products or services – for example, "green bonds," derivatives, dedicated investment funds, or other instruments that take climate-related considerations into account – do banks offer to clients and customers? What risks, if any, do these products or services pose?

Based on our interactions, many of the largest banks currently offer their borrowers a variety of "green" products, such as sustainability-linked loans, derivatives with embedded sustainability KPIs, etc. While we encourage banks to support their client's climate risk management and sustainability efforts, banks should pay attention to the potential unique reputational risks these products entail, such as the risk of "greenwashing" by the bank and/or the borrower. Greenwashing is the process of knowingly or unknowingly conveying a false impression as to how sustainable or environmentally sound a product or service actually is. It can occur when the benefits conferred by the product or service are not material to the bank or borrower, or relevant to the borrower's primary business activity. Such practices may also be considered "deceptive" under Section 5 of the Federal Trade Commission Act, which is enforced by the FDIC for state nonmember institutions.

As such, we ask the FDIC to consider highlighting this risk in its next Supervisory Insights, and continue doing so in future Risk Reviews as it did in May 2022. We also encourage the FDIC to require that bank compliance frameworks are updated to include greenwashing surveillance similar to the SEC's current initiatives to proactively identify ESG-related misconduct.

10. How do financial institutions currently consider the impacts of climate-related financial risk mitigation strategies and financial products on households and communities, specifically LMI and other disadvantaged communities? Should the agencies modify existing regulations and guidance, such as those associated with the Community Reinvestment Act, to address the impact climate-related financial risks may have on LMI and other disadvantaged communities?

For financial institutions to credibly assess the impacts of climate-related financial risk mitigation strategies and financial products on households and communities, specifically LMI and other disadvantaged communities, Ceres recommends that banks commit to principles of diversity, equity and inclusion and that bank board members and senior management are selected from a diverse and inclusive pool of candidates drawn from the

communities that the financial institutions serve. Incorporating the principles of a just and inclusive economy is foundational to any effective climate risk management regime.

Moreover, the Office of the Comptroller of the Currency (OCC), FDIC, and Federal Reserve Board (Fed) should incorporate into its final interagency Community Reinvestment Act (CRA) regulations expectations on how banks should consider the impacts of climate-related financial risk on LMI and other disadvantaged communities. Ceres commends these agencies for releasing this proposed rule, and for including activities that promote climate resiliency and disaster preparedness as activities that qualify under the CRA for community development purposes. We have previously submitted comments on the CRA to support this important work, and will be submitting a more detailed comment to this new proposed rule in addition to what is noted below.

Ceres recommends the agencies develop CRA examination procedures to assess individual bank climate-related performance and to collect aggregate industry data on LMI individuals and communities. The FDIC should also consider incorporating explicit provisions for climate resilience and race as interrelated stability risks which banks must address. This could include activities that support climate resiliency such as explicitly targeting LMI communities of color for investments in urban infrastructure to boost extreme weather resilience; investments in renewable energy and water conservation projects for affordable housing to reduce utility payments; investments in flood resilience activities; and installation of air conditioning in multifamily buildings to reduce heat risks and utility payments.[5] Likewise, the FDIC should incorporate the insights and analysis produced by the Financial Literacy and Education Commission (FLEC)[6] - of which the FDIC is

[5] Although these projects exemplify the beneficial objectives of climate change resilience financing, it is not intended as an exhaustive list of activities that banks should consider in addressing the impacts of climate-related financial risk mitigation strategies and financial products on LMI communities and communities of color.

[6] Under FSOC recommendations 1.8 and 1.9, Treasury and FLEC members should "evaluate climate-related impacts and the impacts of proposed policy solutions on financially vulnerable populations when assessing the impact of climate change on the economy and the financial system," and "engage other members ... to analyze and understand the impact of climate change on the financial well-being of financially vulnerable populations."

a member - into its expectations on how banks consider climate-related financial risks on LMI and other disadvantaged communities.

Further, to properly address the impacts of climate-related financial risk mitigation strategies and financial products on households in LMI and other disadvantaged communities, bank board members and senior management must have proven climate risk management competence, training and experience. To ensure that board members have access to climate and ESG training, Ceres has partnered with Berkeley Law school to offer an online training program which pinpoints how corporate board members can embed ESG into their oversight role. We encourage all bank board directors to participate in appropriate continuing education on these vital issues. We also encourage banks to build on their current efforts to include diverse voices into various levels of decision-making. It is important to have individuals representing different life experiences to advice on key financial decisions.

Additionally, the FDIC should require banks consider whether their climate risk mitigation efforts have fair lending implications, and ensure that examiners and enforcement officials are sufficiently trained to identify issues that may result in disparate treatment. To this end, we recommend the FDIC consider issuing guidance that explains how banks could inadvertently engage in discriminatory practices when addressing climate-related financial risks.

Data, Disclosures, and Reporting

11. What, if any, specific climate-related data, metrics, tools and models from borrowers and other counterparties do financial institutions need to identify, measure, monitor, and control their own climate-related financial risks? How do financial institutions currently obtain this information? What gaps and other concerns are there with respect to these data, metrics, tools or models?

Ceres has published two reports on climate-related financial risks for banks – one on Transition Risk and another on Physical Risk. In these reports, we recommend that banks engage with their borrowing clients on a sector-by-sector basis to obtain climate-relevant data, with consideration given to the unique transition risks (including legal and reputational) and physical risks inherent to each industry sector. Banks should update or

refine their decisions based on this data as they obtain new information. Specifically, we recommend that banks obtain the following data in support of effective climate risk management:

- Scope 1, 2, and 3 GHG emissions data from borrowers;
- Information on planned capital expenditures and their likely impact on company emissions, as well as transition plans (if available);
- Geolocational information of all critical borrower infrastructure; and
- Borrower climate disclosures prepared using the TCFD framework (banks should encourage borrowers to disclose this information using the TCFD framework to ensure that climate-relevant data is comparable across industries and geographies).

