October 8, 2021

Board of Governors of the Federal Reserve System, Docket No. OP-1752
Federal Deposit Insurance Corporation, FDIC RIN 3046-ZA26
Office of the Comptroller of the Currency, Docket ID OCC-2021-0011

VIA ELECTRONIC SUBMISSION

Interos Comments Regarding Proposed Interagency Guidance on Third-Party Relationships: Risk Management

Please accept our comments on the above-noted proposal based on our work as an organization focused on improving supply chain risk management and operational resilience. We would like to commend them for their thoughtful and well-written proposed guidance. That said, we have a number of substantive comments which we believe would strengthen and enhance the proposed guidance and contribute to driving a risk-based approach as third-party risk management continues to evolve.

In summary, our comments are organized in three sections: General Comments, Specific Comments (on certain questions for which the Proposal requests feedback), and Additional Topic which Merit Consideration.

General Comments

1. Change Third-Party Risk Management (TPRM) to Supply Chain Risk Management (SCRM) because this term more accurately describes the subject matter. It also aligns with the NIST 800:53 R5 addition of the "supply chain risk management control family." One can elaborate further on the definition of a 'third party' for clarity of what constitutes “business relationships”.

2. Financial services industry concentration risk in the aggregate, while perhaps beyond the scope of this regulatory guidance, nevertheless bears mention. Suppliers supporting critical activities across multiple financial institutions pose systemic risk to the banking system. Including reference to this point in a FAQ would raise awareness of and concern for this reality across banking organizations.

3. Environmental, Social and Governance (ESG) risks, while not specifically referenced in regulatory guidance to date, are an area of increasing financial services industry focus. Boards of Directors and investors are increasingly holding management accountable on these topics, some of which directly overlap and are in scope of current regulations. Further, financial institutions failing to monitor their loan exposure in an ESG context can result in potential significant additional financial exposure and loss.

Specific Comments:

Page 8: Introduction: *"A prudent banking organization appropriately manages its third-party relationships, including addressing consumer protection, information security, and other operational risks."*

> **Comment:** The proposed guidance does not spell out what the "other operational risks" are. This is a gap and an opportunity to elaborate on what other operational risks financial institutions should be aware of and focused on managing with regard to their supply chain partners. These include financial, governance (as well as the larger ESG topic), compliance, and geographic / concentration risks.

Page 11, Question 1*: "…In what areas should the level of detail be increased or reduced?"*

> **Comment:** There is no direct mention of continuous monitoring of third parties and subcontractors, including but not limited to data hosting providers, network providers, BPO service providers (together, the extended supply chain) in the proposed guidance. In the current environment, continuous monitoring is among the most effective processes and tools for managing operational risks, particularly emerging risks (e.g., SolarWinds, Kaseya).

Page 11, Question 2: *"What other aspects of third-party relationships, if any, should the guidance consider?"*

> **Comment:** View TPRM as a subset of Supply Chain Risk Management (SCRM), which it is. Enhance the guidance for what constitutes a 'critical activity' to provide a more quantitative way of making this determination. For example, if a third party (or subcontractor) has in its possession customer PII or if it has direct access to the infrastructure of the banking organization, that becomes a critical activity as it provides a means of either disabling customers or disabling the operations capability of the bank.

Page 12: Question 5: "*What changes or additional clarification, if any, would be helpful regarding the risks associated with engaging with foreign-based third parties?"*

> **Comment:** Foreign-based hosting of bank customer information; ability to recover customer and bank information in the event of bankruptcy; appropriate legal protections for customer information; ability to prosecute data breach cases; OFAC; potential NDAA Section 889 issues if extended to banking.

Page 13: Question 6: *"How could the proposed guidance better help a banking organization appropriately scale its third-party risk management practices?"*

> **Comment:** By allowing banking organizations to adopt continuous monitoring of their suppliers in place of periodic risk assessments. This would permit scarce resources to be allocated to timely and effective processes and tools and increase scalability of risk management activities.

Page 13: Question 8: *"In what ways could the proposed description of critical activities be clarified or improved?"*

> **Comment:** The definitions provided for critical activities could be enhanced to provide concrete examples, such as (1) sharing PII / confidential information with third parties / subcontractors,

possibly setting a threshold number of records; (2) allowing a third party / subcontractor to have access to a bank's network infrastructure, introducing the possibility of network compromise.

Page 13, Question 10: *"What revisions to the proposed guidance, if any, would better assist banking organizations in assessing third-party risk as technologies evolve?"*

Comment: Incorporate and allow for the use of continuous monitoring processes and tools to perform both third party and subcontractor ongoing monitoring of all operational risks.

