February 17, 2017

Robert deV. Frierson
Secretary
Board of Governors of the Federal Reserve system
20th Street and Constitution Avenue NW
Washington, DC 20551

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

Robert E. Feldman
Executive Secretary
Attention: Comments
Federal Deposit Insurance Corporation
550 17th Street NW
Washington, DC 20429

Via e-mail to: regs.comments@federalreserve.gov (Board of the Federal Reserve (Board))
regs.comments@occ.treas.gov (Office of the Comptroller of Currency (OCC))
Comments@fdic.gov (Federal Deposit Insurance Corporation (FDIC))

RE: Docket No. R-1550 and RIN 7100-AE-61 (Board)
Docket ID OCC-2016-0016 (OCC)
RIN 3064-AE45 (FDIC)

ITI comments in response to Banking Agencies' Advanced Notice of Proposed Rulemaking regarding *Enhanced Cyber Risk Management Standards*

Dear Mr. Frierson, Mr. Feldman et al.:

The Information Technology Industry Council (ITI) appreciates the opportunity to respond to the Advanced Notice of Proposed Rulemaking (ANPR) jointly issued by the Board of Governors of the Federal Reserve System (Board), Office of the Comptroller of Currency (OCC), and Federal Deposit Insurance Corporation (FDIC) (collectively, the "Agencies") regarding Enhanced Cyber Risk Management Standards for large and interconnected entities under their supervision and those entities' service providers (the "Enhanced Standards"). We appreciate, and share, the Agencies' goals of increasing the operational resilience of entities under their regulatory authority such as large banking institutions, and reducing the impact on the financial system of cyber events experienced by such entities. Respectfully, however, we are concerned with the Agencies' contemplated extension of the Enhanced Standards to

third-party service providers in other industries, including the IT sector. Additionally, we are concerned by the apparent redundancy of the Agencies' approach given the numerous existing cybersecurity risk management guidance and requirements already imposed on the financial sector, as well as by the inflexibility and prescriptiveness of the compliance-focused, rather than risk-based, regime of Enhanced Standards under consideration.

ITI is the global voice of the tech sector. We are the premier advocate and thought leader in the United States and around the world for the information and communications technology (ICT) industry. ITI's members comprise leading technology and innovation companies from all corners of the ICT sector, including hardware, software, digital services, semiconductor, network equipment, cybersecurity, Internet companies, and companies using technology to fundamentally evolve their businesses. Cybersecurity and cybersecurity technology are critical to ITI members. Facilitating the protection of our customers (including governments, businesses, and consumers), securing and protecting the privacy of our customers' and individuals' data, and making our intellectual property, technology, and innovation available to our customers to enable them to improve their businesses are core drivers for our companies. Consequently, ITI has been a leading voice in advocating effective approaches to cybersecurity.

Cybersecurity is rightly a priority for the Agencies, as it is for the United States government (USG) and governments around the globe. As companies that provide products and services to large financial services firms and other entities within the regulatory purview of the Agencies, we share the Agencies' interest in the safe and sound operation of these entities, the integrity of the financial system, and the protection of consumers. Financial institutions often choose to address cybersecurity risks and other operational risks today through the use of sophisticated third-party services providers, including some ITI companies, who offer innovative security technology, services, and risk management expertise which may oftentimes be in short supply within the financial institutions themselves. While we understand the Agencies' interest in ensuring that the entities they supervise are effectively addressing the dynamic cybersecurity risks facing us all, we believe reconsideration of the approach embodied in the ANPR is warranted, particularly as applicable to third-party service providers. If effectuated in an obligatory, inflexible fashion, the requirements in the ANPR may discourage and limit the ability of these service providers from continuing to innovate, develop, and expand technologies aimed at improving and enhancing cybersecurity and data protection, having the unintended effect of increasing these entities exposure to cybersecurity risks. Even for those third-parties who are not so discouraged, compliance with the ANPR's Enhanced Standards will doubtless increase the costs of such services to covered entities.

ITI submits our comments against the foregoing backdrop. We have not endeavored to answer all the questions in the ANPR, but instead concentrate our comments on the questions focused on third-party impacts of the proposed Enhanced Standards. We have also commented on those questions on which we believe our insights regarding best practices and standards for cybersecurity risk management could prove useful in informing the Agencies' ongoing efforts in this area. We organize our discussion of these issues under the overarching topic headings identified by the Agencies, as appropriate, and offer our summary recommendations below.