To minimize compliance costs, the FDIC should also encourage and incentivize banks to actively contribute to the development and sharing of climate-relevant borrower data, as appropriate. Banks should collaborate with customers, peers, academics, and regulators to obtain and understand these data. The FDIC should also encourage banks to use a common set of standards, such as the PCAF framework, for measuring their Scope 3 emissions associated with client activities.[7] Without a standardized framework, it may be difficult to accurately assess banks' risk and the effectiveness of their mitigation strategies.

Additionally, banks can take action on many climate-related financial issues despite uncertainty in other areas. For example, the New York Department of Financial Services notes that institutions "should establish board governance and an organization structure that supports the effective management of climate risks and develop their expertise and capacity to assess and manage climate risks on both sides of their balance sheets." Such actions could "be implemented with relative speed and confidence."

[7] Investors are increasingly requesting companies' Scope 3 data, and the SEC's proposed climate disclosure rule includes Scope 3 disclosures. If the SEC includes Scope 3 in its final rule, this will decrease the burden on compliance with any future FDIC rules, and the FDIC could coordinate with the SEC on this issue.

12. How could existing regulatory reporting requirements be augmented to better capture financial institutions' exposure to climate-related financial risks?

In our two recent reports on climate-related financial risks for banks (Transition Risk and Physical Risk reports) we make recommendations that the existing capital adequacy regime be expanded to include climate stress testing with eventual adjustments to both bank liquidity and capital requirements. In 2021, Ceres also provided testimony to the United States House of Representatives on the importance of climate stress tests as part of an effective bank capital adequacy regime.

Additionally, Ceres recommends that the FDIC works with the OCC and the Fed to amend the Call Report to include information relevant to financial institutions' climate-related financial risks. The FDIC should also consider issuing guidance that would provide standards for financial institutions to ascertain data on their GHG emissions to guarantee that disclosures among institutions are consistent, comparable, and reliable. Moreover, we recommend that existing regulatory reporting requirements for banks be expanded to require the use of the TCFD framework to ensure that public disclosure of climate relevant information is comparable across banks of varying asset size, location, and business model.

Furthermore, as part of identifying and quantifying climate-related financial risks, Ceres believes that large banks should establish and disclose net zero plans which describe in detail how they plan to decarbonize their business activities and achieve net zero emissions by no later than 2050. These plans should provide practical, actionable steps for banks to create an effective net zero transition, including assessment of assets that may be exposed to climate transition risk, internal valuation tools, and disclosure of risk assessments that identify climate-relevant sectors and the percentage of at-risk assets in these sectors. Large banks should also set detailed interim decarbonization goals (for example, 2030 or 2040 Paris-aligned goals) and provide a timeline with regular updates towards achieving them.[8]

[8] For example, banks could validate their goals through the Science Based Targets initiative, a recently launched a methodology for banks to set targets that include financed emissions. Although aligning with this methodology will enhance comparability, banks should focus first on a goal that

Finally, all interim goals and 2050 net zero commitments should incorporate the latest science, use credible climate scenarios, and disclose decarbonization progress on a sector-by-sector basis. Banks should engage clients on their own climate strategies by, for example, requiring clients to provide data in key climate-related areas, such as energy technology and emissions profiles; aggregating those data using methods such as carbon accounting; and building climate risk into day-to-day decision-making tools, such as client earnings models. Ceres recommends that the FDIC also incorporate results from its recent Call for Papers regarding "net zero goals and their effects on key segments of the finance industry," including "integrated assessment models and their usage in a climate-risk loss forecasting context." We encourage the FDIC to consider augmenting existing regulatory reporting requirements to include this additional risk-mitigating disclosure.

Scenario Analysis

13. Scenario analysis is an important component of climate risk management that requires assumptions about plausible future states of the world. How do financial institutions use climate scenario models, analysis, or tools and what challenges do they face?

Ceres maintains an active and regular dialogue with U.S. banks of varying asset size, location, and business model. Moreover, most of the U.S.-based G-SIBs are members of Ceres' Company Network. Based on our interactions, it is clear that the uses and challenges banks face regarding climate risk management varies greatly by size. For example, many of the largest banks currently use some form of climate-risk scenario analysis and/or climate-risk stress testing to evaluate the transition and physical risks associated with their lending portfolios. The main challenges they face in advancing their climate scenario analysis and stress testing programs are technical in nature:

- Even with considerable client engagement, they face difficulty in obtaining borrower-specific climate data (for example, GHG emissions).

will incentivize action internally and reflect their risk management strategy to the greatest possible extent.

- In general, larger, publicly-listed borrowers are more likely to provide banks with climate data, whereas small to mid-size and privately-owned borrowers are less willing or able to generate this information.
- In some cases, large banks are unsure of which climate scenarios are most relevant for their business model or the most relevant scenarios do not provide sufficient detail in some areas critical to financial institutions.

In contrast, the use of climate-risk scenario analysis and/or climate-risk stress testing for regional and community banks can be characterized as being in its infancy. Moreover, the main challenges they face in advancing their climate scenario analysis and stress testing programs are both technical and operational in nature:

- Some regional and community banks do not yet consider climate to be a material risk factor, and so are not engaging their borrowers in obtaining climate-relevant data.
- When client engagement does occur, borrowers are unable or unwilling to provide climate data (for example, GHG emissions).
- In some cases, regional and community banks are unsure of which climate scenarios are most relevant for their business model.
- Often, banks wait for regulatory guidance before investing resources in the design of climate-risk scenario analysis and/or climate-risk stress capabilities.

