International Bancshares Corporation

January 13, 2017

Robert deV. Frierson
Secretary
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW
Washington, DC 20551
regs.comments@federalreserve.gov
RE: IBC Comments on Enhanced Cyber Risk Management Standards, Docket No. R-1550, RIN 7100-AE-61

Legislative and Regulatory Activities Division
Office of the Comptroller of the Currency
400 7th Street SW
Suite 3E-218, Mail Stop 9W-11
Washington, DC 20219
regs.comments@occ.treas.gov
RE: IBC Comments on Enhanced Cyber Risk Management Standards, Docket ID OCC-2016-0016

Robert E. Feldman
Executive Secretary
Federal Deposit Insurance Corporation
550 17th Street NW
Washington, DC 20429
comments@fdic.gov
RE: IBC Comments on Enhanced Cyber Risk Management Standards, RIN 3064-AE45

Ladies and gentlemen:

The following comments are submitted on behalf of International Bancshares Corporation (IBC) (NASDAQ: IBOC), a multi-bank financial holding company headquartered in Laredo, Texas with five bank subsidiaries operating throughout Texas and Oklahoma that are supervised by the FDIC as their primary federal regulator. IBC appreciates the opportunity to comment on the Agencies' joint advance notice of proposed rulemaking (ANPR) regarding enhanced cyber risk management standards for certain entities supervised by the Agencies. As described in the ANPR, the Agencies are considering establishing these enhanced standards for "the largest and most interconnected entities under their supervision, as well as for services that these entities receive from third parties."

P.O. DRAWER 1359, LAREDO, TEXAS 78042-1359 (956) 722-7611

The Agencies are considering implementing the enhanced standards using a tiered approach, in which more stringent standards would be imposed on the systems of covered entities that are deemed critical to the functioning of the financial sector.

As the Agencies consider which entities to subject to the enhanced standards, we urge the Agencies to make clear that the standards do not apply to smaller financial institutions — whose cyber risks, while not insignificant, do not threaten the financial system as a whole in the same way as larger and more systemically significant financial institutions. Institutions like IBC are already subject to a panoply of requirements regarding cybersecurity, including multiple federal and state laws, regulations, and supervisory expectations, and we allocate a substantial amount of resources to this area. Adding more, and heightened, requirements would be unduly burdensome, unwarranted, and unhelpful to the economy as a whole. The Agencies' proposal appears more properly addressed to larger institutions whose operations — and disruption of those operations — directly and indirectly affect more financial industry participants than IBC's operations would, and in a more significant way. In addition to avoiding explicit coverage of smaller entities, it is of vital importance that the Agencies avoid drafting ambiguities that could arguably be read as to sweep in smaller institutions.

Also, even if the framework as contemplated by the ANPR does not cover IBC and its subsidiaries, we nonetheless would like to take this opportunity to provide our perspective on certain substantive aspects of the standards. One reason is that even if the ultimate thresholds for coverage exclude IBC, we anticipate that there may be a "spillover" effect to smaller institutions, in which, for instance, the Agencies may expect smaller banks to incorporate some of the standards as best practices. There may also be a "trickle-down" effect as the covered entities, and/or their service providers, impose requirements on smaller banks with which they engage. Therefore, we believe that the perspective of smaller institutions on the standards as proposed is important for the Agencies to consider as well.

QUESTIONS ON THE SCOPE OF APPLICATION

1. How should the agencies consider broadening or narrowing the scope of entities to which the proposed standards would apply? What, if any, alternative size thresholds or measures of risk to the safety and soundness of the financial sector and the U.S. economy should the agencies consider in determining the scope of application of the standards? For example, should "covered entity" be defined according to the number of connections an entity (including its service providers) has to other entities in the financial sector, rather than asset size? If so, how should the agencies define "connections" for this purpose?

Whether the Agencies opt to define "covered entity" in terms of factors *in addition* to asset size, asset size should be a necessary threshold factor for coverage. Smaller institutions do not pose the same types of system-wide risks related to cybersecurity as do the largest financial institutions, such as those considered systemically important financial institutions (SIFIs). We request that the Agencies recognize this in carefully drafting coverage language.

In the ANPR, the Agencies state that the asset size threshold being considered is currently $50 billion, measured on an enterprise-wide basis. While we would not object to a $50 billion threshold if measured at the *individual* institution level, we respectfully suggest that the number be increased if the measure is to be on a consolidated basis.

Establishing the asset size threshold as $50 billion on a consolidated basis could impose unwarranted burden on smaller entities that do not raise the concerns discussed in the ANPR and in the *Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System* (Sound Practices Paper), which the Agencies quote in the ANPR, such as "the immediate systemic effects of a wide-scale disruption on critical financial markets[.]"[1] It is possible that a bank holding company may have multiple small community bank subsidiaries whose asset size, in the aggregate, reaches $50 billion, yet none of the institutions, individually or collectively, would pose the types of risks of system-wide disruption that the ANPR appears meant to address.