Summary Recommendations

Orient Financial Sector Cybersecurity Approaches around the Cybersecurity Framework. The visionary work led by NIST, in cooperation with the private sector and other stakeholders, including those from the financial sector, to develop the voluntary Framework for Improving Critical Infrastructure Cybersecurity[1] (the "Framework") should anchor the Agencies efforts to help large financial institutions better manage cybersecurity risk and avoid systemic consequences of those risks, rather than serving as just another layer of inspiration. The Framework leverages public-private partnerships, is grounded in consensus risk management principles, and helps foster innovation due to its flexibility and basis in global standards, including ISO 27001. The Framework has also consistently been lauded for providing a common language to better help organizations comprehend, communicate and manage cybersecurity risks, including by other financial sector agencies including the SEC and FFIEC.

Eliminate or Clearly Narrow the Applicability of the Enhanced Standards to Third-Parties. The Agencies propose *direct* applicability and enforcement of the Enhanced Standards not only to and against Covered Entities within their regulatory purview, but to and against third-party service providers of varying sizes in multiple other sectors. This "one-size fits all" scheme effectively substitutes the Agencies' judgment for that of the entities who are best situated to identify, assess, evaluate, and address the risks posed by third-party service providers. This would be a major, unprecedented and arguably inappropriate expansion of the Agencies' current regulatory powers, with little justification for such expansion offered beyond the "interconnectedness" of entities. Interconnectedness alone should not serve as a rationale for federal agencies to expand their sectoral regulatory powers to sweep interdependent entities from other sectors - such as IT, telecommunications and energy - in scope. There are practical reasons why endeavoring to cover third-parties as suggested in the ANPR will likely negatively impact the security of Covered Entities, including by: (1) increasing the costs of security services; and (2) impacting the availability of security services by discouraging certain providers from participating in the market. Alternative approaches for the Agencies to consider to address third-party risks more flexibly include encouraging the expanded the use of the Framework by third-party suppliers, and working with interagency partners to better understand the cybersecurity and implementation challenges faced by organizations of all sizes, and tailoring solutions accordingly.

Streamline Existing Financial Sector Cybersecurity Regulatory Efforts to avoid Duplicative Requirements. While the Framework has frequently been cited as providing a common language which can help companies better communicate risk management to improve cybersecurity internally (for instance with company executives or boards) and externally across their ecosystems (such as with business partners including suppliers), the Framework also provides a common language that the Agencies themselves can leverage. The potential of the Framework to provide a common language or taxonomy for policymakers has clearly not yet been fully realized. Promoting the Framework as a common language for policymakers can help align the Agencies' cybersecurity and risk management

[1] *See* NIST Framework for Improving Critical Infrastructure Cybersecurity, http://www.nist.gov/cyberframework/index.cfm

efforts by orienting them around a common point, and we urge the Agencies to use the NIST Cybersecurity Framework as such a cyber risk reference point.

Assess and Leverage Existing Policies and Build upon Existing Public-Private Partnerships to Address Financial Sector Cybersecurity Challenges. There has been significant progress on cybersecurity policy development in the U.S. over the past few years, notably EO 13636 that launched the Cybersecurity Framework, set up a process to designate Critical Infrastructure at Greatest Risk, and directed the streamlining of federal agencies' regulations. These new initiatives complement well-established public-private partnership activities, and together the public and private sector have just begun implementing and utilizing many of these policy instruments. There is much work yet to be done to achieve the "regulatory streamlining" envisioned by EO 13636. The Agencies should more fully assess this existing collaborative work before developing a new regulatory scheme for cybersecurity risk management across the financial sector and its most critical systems, and should support collaborative development of risk-based cyber programs rather than create prescriptive requirements.

Prioritize Investment in Cybersecurity Workforce Development and Training. The ANPR contemplates several requirements that will necessarily require the hiring of personnel with deep cybersecurity risk management expertise. However, there is currently a demonstrable shortfall of qualified cybersecurity experts in the U.S. The Agencies should work with federal and industry partners to prioritize paying down the "cyber debt" and reversing the current cybersecurity talent shortage. We recommend that the USG expand initiatives like the CyberCorps Reserve program and stand up a Cyber National Guard to train and recruit new talent to protect public and private digital infrastructure, and we urge the Agencies to consider lending their support to such initiatives.