14. What factors are most salient for the FDIC to consider when designing and executing scenario analysis exercises?

When designing and executing scenario analysis, at a micro-level, we believe that the scientific rigor and transparency of the scenarios are paramount. As such, banks should ensure that their scenarios:

- Are science-based and aligned with the most current climate science;
- For transition risk, the scenarios should consider both an “orderly” and “disorderly” transition;
- For physical risk, the scenarios should contain at least one "worst case" scenario;
- Assumptions regarding both demand and prices for commodities (such as oil) should be transparent and clearly stated; and

- Scenarios should be aligned with current best practices (i.e., IEA and NGFS scenarios).

From a macro-standpoint, the U.S. regulatory regime has proven itself to be robust and flexible enough to meet the challenge of many recent perils. For example, through necessity and quick action, regulators have been able to successfully navigate new threats to bank safety and soundness such as cybersecurity and the coronavirus pandemic.

Thus, when considering which macro factors are most salient to designing and executing climate scenario analysis, we recommend first and foremost that the FDIC continue to act with a sense of urgency around this existential and systemic threat. The FDIC should begin conducting these exercises quickly. Although initial models may be simplistic, the FDIC should eventually provide multiple scenarios as described above.

Second, as climate risk permeates all aspects of the capital markets and poses grave threats to financial institutions of all sizes and business models, we recommend that these scenario analyses eventually be adopted by all U.S. banks irrespective of asset size, location, or business model. For example, regional banks may experience higher rates of failure climate events and natural disasters that impact discrete geographic areas. Scenario analysis implementation could initially be tailored by bank size, with the threshold lowered overtime as more data becomes available to smaller banks, allowing those banks to build capacity.

Third, the FDIC must ensure that banks have access to educational resources in support of bank innovation regarding climate scenarios, models, and data.

Finally, we believe that climate scenario analysis exercises should eventually evolve into a formalized climate stress testing regime which informs regulatory capital adequacy metrics. The FDIC should also review financial institutions' models to ensure they are suitably robust, and that financial institutions are not "model shopping" to avoid poor outcomes. Without climate stress testing (including a comprehensive capital adequacy regime), we believe that banks are at risk of running a higher quantum of enterprise risk than they are aware of, posing a danger to the safety and soundness of our financial system.

Once again, we congratulate the FDIC for its fine work in developing these Principles. The agency's leadership on this critical issue is deeply valued. We would be pleased to discuss any questions you may have on our feedback. In addition to the undersigned, you may also contact our Manager of Banking Financial Regulation, Kelsey Condon (kcondon@ceres.org) at your convenience.

Sincerely,

Isabel Munilla
Director, U.S. Financial Regulation
Ceres Accelerator

Jim Scott, CFA
Senior Advisor, Financial Institutions
Ceres Accelerator

Kelsey Condon
Manager, Banking Financial Regulation
Ceres Accelerator

Steven M. Rothstein
Managing Director
Ceres Accelerator

Attachment 1: Recommendations for FDIC Action to Address Climate-related Financial Risks

I. Recommendations for FDIC Action to Address Climate-related Financial Risks

1. The FDIC should include climate as a risk that may affect banks or the Deposit Insurance Fund in the Risk Review

The Federal Deposit Insurance Commission (FDIC) acknowledges the transition risks from climate to the energy sector. Given the threats to the stability of the financial system posed by climate, the FDIC should continue to amplify both these transition risks as well as physical risks in its Risk Review.

In addition, the FDIC refers to climate change and environmental, social, and governmental (ESG) risk mitigation considerations by banks. While "understanding changes in policy, technology, and investor sentiment as they relate to ESG risk" is important, transition and physical risks to individual banks are a safety and soundness concern and should be treated as such by the FDIC.

2. The FDIC should issue guidance to regulated banks on climate risk

The FDIC should issue guidance through a Financial Institution Letter (FIL) to first acknowledge that climate poses risks to both the financial system and to individual financial institutions and then to provide guidance to FIs on how to identify and monitor climate-related risks.

3. The FDIC should include climate risk as a supervisory priority in its Annual Performance Plan

For its 2022 Annual Performance Plan, the FDIC should add a Performance Goal to assess climate risk in supervised institutions. The FDIC should also add climate as an "external factor" that could affect the banking industry and the FDIC. The pandemic clearly

demonstrated that external shocks can have a significant impact on the financial services industry. While COVID-19 could not have been predicted, climate change and its effects are occurring today and will continue to worsen. Climate risk should therefore be a supervisory priority for the FDIC.

4. The FDIC should conduct a Tech Sprint to identify tools for financial institutions to measure climate risk

The FDIC has been a leader among financial regulators through its Tech Sprint Program in using a creative crowdsourcing technique to address complex problems. The FDIC should solicit banks, non-profit organizations, technology and data analytics companies, and other members of the public to convene and collaborate on finding data, tools, and other measures of climate risks in banks. Such tools could be helpful for all financial institutions, but particularly for community banks that may lack the resources or expertise to measure or monitor such risks.

5. The FDIC should issue an RFI on Climate Risk

The FDIC should issue a Request for Information (RFI) to inform the agency on how banks in the U.S. and other parts of the world measure and monitor climate risk. The RFI can ask for input on how the FDIC should approach climate from a supervisory perspective. Finally, the RFI could inquire whether additional guidance from the FDIC would be helpful to financial institutions as they look to measure and monitor their climate risks.

6. The FDIC should join the Network of Central Banks and Supervisors for Greening the Financial System

Like Global Financial Innovation Network (GFIN), the Network of Central Banks and Supervisors for Greening the Financial System (NGFS) is a global network of central banks and supervisors. They work together to share their experiences and develop nonbinding best practices. The Federal Reserve Board (the Fed or FRB) and the Office of the Comptroller of the Currency (OCC joined NGFS in the last year. The FDIC is already an active member of the Basel Committee's Task Force on Climate-related Financial Risks (TFCR). The FDIC should join the NGFS to both learn from global peers and contribute to the development of tools and practices to address risks to the financial system from climate change.