The standards also should explicitly state that the Agencies must review the size threshold periodically and adjust it upward for inflation, as appropriate. The standards should also explicitly state that the Agencies cannot *decrease* the asset size threshold — which would expand coverage of the standards — without first issuing a new proposal for public comment.

As to whether "covered entity" should be defined "according to the number of connections an entity (including its service providers) has to other entities in the financial sector," we caution that such a definition is likely to cast too broad a net. In particular, the parenthetical "(including its service providers)" is troubling. Community banks typically use one or more service providers. This may be for a number of reasons, including having more limited in-house resources than larger institutions. Many of these service providers are often service providers that deal with a wide variety of entities, including SIFIs and other large financial institutions. Smaller institutions may rely on such service providers precisely because they are so widely used, and perceived to be more reliable and to have a broad perspective on standards and developments across the industry. By their nature, then, these vendors would have many relationships with entities in the financial sector. It is unclear whether the Agencies would define such relationships as "connections," but if so, it raises the possibility that mere use of such vendors, even by a small bank, could trigger coverage under these standards.

We therefore urge the Agencies to refrain from using any language in the rule that states or implies that a financial institution can become a "covered entity" under the rule merely due to its use of any particular service provider, such as one with a certain number of "connections."

2. What are the costs and benefits of applying the standards to covered entities on an enterprise-wide basis? If the agencies were to consider exempting certain subsidiaries within a covered entity from the standards, what criteria should be used to assess any such exemptions? What safeguards should the agencies require from a subsidiary seeking to be exempted from the standards to ensure that an exempted subsidiary does not expose the covered entity to material cyber risk?

---

[1] 81 FR 74315 at 74318 (Oct. 26, 2016), quoting the *Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System.*

As we discuss above in our response to Question 1, we ask the Agencies to either measure asset size for the purposes of coverage on an individual, non-consolidated, basis, or to increase the asset size threshold.

Exempting certain subsidiaries within a covered entity sounds appealing in theory, such as where a subsidiary is a smaller entity with less potential impact on the financial system as a whole. However, it is unclear whether such an exemption would be feasible in practice. This approach seems most plausible in a situation where a covered entity does not interact at all with a given subsidiary, including no sharing at all of any data or systems. It is unclear how common such a situation would be. By contrast, where a covered entity and its subsidiary share data, systems, service providers, or other functionality, it seems that the "exempted" subsidiary will still have to comply with the standards so that the covered parent entity may fulfill its obligations under the standards.

It also seems plausible that the supervising agency of the supposedly exempted subsidiary would still inquire of that subsidiary how the subsidiary is meeting the enhanced standards. Rather than take such a piecemeal approach, it would seem most efficient to establish a framework whereby only the top-tier entity is to be examined for conformance with the standards. Particularly if the Agencies do define "covered entity" to mean an entity with $50 billion or greater in assets on a consolidated basis, it may be more efficient to place direct responsibility only on the top-tier parent entity rather than also holding each (smaller) subsidiary responsible.

4. What are the most effective ways to ensure that services provided by third-party service providers to covered entities are performed in such a manner as to minimize cyber risk? What are the advantages and disadvantages of applying the standards to services by requiring covered entities to maintain appropriate service agreements or otherwise receive services only from third-party service providers that meet the standards with regard to the services provided, rather than applying the requirements directly to third-party service providers?

All of the Agencies have described in detail, repeatedly, their supervisory expectations regarding third-party risk management. The Agencies have made clear that financial institutions remain responsible for compliance with all applicable laws and regulations, and for implementing all applicable supervisory guidance, regarding any activity those institutions conduct, whether directly or through a third party. Therefore, to the extent a given financial institution will be subject to certain enhanced cybersecurity standards, the institution will already need to ensure that it meets such standards in connection with any activity it carries out through use of a third-party service provider.

Given that, the Agencies' reference to "requiring covered entities to…receive services only from third-party service providers that meet the standards with regard to the services provided" is particularly confusing. As noted above, under the Agencies' long-established third-party risk management standards, financial institutions already are expected to ensure that they, and their service providers, meet all applicable legal and supervisory requirements for any activity they conduct.

Unless the Agencies are contemplating increased direct examination of third-party service providers, the approach described in the quoted language would not appear to markedly differ from the Agencies' existing supervisory expectations regarding third-party risk management. Thus, it would be helpful for the Agencies to clarify whether they are intending to directly examine service providers, pursuant to their authority under the Bank Service Company Act or to some other authority. If not, it seems that the Agencies would not need to do any more than issue standards applicable to their supervised institutions; the institutions would remain responsible for overseeing their service providers to ensure their own compliance responsibilities were met.

QUESTIONS ON SECTOR-CRITICAL SYSTEMS

12. In some cases, entities, such as smaller banking organizations, may provide services considered sector-critical services either directly to the financial sector or through covered entities. What criteria should the agencies use to evaluate whether a financial entity that would not otherwise be subject to the enhanced standards should be subject to the sector-critical standards? How should the agencies weigh the costs of imposing the sector-critical standards to such smaller banking organizations against the potential benefits to the financial system?