Comments on Sections I, II - Background, Relationship to Existing Requirements and Guidance

The Agencies' stated purpose in considering the Enhanced Standards is to address potentially systemic consequences of catastrophic cyber attacks on large financial institutions – such entities are generally defined in the ANPR as those companies with total consolidated assets totaling $50B or more ("Covered Entities"). (ANPR 13). In other words, these proposed Covered Entities are those that were deemed "too big to fail" during and after the 2008-2009 financial crisis (*see* Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank)). Protecting these Covered Entities is a sensible policy goal to address acknowledged cybersecurity risk. ITI's members share this goal, and are constantly innovating security solutions aimed at protecting customers of every size across multiple sectors, and the security of the Internet ecosystem.

We share the Agencies' concerns regarding the security of financial systems and data. However, we recommend that the Agencies leverage the many existing cybersecurity risk management requirements already imposed on, and guidelines directed at, companies in the financial sector, such as those referenced below. Indeed, at the outset of the ANPR, the Agencies acknowledge that the financial sector is already subject to a multilayered web of guidance and regulatory requirements intended to address cybersecurity risks across the financial system.

The existing requirements summarized by the Agencies include:

- The Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework), which has been endorsed by the SEC and FFIEC amongst others.
- Uniform Rating System for Information Technology (URSIT Framework), issued through the FFIEC, used to uniformly assess IT risks across the financial sector.
- Federal Financial Institutions Examination Council's Information Security Booklet (FFIEC Guidance) updated in September 2016 to provide a tool for financial institutions to implement a cybersecurity program consistent with the Cybersecurity Framework.
- Federal Interagency Guidelines Establishing Information Security Standards, issued pursuant to the Gramm-Leach-Bliley Act of 1999 (GLB) and requiring insured depository institutions to implement information security programs and GLB safeguarding requirements. (ANPR 9-10)
- Federal Reserve, OCC and SEC Interagency Paper on Sound Practices to strengthen the Resilience of the U.S. Financial System ("Sound Practices Paper") (ANPR 12)
- Committee on Payments and Market Infrastructures, Board of the International Organization of Securities Commissions "guidance on cyber resilience for financial market infrastructures." (ANPR 11-12)
- The Agencies also acknowledge the recently proposed New York Department of Financial Services cybersecurity rules for financial institutions, which add another layer on top of the existing federal requirements and guidance.

While the Agencies are to be commended for teaming up to produce the ANPR (rather than taking a tripartite approach that would lead to further fragmentation), we are concerned that the approach contemplated would apparently not eliminate or clearly reconcile these existing requirements and guidelines, instead imposing yet another layer of compliance obligations on Covered Entities.

We recommend that, as a first step, the Agencies take a step back, and focus their efforts on evaluating, coordinating and reconciling existing approaches.

We also question whether the Agencies' apparent decision to make some of these existing sets of guidance "binding" makes sense in a threat environment that is acknowledged by the Agencies elsewhere in the ANPR to be both complex and rapidly changing. The prescriptive approach outlined in the ANPR seems contrary to the dynamic risk management processes the Agencies acknowledge are necessary throughout the document, and are embodied in several of the existing authorities, including the Cybersecurity Framework.

The Agencies indeed acknowledge that flexibility and continuous improvement are key aspects of cybersecurity risk management in their discussion of the Framework. "The CSF is intended to be customized by different business sectors and individual organizations to best suit their risks, situation, and needs." (ANPR 11). The Agencies also make plain that "the binding requirements set forth in the enhanced standards would be designed specifically to address the cyber risks of the largest, most interconnected U.S. financial entities." (ANPR 11). Yet just a few pages later, the Agencies

contemplate applying those same targeted Enhanced Standards to third-party providers of all sizes, across variegated industries.

The ANPR does not offer a compelling rationale to explain why prescriptive, binding standards are superior to the existing voluntary guidelines cited in the ANPR, such as the Framework or FFIEC tool. Further, the ANPR does not include an explanation as to how applying Enhanced Standards that are directed at large financial institutions to third-parties of varying sizes in diverse industries makes sense, from a risk management standpoint. We suggest that the Agencies seek to identify and articulate a rationale explaining how the existing sets of cybersecurity guidance cited in the ANPR are insufficient before adding another layer of regulatory requirements.

Comments on Section III. Scope of Application (Focused on 3rd parties)

Perhaps the most troubling aspect of the ANPR from ITI's perspective involves its proposed overbroad scope, particularly with respect to the Agencies' intended direct and indirect application of the Enhanced Standards to third-parties, including third-party service providers. The ANPR contemplates that the Enhanced Standards would apply directly to "critical service providers" and indirectly to many other third-party service providers, by requiring Covered Entities to verify that their service providers are also complying with the Enhanced Standards. Such obligations would likely be effectuated through contracts between the Covered Entities and third-party service providers, which is doubtless how many regulated entities currently ensure compliance with their obligations. However, the Agencies here propose *direct* applicability and enforcement of the Enhanced Standards to and against *both* Covered Entities and service providers – effectively imposing a "one-size fits all" contractual obligation on all providers via regulation.