II. Interagency Recommendations

Interagency Case Studies and Recommendations

Short-term actions by each of the Financial Stability Oversight Council (FSOC) members individually is critical to address the risks to the financial system from climate change. While individual agency actions are important, collective action can sometimes send a more powerful and consistent message to the financial services industry. The benefits from the government acting on a joint or Interagency basis are clear. Such joint actions avoid conflicting or duplicative messages which create burden for industry and they can result in a more efficient allocation of resources by the agencies.

Interagency Case Studies

The agencies have demonstrated in the past that they can work quickly when they believe an emerging risk is significant and imminent. Appendix A details two case studies of timely responses to identified threats to the financial system. In the first example the agencies acted together over the course of four years to address the concern that the effect of the year 2000 date change on computer systems could have severe, far-reaching consequences for financial institutions. During the course of the four years, the agencies issued more than 20 interagency policy statements on multiple related topics, trained and deployed examiners who conducted multiple examinations at each institution, developed and disseminated educational content and conducted outreach, tracked and monitored progress, took action to address deficiencies and engaged in contingency planning.

The second example involves the agencies' collective action to address increasing cybersecurity risks. In roughly a year from identifying cybersecurity as a top priority for the Federal Financial Institutions Examination Council (FFIEC), the agencies had developed a risk assessment tool. The FFIEC quickly launched a dedicated page on cybersecurity for financial institutions and examiners, piloted a program at over 500 community institutions to assess management of cyber risks, published general observations from the pilot, outlined its cybersecurity priorities for the remainder of the year, and released a Cybersecurity Assessment Tool (CAT). The agencies have since taken

additional actions, but their collective efforts to highlight the importance of the issue, understand its implications for the regulated institutions, and give the industry a self-assessment tool, as well as a tool for examiners, in such a short period of time is instructive.

These examples are evidence of constructive, timely, coordinated and effective actions agencies have taken collectively to address emerging issues. These examples provide a roadmap for interagency statements, guidance, outreach, training, examination, and accountability that could all be deployed in addressing climate risks.

Recommended Interagency Actions

1. Conduct a Climate Risk Policy "Sprint"

Regulators have begun to embrace the idea of a "Tech Sprint." A Tech Sprint is a short, time-bound initiative to develop innovative and creative solutions to a specific problem in a collaborative way. Pioneered by the Financial Conduct Authority (FCA), the concept has been adopted by both the Federal Deposit Insurance Corporation (FDIC) and the Consumer Financial Protection Bureau (CFPB) to solve challenging issues that transcend the capacity of one agency or organization to tackle. More recently, the FDIC, FRB, and OCC announced that they are working on a Digital Assets Sprint Initiative (also called the Crypto Sprint) and just issued their first interagency statement based on the sprint. The purpose of the initiative is to increase collaboration and clarity around digital assets and involves a series of four sprints to address in a timely manner the many issues raised by cryptocurrencies. As stated by Acting Comptroller Hsu in his August 3, 2021 testimony before the Senate Banking Committee:

> The first sprint focuses on developing a common taxonomy for digital assets and agreed upon definitions to ensure a common language and understanding of the basic terms and concepts for future discussions. The second sprint centers on understanding use cases and risks associated with cryptocurrencies and digital assets. The third sprint concentrates on potential gaps in regulation and supervision and prioritizing those gaps for additional consideration. The fourth sprint will consider the policy needs based on the work conducted during the previous sprints.

The FFIEC members should immediately create a Climate Risk Sprint initiative. This recommendation is consistent with FSOC Recommendation 2.1 (Fill data gaps) and Recommendation 2.5 (Data metrics and standardization). Using the Digital Asset Sprint Initiative as a model, the agencies should conduct rapid sprints to first develop a common set of definitions to inform discussions and then review current and evolving risks to financial institutions. The agencies should conclude by collaborating in conducting sprints to evaluate the regulatory and policy gaps in supervision.

Additionally, the FFIEC members could consider a TechSprint that involves the participation of outside experts – industry representatives, scientists, data specialists – to collaborate side-by-side with government officials to address potential data and technology solutions to assessing and managing climate risks. Such a collaboration facilitates new and beneficial connections and networks and focuses great energy and creativity to problem solving in a compressed time period. This type of TechSprint has been used repeatedly by the FCA and has also been adopted by the FDIC and CFPB.

2. Establish FFIEC Working Group

As noted in the above case study on cybersecurity, the FFIEC was able to act with relative speed to address the rising cybersecurity risks to the financial system when it announced the creation of the Cybersecurity and Critical Infrastructure Working Group (CCIWG). The CCIWG was formed in 2013 "to enhance communication among the FFIEC member agencies and build on existing efforts to strengthen the activities of other interagency and private sector groups" and quickly rolled out a series of announcements resulting in the release of the first version of the CAT in 2015.

Similarly, the FFIEC should announce the creation of the Climate Risk Working Group, reporting to the Council through the Task Force on Supervision (TFOS). The purpose of the Climate Risk Working group would be similar to the CCIWG (i.e. enhance communication among members, and build on existing efforts by other agencies and private sector groups). The FFIEC can use the Climate Risk Working Group to develop a means to begin to assess and enhance the state of industry preparedness. Finally, the Working Group can identify gaps in the agencies' examination procedures and training that can be closed to strengthen the oversight of climate risk readiness.

The regulators could also consider establishing a body, such as the UK Climate Financial Risk Forum (CFRF), composed of industry representatives and convened several times a year by the regulatory agencies.[1] The CFRF has published a couple of best practices guides to assist financial institutions in identifying climate-related financial risks and opportunities. The latest guide is focused on risk management, scenario analysis, disclosure, innovation and climate data and metrics.