As a smaller financial institution, we are particularly concerned about the potential import of this question. In the ANPR, the Agencies' discussion of what may be "sector-critical," also described as "critical to the functioning of the financial sector," seems to leave open the possibility that even some day-to-day activities of smaller banking organizations could be deemed "sector-critical."

In discussing their thinking about what may be "sector-critical," the Agencies observe that "a technology failure or cyber-attack at one covered entity could have wide-ranging effects on the safety and soundness of other financial entities, both within and outside the United States. While this interconnectedness warrants comprehensive cyber risk management by all financial market participants, it is especially important in the case of covered entities with sector-critical systems." As seemingly acknowledged in this passage, it could be argued to some extent that all financial institutions have some interrelation and potential impact on other participants and on the market as a whole. That is presumably why financial institutions are already subject to so many laws, regulations, and supervisory policies, on both the federal, state, and even local levels, that relate in some way to cyber risk.

More specifically, the Agencies "are considering whether systems that support the clearing or settlement of at least five percent of the value of transactions (on a consistent basis) in one or more of the markets for federal funds, foreign exchange, commercial paper, U.S. Government and agency securities, and corporate debt and equity securities, should be considered sector-critical systems for the purpose of the sector-critical standards.

The agencies also are considering whether systems that support the clearing or settlement of at least five percent of the value of transactions (on a consistent basis) in other markets (for example, exchange-traded and over-the-counter derivatives), or that support the maintenance of a significant share (for example, five percent) of the total U.S. deposits or balances due from other depository institutions in the United States, should be considered sector-critical systems." If the Agencies stopped their analysis there, it could lead to a reasonable conclusion: establishing the cutoff as consistently clearing or settling at least five percent of transactions in one or more given markets would appear to properly exclude smaller entities whose activities do not pose the type of widespread risk that the Agencies appear concerned with in this aspect of the standards.

However, the Agencies go on to say that they are also contemplating expanding the "sector-critical" concept to include "additional factors to identify sector-critical systems, such as substitutability and interconnectedness. Systems that provide key functionality to the financial sector for which alternatives are limited or nonexistent, or would take excessive time to implement (for example, due to incompatibility) also could have a material impact on financial stability if significantly disrupted. Systems that act as key nodes to the financial sector due to their extensive interconnectedness to other financial entities could have a material impact on financial stability if significantly disrupted." This focus on "interconnectedness" could have the unintended consequence of drawing smaller entities into the standards due to their reliance on other entities, including service providers that deal with numerous other entities. We respectfully request that the Agencies limit their definition of "sector-critical" to those entities whose activities comprise a significant share of transactions of the United States economy as a whole, such as the five-percent threshold discussed above.

QUESTIONS ON STANDARDS FOR SECTOR-CRITICAL SYSTEMS OF COVERED ENTITIES

30. What impact would a two-hour RTO have on covered entities' use of third-party service providers? What challenges or burdens would be presented by the requirement of a two-hour RTO for covered entities who rely on third-party service providers for their critical systems? How should the agencies weigh such costs against other costs associated with implementing the enhanced standards outlined in this ANPR?

As stated in the ANPR, the Agencies are considering two tiers of standards, with more stringent standards to apply to systems of covered entities that are critical to the functioning of the financial sector. First, the agencies are considering a requirement that covered entities minimize the residual cyber risk of sector-critical systems by implementing the most effective, commercially available controls to mitigate the risk of a disruption or failure due to a cyber event.

As a second sector-critical standard, the Agencies are considering requiring covered entities to establish a recovery time objective (RTO), described as the "amount of time in which a firm aims to recover clearing and settlement activities after a wide-scale disruption with the overall goal of completing material pending transactions on the scheduled settlement date." The Agencies are considering setting an RTO of two hours for covered entities for their sector-critical systems to recover from a disruptive, corruptive, or destructive cyber event.

While, generally, financial institutions certainly would prefer to have their systems back up and running in the shortest time possible after a cyber event — and will face harm to their businesses and reputations from any delay — the timeframe for such restoration is not completely within the control of the financial institution. For one thing, many smaller banks rely substantially on the services of third-party service providers to maintain their core systems and operations.

Even if this RTO is not imposed on smaller entities, it seems conceivable that regulators may eventually also expect smaller entities to meet a comparable RTO. We fear that this will mean requiring an unreasonably short turnaround time and penalizing those institutions that cannot meet such a timeframe. We encourage the Agencies to make any RTO standard reasonable under the circumstances, and to take into account the factors that may be outside the control of the supervised institution itself.

In closing, again, we urge the Agencies to make clear that the standards do not apply to smaller banking organizations such as IBC. More broadly, we request that the Agencies make any standards reasonable.

Thank you again for your consideration of our comments on this ANPR. We look forward to reviewing the proposed rule when it is issued and providing additional comments at that time.

Sincerely,

Dennis E. Nixon
Chairman, International Bancshares Corporation