This would be a major, unprecedented and arguably inappropriate expansion of the Agencies' current regulatory powers.

To explain why, it is helpful to recall the primary targets of the Enhanced Standards – large financial institutions with greater than $50 billion in assets. In other words, during and after the 2008-09 financial crisis these were the institutions that were deemed "too big to fail." Tying a Dodd-Frank style approach to cybersecurity risk management appears fundamentally flawed, as illustrated by the "interconnectedness" argument offered in the ANPR as partial justification for the expansive scope of the proposed regulations.

Interconnectedness does not obviate the need for all entities to engage in risk management. The Agencies acknowledge both the "interconnectedness" of entities in the modern digital age, as well as the "rapidly changing and complex threat landscape" in the ANPR. Correctly citing the interconnectedness of large financial institutions, the Agencies seem to lean on such interconnectedness as a rationale for applying the Enhanced Standards to third-parties and other entities. A possible justification is hinted at by the Agencies' pointing to the potential of subsidiaries to act as points of cyber vulnerability. Yet, given this interconnectedness, logically every third-party, SMB, international partner, etc. of a large financial institution would also constitute a potential point of vulnerability. If all of these entities are interconnected, and the Agencies contemplate applying the Enhanced Standards to

not only subsidiaries but to third-party services providers within financial institutions' ecosystems, then it is difficult to understand what the point is of setting $50B thresholds. Does the "threshold" approach really make sense, if everything is interconnected? Rather, the foregoing helps illustrate why, in every case, an evaluation of cyber risk must still occur.

Further, interconnectedness should not serve as a rationale for federal agencies to expand their sectoral regulatory powers to sweep "interconnected" or interdependent entities from other sectors - such as IT, telecommunications and energy - in scope. Leaving aside the substance and wisdom of the Enhanced Standards themselves, from neither a resources standpoint nor a cybersecurity risk management standpoint should Enhanced Standards directed at huge financial institutions extend to third-party service providers of varying and divergent sizes, with completely different business models, in diverse sectors. Just because these entities are interconnected does not mean they share the same risk profiles, critical assets, risk environments, etc. In other words, citing interconnectedness is not a substitute for the ongoing need for each of the entities to engage in a risk management analysis specific to their organizations.

Extending the ANPR to third-parties is likely to negatively impact security. There are practical reasons why endeavoring to cover third-parties as suggested in the ANPR will likely negatively impact the security of Covered Entities, including by: (1) increasing the costs of security services; and (2) impacting the availability of security services by potentially driving third-parties out of the market.

Increasing Costs. Sweeping all third-parties under the Agencies' regulatory purview will inevitably increase costs. Indirect and direct expansion of the Enhanced Standards to third-party service providers will increase compliance costs on the third-parties, who will in turn likely need to raise the prices of such services to Covered Entities. The net result of the scheme laid out in the ANPR will thus be that the standards (and costs) will in turn also be imposed on smaller financial and non-financial entities, thereby increasing the costs of cybersecurity across nearly all industries and industry participants.

Applying a regulatory compliance model inspired by the financial crisis, by applying banking regulations to third-party service providers in the IT sector and other sectors, is a flawed approach. For instance, this approach will substantially raise both compliance and operational costs for these entities, and may also require a significant expenditure on the part of all Covered Entities to restructure existing risk management programs and systems – even though the Agencies offer no evidence that such systems are insufficient - to comply with the Enhanced Standards. Of course, additional costs borne by the covered entities will ultimately be passed along to their clients as well.

Availability of Services. Applying the Enhanced Standards to third-party service providers could also have the adverse effect of compromising the ability of Covered Entities to obtain certain security services. First, this approach would place an additional burden on both the covered entities as well as their third-party providers. Many third-party providers to financial institutions are likely to be caught up in this net – a circumstance that may prove challenging to third-party suppliers that have had no prior experience in dealing with federal financial regulators. To illustrate, some third-parties provide innovative security services to large financial institutions. As written, the broad wording of the ANPR could be construed to apply to such companies, thus subjecting them to demonstrating all the same requirements targeted at the "too big to fail" financial entities, including, e.g., how their boards of

directors are providing governance of cyber risks, and how they are managing cyber risks at the business unit, enterprise-wide, and internal audit levels. These third-parties would then have to provide evidence of the foregoing to any financial sector client when requested, and would likely be contractually required to do so.