3. Issue Guidance through the FFIEC

Using the CCIWG as a model, the FFIEC should issue Guidance to the industry to raise awareness of the risks, encourage financial institutions to integrate climate risks into their enterprise risk frameworks, and provide guidance on how to measure and mitigate risks, including through best practices. Guidance can be sequenced to first provide a declaratory statement that climate is a risk to both the financial system and to individual institutions. Subsequent Guidance can address first physical risks and then transition risks associated with climate change. Such actions can help fulfill FSOC Recommendations 4.7 and 4.8 (Review of supervisory and regulatory tools). Agencies can also help raise awareness by highlighting relevant events or milestones (see proposed Climate Risk Awareness Month below).

4. Develop a "Resources" section for climate risk on the FFIEC web page

The FFIEC should develop a page on its website to list resources related to climate risk to the financial services industry. First, it can list all Guidance from the FFIEC or from the member agencies. The site could also link to other federal resources or agencies that offer helpful information. Given the increasing frequency of natural disasters, the agencies may want to create a section to consolidate interagency statements on regulatory relief for natural disasters. The agencies should also amend the Interagency Supervisory Examiner Guidance for Institutions Affected by a Major Disaster, adopted in 2017, which makes no mention of climate change. The Guidance should be amended to cite the risks associated with climate change and note that in many cases, natural disasters are no longer "exceptional."

5. Create a Flood Insurance Resource Page and Update Flood Insurance Guidance

Pursuant to 12 U.S.C. § 3305(g), the FFIEC is required to consult with the agencies responsible for supervising for compliance with the National Flood Insurance Program (FDIC, FRB, National Credit Union Administration (NCUA), and OCC as well as the Farm Credit Administration) and develop uniform standards for use by financial institutions. While the Task Force on Consumer Compliance (TFCC) has had working groups to develop flood insurance compliance examination procedures for the agencies as well as Interagency Questions and Answers Regarding Flood Insurance, no information on the National Flood Insurance Program (NFIP) is available on the FFIEC website. The FFIEC should take the following actions to both facilitate compliance with the NFIP by financial institutions as well as reduce the risks to financial institutions from uninsured and underinsured properties:

- Create a section on the FFIEC website devoted to flood insurance with information on the NFIP from the agencies or from the Federal Emergency Management Agency (FEMA).
- Issue updated guidance on flood insurance that incorporates risks from climate change.
- Develop tools to facilitate compliance by financial institutions with the NFIP.
- Given that the flood insurance maps are out of date and do not reflect current risks, the agencies should encourage financial institutions to move beyond compliance with the Flood Disaster Protection Act and recognize that there are substantial flood risks for properties that do not lie within a flood zone. Financial Institutions should therefore consider the safety and soundness risks for uninsured or underinsured properties that lie outside of a flood zone when underwriting a mortgage.

6. <u>Amend the Call Report</u>

Under the auspices of the Task Force on Reports (TFOR), the FFIEC should amend the Call Report to collect information on institutions' climate-related financial risks, consistent with the FSOC Recommendations 3.1, 3.2, 3.3, and 3.7 (Enhancing Public Climate-related Disclosures), using data terms defined by the Climate Risk Sprint (see above). The NCUA, as a member of the TFOR should also incorporate such changes into its call report for credit unions. As noted in FSOC Recommendation 3.7, such information collection should consider an institution's size, complexity, and activities.

7. Amend the UBPR

The Uniform Bank Performance Report (UBPR) is an invaluable tool for examiners to assess a bank's financial condition and risks and to compare an institution with its peers. The UBPR, as a publicly accessible report, is also widely used by industry to conduct a peer analysis. The data from the UBPR comes directly from the Call Report. Following any amendments to the Call Report, the Task Force on Surveillance Systems (TFSS) should create standardized measurements of climate risk in the UBPR. Such metrics should be able to identify risks at individual institutions as well as risks among peer groups and in the aggregate. This recommendation is consistent with FSOC recommendations 2.5 (Data metrics and standardization) and 3.3 (Enhancing Public Climate-related Disclosures).

8. Host a webinar(s) for industry on risks associated with climate

Over the years, the FFIEC and its member agencies have held numerous webinars and conferences for industry on various risk topics, including cybersecurity, Bank Secrecy Act/ Anti-money Laundering (BSA/AML) and the LIBOR transition. The FFIEC should host one or more webinars for banks and credit unions on the risks of climate to financial institutions of all sizes and the need to measure and mitigate climate risks.

9. Develop a Climate Risk Assessment Tool

Following the creation of the CCIWG, the FFIEC released the first version of the CAT. The CAT was a unique development by the agencies; rather than releasing a regulation or regulatory guidance and expecting institutions to comply on their own, the FFIEC developed a tool to help financial institutions to understand and assess their cybersecurity risk and preparedness. This was particularly helpful to smaller financial institutions that lack the resources to conduct such an analysis internally.

Similarly, the FFIEC's Climate Risk Working Group should develop a Climate Risk Assessment Tool to help financial institutions, particularly smaller, community financial institutions, be able to identify their risks associated with climate change as well as their preparedness under various climate scenarios. By clarifying expectations, FFIEC members will address FSOC Recommendation 4.8 (Review of supervisory and regulatory tools). Ideally, the Tool would be based on accepted national or international standards

and would provide financial institution management with actionable steps to mitigate risks.

10. Include climate risk as a topic in the FFIEC "Supervisory Updates and Emerging Issues" conference for examiners

The FFIEC provides specialized education and training for examiners from the agencies. One such offering is the Supervisory Updates and Emerging Issues Conference. The conference provides experienced examiners with training on developments in the financial services industry, including new products, new technologies, and emerging risks and other issues. The FFIEC should include climate risk as a topic in its emerging issues conference to update examiners on this risk to the financial services industry and the measures being taken by both regulators and banks and credit unions to mitigate such risks.