Page 14, Question 12: *"What risk management practices do banking organizations find most effective in managing business arrangements in which a third party engages in activities for which there are regulatory compliance requirements? How could the guidance further assist banking organizations in appropriately managing the compliance risks of these business arrangements?"*

Comment: Real-time, continuous monitoring of the extended supply chain for negative supplier news, prohibited and restricted entities and transactions, undisclosed ownership stakes and other instances of supplier non-compliance with banking rules and regulations.

Page 16, Question 15: (a) *How could the proposed guidance be enhanced to provide more clarity on conducting due diligence for subcontractor relationships?*

Comment: Incorporate and allow for the use of continuous monitoring processes and tools to perform both third party and subcontractor due diligence and ongoing monitoring of all operational risks.

Page 16, Question 15 (b): *To what extent would changing the terms used in explaining matters involving subcontractors (for example, fourth parties) enhance the understandability and effectiveness of this proposed guidance?*

Comment: Stop using the terms fourth party, nth party, etc. Standardize on third parties (as there is a need for this term to describe all business relationships); and use "extended supply chains". Adopt for the entire guidance the term Supply Chain Risk Management to align with the NIST 800:53 new control family of the same name.

Page 16, Question 15 (c): *What other practices or principles regarding subcontractors should be addressed in the proposed guidance?*

Comment: A statement that, as for third parties, the use of continuous monitoring both to perform due diligence and especially for ongoing monitoring represents an effective controls environment. Continuous monitoring provides the ability to know on a daily basis the status of a banking organization's third-party inventory. Most important, with examples of systemic vulnerabilities such as SolarWinds and Kaseya, by adopting continuous monitoring, banks will have the ability in near real-time to identify affected third parties and subcontractors within their supply chains.

Page 16, Question 16: "*What factors should a banking organization consider in determining the types of subcontracting it is comfortable accepting in a third-party relationship? What additional factors are relevant when the relationship involves a critical activity?"*

Comment: Important factors to consider are whether the third party is sharing PII or confidential information with the subcontractor or whether the third party has granted access to the bank infrastructure to the subcontractor.

Page 17, Question 18: *"To what extent should the concepts discussed in the OCC's 2020 FAQs be incorporated into the guidance? What would be the best way to incorporate the concepts?"*

Comment: Since the level of detail provided in the FAQs is extensive, the FAQs would be best left as FAQs to guide banking organizations as they work to comply with regulations.

Pages 19-20: Section B - Background: *"It is therefore important for a banking organization to identify, assess, monitor, and control the risks associated with the use of third parties and the criticality of services being provided."*

Comment: What happens when a banking organization fails to control risks? Address this by adding: "and in the event of a failure to control risks, respond and recover in a timely manner." This creates a stronger link with the NIST Cybersecurity Framework.

Page 30: Section j Operational Resilience: *"Consider risks related to technologies used by third parties, such as interoperability or potential end of life issues with software programming language, computer platform, or data storage technologies that may impact operational resilience."*

Comment: Add a reference to ransomware here: "that may impact operational resilience, including ransomware attacks upon critical activities operated within bank's extended supply chains." The rise and increasing frequency of ransomware attacks and their societal impact merits reference within the proposed guidance.

Page 32: Section n – Reliance on Subcontractors: *"Evaluate whether additional risks may arise from the third party's reliance on subcontractors and, as appropriate conduct similar due diligence on third parties' critical subcontractors…"*

Comment: If as is mentioned in item #6 below, periodic risk assessments are viewed as a requirement for third party onboarding, then this statement may be construed as a requirement to perform periodic assessments for critical subcontractors. This would add significant due diligence burdens to banking organizations, when, as mentioned in #6 below, there are alternative and more effective ways of performing due diligence and ongoing monitoring.

Page 34 Section a – **Nature and Scope of the Agreement:** In light of the May 12, 2021 "Presidential Order on Improving the Nation's Cybersecurity, section 4: Enhancing Software Supply Chain Security" section (e) and specifically subsection (vii) "providing a purchaser a Software Bill of Materials (SBOM) for each product directly or by publishing it on a public website", along with section (f) "Within 60 days of the date of this order, the Secretary of Commerce, in coordination with the Assistant Secretary for Communications and Information and the Administrator of the National Telecommunications and Information Administration, shall publish minimum elements for an SBOM.", add a provision for contracts between banking organizations and third parties software providers that they provide an SBOM as part of the contract. This will allow the ability to determine all versions of third party and subcontractor software used to provide a service to the banking organization, and to provide a mechanism for rapid response in the event of a software compromise, enhancing operational resilience.

Page 48 Section c – Independent Reviews: *"Understand and monitor concentration risks that may arise from relying on a single third party for multiple activities or from geographic concentration of businesses."*

> **Comment 1:** "…relying on a single third party throughout your extended supply chain, creating bottlenecks or for multiple critical…". This is an important point because individual suppliers may operate at different tiers within a banking organization, and this may not be readily apparent when just considering 'third-party usage'.
>
> **Comment 2:** Clarify / add "…geographic concentration of businesses**,** such as geopolitical issues, catastrophes, restrictions by country." Does this mean multiple banking organization businesses located in a specific geography and making reliance upon a key (or a small number of) supplier(s) with only a limited geographic presence for critical activities? Or does it mean multiple businesses making reliance on a supplier located in a specific, limited geography? Or both?