11. Use the upcoming modernized CRA proposed rules to Address the Disproportionate Impact of Climate Change on Low and Moderate Income Communities

The FSOC report on climate-related financial risk explicitly recognizes that "climate change disproportionately affects financially vulnerable populations potentially including lower-income communities, communities of color, Native American communities, and other disadvantaged or underserved communities." Noting that while vulnerable communities may be more exposed to climate-related risks, there's also a recognition that actions to address such risk, such as through higher insurance and credit costs, may disproportionately impact financially vulnerable communities. The report calls for thoughtful and balanced policy responses.

The interagency efforts underway to modernize the Community Reinvestment Act (CRA) rules provide an opportunity for a thoughtful and balanced policy response. There are myriad ways in which the forthcoming proposed CRA rules could address the impact of climate change on low and moderate-income communities and communities of color. Ceres submitted two CRA-related comment letters.[2] These include several specific recommendations for your consideration with the upcoming updates of CRA.

12. Update the Shared National Credit Program to account for climate-related risks

The Shared National Credit (SNC) Program assesses credit risks and trends as well as the risk management practices associated with the largest and most complex credits shared by multiple regulated financial institutions. The SNC Program is conducted by the FRB, the OCC, and the FDIC for credits involving three or more regulated institutions for aggregate credit commitments of $100 million or more. The most recent SNC Report highlighted the high and increasing risk of leveraged loans as well as the industries most impacted by COVID-19 in the pool of SNC loans. The industries most impacted were oil and gas, entertainment and recreation, and transportation services.

Given the size and impact of SNCs, the three federal prudential regulators should update the SNC review process to account for climate-related risks. While some SNC commitments could be vulnerable to severe weather events, other SNC commitments to industries that are highly dependent on fossil fuels may be affected by transition risk. To the extent that there are trends associated with climate-related risk, the agencies should highlight those in the SNC Program report.

13. Urge the White House to designate a "Climate Risk Awareness Month/Week/Day" at the federal level

There are commemorative designations for each month, week, and day of the year to raise awareness of issues. September is National Preparedness Month; October is Cybersecurity Awareness Month. The federal government should designate a month (or week or day) to climate risks, including risks to the financial system. Congress can do so by enacting legislation but the White House can also provide for commemorative designations by proclamation.[3] Dedicating a month or week to the risks posed to the financial and other industry sectors from climate change would help raise awareness of such risks beyond the environmental toll. Once designated, the financial regulators should promote the date(s) to help raise awareness.

Appendix A - Interagency Case Studies

I. Interagency Coordination on Y2K

Overview of Process

Financial regulators began preparing for the Year 2000 date change (Y2K) as early as June 1996, when the Federal Financial Institutions Examination Council (FFIEC) issued an interagency joint statement concerning the potential effect of year 2000 on computer systems.[4,5] To address potential challenges raised by Y2K, the regulators promulgated guidance and implemented regulations over a four-year period between 1996 and 1999.

According to a statement in September 1999 from then-Comptroller of the Currency John D. Hawke, Jr., the effort consisted of the following actions[6]:

> First, we rigorously studied the likely impact of Y2K on the banking system and we calculated what it would take to prepare for it. Second, we looked at our own internal systems and earmarked the necessary resources to bring them to a state of readiness. Third -- and perhaps most important -- we began working with the financial institutions we supervise to heighten their awareness and encourage them to move with all due haste toward Y2K solutions of their own. We encouraged, we supported, and we cajoled. Through the FFIEC, we issued more than 20 interagency policy statements, dealing with such things as testing, contingency planning, customer awareness, and more. We even took enforcement actions in those cases where it seemed warranted.

Leading up to the year 2000, bank examiners conducted Y2K-related examinations multiple times - between two and four times for each insured financial institution - and continued to oversee the largest banks. By September 1999, 99.7 percent of all federally supervised financial institutions had finished renovating and testing their systems -- "not

just the systems that house their records and run their elevators, but the systems that bank customers rely upon for access to their funds."[7]

The FFIEC agencies also developed educational content such as videos and brochures for financial institutions to use in communicating to their customers the measures taken to ensure customer funds were safe.[8]

Comptroller Hawke detailed the steps the FFIEC had taken to Congress in April 1999 and said the interagency coordination consisted of[9]:

- Developing and disseminating detailed policy guidance to supervised institutions;
- Training and deploying examiners to conduct three or more onsite examinations of each institution;
- Setting up systems to track and monitor progress;
- Establishing and implementing vigorous enforcement programs to deal with deficiencies;
- Coordinating with other government agencies as well as private enterprises, domestically and internationally, to share valuable Year 2000-related information;
- Conducting numerous outreach programs to educate banks and the public; and
- Helping to organize and participating in a series of interagency contingency planning groups to plan for the orderly resolution of problems or issues that may arise either systemically or with individual banks.

The FFIEC published guidance documents on the following topics and published an interim rule, which became final one year later, on Y2K-related safety and soundness standards for financial institutions.

Guidance:

- The Effect of Year 2000 on Computer Systems (June 1996);
- Year 2000 Project Management Awareness (May 5, 1997);
- Safety and Soundness Guidelines Concerning the Year 2000 Business Risk (December 17, 1997);

- Guidance Concerning Institution Due Diligence in Connection with Service Provider and Software Vendor Year 2000 Readiness (March 17, 1998);
- Guidance Concerning the Year 2000 Impact on Customers (March 17, 1998);
- Guidance Concerning Testing for Year 2000 Readiness (April 10, 1998);
- Guidance Concerning Contingency Planning in Connection with Year 2000 Readiness (May 13, 1998);
- Guidance on Year 2000 Customer Awareness Programs (May 13, 1998);
- Customer Brochure on Year 2000 (July 6, 1998);
- Year 2000 Phase II Workprogram (July 8, 1998);
- Answers to Commonly Asked Y2K Questions (August 31, 1998);
- Frequently Asked Y2K Questions on Contingency Planning (December 11, 1998);
- Additional Year 2000 Guidance on Customer Communications (February 17, 1999); and
- Additional Y2K Questions on Contingency Planning (May 6, 1999).

Deep Dive into Interagency Action on Y2K

On June 17, 1996, the FFIEC issued its first interagency joint statement on the potential effect of Y2K on computer systems to the CEOs of all federally supervised financial institutions, senior management of each FFIEC agency, and all examining personnel.[10] The joint statement cautioned that the two digit field "00" in the year 2000 that would replace “99” in records would be recognized as the year 1900, which would create erroneous data or cause a system failure based on incorrect calculations. The potential impact of Y2K could have affected “all forms of financial accounting (including interest computation, due dates, pensions, personnel benefits, investments, legal commitments)” and “record keeping, such as inventory, maintenance, and file retention.”

The joint statement urged examinations to “review all aspects of computer systems to include those provided by service bureaus, hardware vendors, and other software vendors.” It stated that management must ensure:

- External vendors and servicers are addressing adequately the system and software issues related to Y2K; and

- In the event external vendors are unable to achieve the requirements, institutions have taken the steps needed to continue critical operations.

The joint statement also outlined the following plan for financial institutions to mitigate Y2K-related risk:

I. Establish a Year 2000 Team

A. Management should consider utilizing both internal and external information systems and audit resources to ensure that a risk-based Year 2000 Action Plan is developed.

B. An inventory of all computer operating systems, applications and files should be created. All those with year 2000 issues must be identified.

II. Develop an Institution Wide Year 2000 Plan

A. The initial step in developing the plan should be to consider whether current systems and files should be modified, replaced, outsourced, or discontinued. It should be noted that even if new systems are purchased, old files may still have to be modified. (All computer systems, including mainframes, personal computers, local area networks, etc., should be considered).

B. The year 2000 plan should also identify and prioritize applications and processes that are the most date sensitive and those which are most vulnerable. Interdependent applications should be grouped together.

C. Management and the board of directors need to ensure that adequate funds and resources are allocated so that all year 2000 projects are completed in a timely manner.

III. Year 2000 Plan Implementation

A. Initiate pilot projects to test solutions to identified problems. It may be feasible to work with more than one vendor in order to evaluate their various solutions/capabilities before making a final decision.

B. Begin the process of systematically implementing year 2000 changes by priority in accordance to risk. These projects should be conducted

within the framework of the system development life cycle process currently in place.
C. Conduct post implementation reviews to ensure the integrity and functionality of the modified systems.

Interagency communications developed through the FFIEC were transmitted through the federal regulators to examiners and the financial institutions they supervised. The OCC relied on advisory letters to transmit the information, the Fed, FDIC, and Office of Thrift Supervision (OTS) used press releases, and the NCUA used letters to supervised institutions to relay the information.

On May 5, 1997, the FFIEC issued a second statement that set out a project management process strongly encouraging federally insured depository institutions to complete an inventory of core computer functions and outline priorities for Y2K goals by September 30, 1997. The statement provides that the "five management phases necessary to complete a computer conversion program are: awareness, assessment, renovation, validation, and implementation." Banks were expected to largely complete programming changes and have testing underway for mission critical systems by December 31, 1998.

The statement included in an appendix a questionnaire from the FFIEC Task Force on Supervision to help regulatory agencies conduct assessments of financial institutions' planning efforts.[11] Regulators used the results of these assessments to determine which supervisory reviews to prioritize based on examination procedures included in a second appendix to the statement. Conversion efforts were expected to be completed by mid-1998.

In 1998, the FFIEC agencies also began supervising for Y2K-related risk for service providers and vendors in examinations, and they included risk analysis on a quarterly basis.[12]

In February 1998, the OTS began publishing a monthly newsletter for the agency's 750 examiners and 1200 thrift institutions it supervised.[13] Content included summaries of its

findings from off-site examinations related to Y2K and the key OTS staff contacts for Y2K-related matters.

In May and October 1998, the FFIEC hosted seminars for risk management planning that included as agenda items managing the risks of emerging technologies and Y2K concerns.[14]

On August 31, 1998, the FFIEC issued the first of three FAQs and answers (the FAQs) regarding Y2K.[15] The FAQs focused on testing, documentation, and the FFIEC report distribution process. They also covered the following topics:

- Clarification of FFIEC policy concerning the types of testing documentation that financial institutions should retain;
- Expectations regarding software and operating system upgrades in 1999;
- Conversions to new mission-critical systems in 1999; and
- Procedures for regulators to examine service providers and software vendors.

On October 15, 1998, the FFIEC agencies published joint interim guidelines to adopt Y2K safety and soundness standards. The guidelines were implemented as a final rule the following year on November 29, 1999 with minimal changes.[16] The standards focused on the following topics:

- Review of mission-critical systems for Year 2000 readiness;
- Renovation of internal mission-critical systems;
- Renovation of external mission-critical systems;
- Testing of mission-critical systems;
- Business resumption contingency planning;
- Remediation contingency planning;
- Customer risk; and
- Involvement of the board of directors and management.

On December 11, 1998, the FFIEC published its second FAQ resource regarding contingency planning that supplemented the previous FAQs and clarified expectations for completing remediation and business resumption contingency plans.[17]

On May 6, 1999, the FFIEC published additional answers to three Y2K FAQs regarding contingency planning.

On July 6, 1999, the FFIEC released guidance on Y2K-related fraud prevention.[18] The guidance encouraged institutions to enhance internal controls and security procedures and to communicate with customers about how to protect against Y2K-related fraudulent schemes. It also issued a consumer advisory for financial institutions' customers regarding Y2k-related fraud.