Pages 48: Section c - Independent Reviews: *"Confirming appropriate staffing and expertise to perform risk assessment, due diligence, contract negotiation, and ongoing monitoring and management of third parties".*

> **Comment:** Periodic assessments appear to be mandatory under the proposed regulations. In today's environment, where many banking organizations continuously monitor their third parties and extended supply chains for new and emerging risks, performing periodic risk assessments yields little incremental value and is unresponsive to the increasing number of real-time risks banking organizations are exposed to. The periodic risk assessment approach also keeps banks focused on a compliance culture, ensuring they perform risk assessments and secondarily addressing the risks that are identified. Enhancing this requirement to either perform periodic assessments "or continuously monitor critical and other suppliers" gives flexibility to banks in their TPRM programs and encourages them to mitigate identified risks in near real-time on a continuous basis.

Pages 50: Ongoing Monitoring: *"Because both the level and types of risks may change over the lifetime of third-party relationships, banking organizations adapt their ongoing monitoring practices accordingly. Management's monitoring may result in changes to the frequency and types of reports from the third party, including service-level agreement performance reports, audit reports, and control testing results. As part of sound risk management, banking organizations dedicate sufficient staffing with the necessary expertise, authority, and accountability to perform ongoing monitoring, which may include periodic on-site visits and meetings with third-party representatives to discuss performance and operational issues."*

> **Comment:** The 'Ongoing Monitoring' section of the proposed guidance does not directly address the increasing need for real-time monitoring of supplier risks (i.e., continuous monitoring processes). The Threat and Vulnerability Assessment (TVA) environment now requires real-time notification and remediation actions. Evidence Solar Winds, Kaseya, and other recent security breaches. Regulatory guidance on this key control is necessary for critical third parties and their extended supply chains to protect both banking organizations and their customer information across all relevant operational risk domains.

Page 54: Supervisory Reviews of Third-Party Relationships: *"Assess the banking organization's ability to oversee and manage its relationships."*

Comment: In the third-party and extended supply chain portfolio, there is an opportunity to introduce portfolio risk management using qualitative and quantitative techniques and processes. By developing a weighting and scoring process based on the risk and complexity of third-party relationships, aligned with functional categorization of suppliers into risk domains and leveraging criticality and the control environment in place at suppliers, a score can be assigned to each third party, risk domain and the overall third-party portfolio. The complexity of this portfolio risk-scoring model and process is an individual banking organization decision; however, measurement of changes in portfolio risk dynamically using data analytics techniques can be used to build a dynamic portfolio risk scoring model. This approach needs to consider regulatory model guidance, 2011-12, Sound Practices for Model Risk Management, but has the potential significantly enhance third-party portfolio risk management on an ongoing basis.

Page 54: Supervisory Reviews of Third-Party Relationships: *"carefully review the banking organization's plans for appropriate and sustainable remediation of such deficiencies, particularly those associated with the oversight of third parties that involve critical activities."*

Comment: Adoption and enhancement of a Resilience Operations Center (ROC) model to automate and sustainably manage third party and extended supply chain remediation process workflow would make a significant contribution to ensuring banking organizations are accountable for, address and remediate identified operational risks in a timely manner. It would also provide visibility and assurance to regulators "for appropriate and sustainable remediation of such deficiencies". Issue remediation is commonly the weakest aspect of TPRM programs and would benefit from more regulatory focus in the proposed guidance. The ROC leverages and builds upon the Security Operations Center (SOC) model already implemented within banking organizations to automate and manage identified security risks not just through remediation. It also provides a mechanism for ensuring lessons learned from incidents become incorporated into operations processes going forward. Leveraging the ROC approach would also be helpful in moving banks away from focusing on TPRM program compliance and to effective and efficient risk management practices.

Additional topics which merit coverage in the proposed guidance:

Monitoring for occurrence of trigger events in TPRM, indicating potential third-party issues, and steps required to address such trigger events, including:

- Data breaches
- Financial performance degradation
- Data center moves
- Mergers, Acquisitions, or Divestiture (MAD)
- Key personnel turnover and resulting loss of subject matter expertise, impacting operational resilience
- Data governance and privacy –add evaluation of specific countries' laws on data protection, to determine the potential for host country government requirements to transfer confidential or restricted information to the government and its impact, where no due process exists. GDPR does not cover this.

***

Interos respectfully requests that the agencies consider the foregoing comments in respect of the Proposed Guidance. Thank you for this opportunity to comment and provide feedback. Should you wish to discuss any of these comments further, please do not hesitate to contact us.

Interos