On June 9, 1999, the FDIC adopted an interim final rule that required certain FDIC-insured banks to implement asset and liability backup programs so that financial records would be preserved in case it suffered a Y2K-related problem and had to be placed in receivership.[19] The rule applied to FDIC-insured banks that scored less than "satisfactory" in their Y2K ratings on or after July 31, 1999.

Following the transition from 1999 to 2000, the FFIEC published on March 21, 2000, a document detailing the lessons learned from its Y2K-related preparation.

The FFIEC stated that it believed the institutions that were best prepared possessed most or all of the following 10 characteristics:

- Senior management and director involvement to ensure that the project plans were clearly defined, supported and monitored;
- Consolidation, elimination or integration of technology on an enterprise-wide basis by developing current inventories of information technology systems and applications;
- Improved oversight of service providers, software vendors and consultants;
- More formalized and effective strategies and standards for testing information technology systems;
- Detailed contingency plans that analyzed the effect of potential system failures on core business processes (e.g., deposit taking, lending, fiduciary services, etc.);
- Better safeguards to detect fraudulent, malicious, and negligent acts from both internal and external sources;
- Review of testing and contingency planning processes by internal auditors;

- Open information sharing for developing strategies and to respond to media reports or perceptions that could reduce public confidence in the financial services industry;
- Improved public relations with customers; and
- Thorough legal review to assist in vendor management, documentation retention, and legal defense.

II. Cybersecurity Assessment Tool

The FFIEC developed its risk assessment tool for cyber risk less than one year after recognizing cybersecurity as a priority. When he assumed the chairmanship of the FFIEC, Comptroller Curry announced cybersecurity as his top priority.

On June 24, 2014, the FFIEC launched a dedicated page on cybersecurity to serve as a resource for financial institutions and examiners. The FFIEC stated[20]:

> While information security has been a core focus of supervision for decades, the FFIEC members are taking a number of steps to raise awareness of cybersecurity risks at financial institutions and the need to identify, assess, and mitigate these risks in light of the increasing volume and sophistication of cyber threats that pose risks to all industries in our society. The FFIEC Web page provides links to joint statements, webinars, and other information that may help financial institutions when thinking about the issue of cybersecurity.

It also launched a pilot program at over 500 community institutions to enable state and federal regulators to assess how the community institutions manage cybersecurity and mitigate cyber risks. In their assessments, regulators focused on: risk management and oversight; threat intelligence and collaboration; cybersecurity controls; service provider and vendor risk management; and cyber incident management and resilience. The pilot also served to help regulators enhance supervisory programs' effectiveness, guidance, and examiner training.

Within four months, on November 3, 2014, the FFIEC published general observations from its cybersecurity assessment pilot, including findings regarding inherent risks of cybersecurity and institution preparedness.[21]

Following the publication of its observations from its cybersecurity pilot, the FFIEC outlined its cybersecurity priorities for the remainder of 2015 on March 17, 2015.[22] The priorities included establishing seven workstreams, including a workstream on developing and issuing a self-assessment tool for financial institutions to use in evaluating their cybersecurity preparedness and respond to cyber threats. The seven workstreams focused on the following topics[23]:

- Cybersecurity Self-Assessment Tool—The FFIEC plans to issue a self-assessment tool this year to assist institutions in evaluating their inherent cybersecurity risk and their risk management capabilities.
- Incident Analysis—FFIEC members will enhance their processes for gathering, analyzing, and sharing information with each other during cyber incidents.
- Crisis Management—The FFIEC will align, update, and test emergency protocols to respond to system-wide cyber incidents in coordination with public-private partnerships.
- Training—The FFIEC will develop training programs for the staff of its members on evolving cyber threats and vulnerabilities.
- Policy Development—The FFIEC will update and supplement its Information Technology Examination Handbook to reflect rapidly evolving cyber threats and vulnerabilities with a focus on risk management and oversight, threat intelligence and collaboration, cybersecurity controls, external dependency management, and incident management and resilience.
- Technology Service Provider Strategy—The FFIEC's members will expand their focus on technology service providers' ability to respond to growing cyber threats and vulnerabilities.
- Collaboration with Law Enforcement and Intelligence Agencies—The FFIEC will build upon existing relationships with law enforcement and

intelligence agencies to share information on the growing cybersecurity threats and response techniques.

Shortly after, on June 30, 2015, the FFIEC released its Cybersecurity Assessment Tool (CAT)[24] to help institutions identify risks and assess cybersecurity readiness.[25] The CAT was intended for use by financial institutions of all sizes and was designed to be dynamic so that it could be updated as threats, vulnerabilities, and operational environments became more sophisticated. It also served to help examiners in their assessments of cyber risk. The FFIEC published resources to encourage use of the CAT such as "an executive overview, a user's guide, an online presentation explaining the Assessment, and appendices mapping the Assessment's baseline maturity statements to the FFIEC Information Technology Examination Handbook, mapping all maturity statements to the National Institute of Standards and Technology's Cybersecurity Framework, and providing a glossary of terms."[26]

On October 26, 2016, the federal banking regulators - OCC, Fed, and FDIC - published an advance notice of proposed rulemaking (ANPR) to enhance cyber risk management standards for large and interconnected entities under their supervision and the entities' service providers.[27] The ANPR covered the following topics: cyber risk governance; cyber risk management; internal dependency management; external dependency management; and incident response, cyber resilience, and situational awareness.

Meanwhile, the FFIEC updated the CAT in 2017 to address changes to the FFIEC IT Examination Handbook and provide additional response options and practices and processes that represented the practices of the institution in supporting its cybersecurity activity assessment.[28]

The ANPR has not yet come to fruition as a proposed or final rule, however, in March 2020, the Fed was expecting further action on the enhanced standards.[29]