Further, implementing the Enhanced Standards directly against service providers will, as previously described, likely materially increase providers' costs. While some of these costs can be passed on to the Covered Entities, many may not be – such that many smaller service providers offering the most innovative cybersecurity products and services might well be pushed out of the market by the specter of costly, onerous regulatory requirements. Moreover, larger service providers, when faced with the decision of either absorbing the increased costs under the Enhanced Standards to innovate and provide cybersecurity solutions to Covered Entities, or sacrificing critical product research and development opportunities, may ultimately be forced to forego developing technologies needed by Covered Entities to keep pace with constantly evolving cyber threats. The entities that will ultimately be most impacted if this scenario comes to pass are the large financial institutions who the ANPR is targeted at in the first place, as they will not have the benefit of availing themselves of state-of-the art security solutions.

The Agencies Should Clarify and Reconcile Existing Authorities Regarding Third-Parties. At a minimum, the Agencies must add specificity to more clearly delineate which categories of service providers are in or out of scope. A good starting place might be the Bank Service Company Act (BSCA), 12 USC 1867(c), which has traditionally been applied to service providers providing core banking services to financial institutions – not supporting services such as IT or telecommunications. Third-party services that do not support core banking functions should not be affected by the proposed standards, neither directly nor indirectly. As for third-party services that do support core banking functions, financial institutions should ensure that these services enable them to comply with their obligations under the proposed standards.

The reality is that service providers' relationships with Covered Entities will vary widely, as will the size, type and geographical location of such service providers. The existing provisions of the FFIEC IT Examination Handbook and related federal regulatory guidance have, for decades, recognized this reality and provide an adequate framework for Covered Entities to govern their relationships with technology service providers in a prudent manner without imposing an inflexible "one size fits all" regulatory approach that will prove extremely burdensome for both Covered Entities and service providers. Ironically, adopting such an approach would push Covered Entities to be primarily focused on contract terms and provisions, as opposed to the quality of service and overall sophistication of service providers. Less sophisticated service providers will be more amenable to signing boilerplate contract terms proffered by a Covered Entity than will more established and sophisticated service providers.

Directly regulating service providers, as contemplated in the ANPR, would be an even more extreme step than effectively imposing a "one size fits all" contractual relationship on them. The BSCA provides federal regulators with the means to deal with the inadequacies of service providers when circumstances indicate this would be appropriate. Regulating technology service providers would be a radical departure from financial regulation as it has been practiced to date. Arguably neither the regulators nor the service providers are configured for such a departure from current practice, and such

a regulatory regime would be burdensome and costly and to both service providers and Covered Entities alike.

Alternative approaches to consider to address third-party risks. We do not intend to minimize the importance of addressing third-party cybersecurity risks – rather, we suggest alternative approaches to addressing this issue more flexibly and appropriately.

The Agencies could play an important and helpful role by helping to encourage the expanded the use of the Framework by third-party suppliers. In recognition of the importance of addressing global supply chain security concerns, some companies already have begun exploring how to expand Framework use with their suppliers. One option for the Agencies' consideration is to recommend that Covered Entities include the Framework in their third-party supplier cybersecurity requirements, provided the Agencies refrain from directing financial institutions to REQUIRE their suppliers to use the Framework. Two types of instances in which Covered Entities should themselves consider requiring use of the Framework across their supply chains are: (1) where an owner/operator has outsourced the management of any part of its operation via a managed services partnership; and (2) where the supplier is considered a critical business partner, such that any disruption of their business would affect the delivery of critical services. Companies can also take proactive steps to encourage use of the Framework across their ecosystem partners by, for example, integrating the Framework into their supplier guidelines.

Another option is for the Agencies to work with interagency partners including NIST, the Department of Homeland Security (DHS), the Small Business Administration, and others to better understand the cybersecurity and implementation challenges faced by organizations of all sizes, and consider ways to make the Framework more approachable for all organizations across the financial sector. Not all companies have mature programs or the technical expertise to keep up with the latest developments in cybersecurity – such as the Framework – to appropriately manage cyber risk. SMBs in particular have reported being confused and even overwhelmed by the size and complexity of the current Framework. Given the interconnected nature of the cyber ecosystem, we are keenly aware that cyber elements of the critical infrastructure can be compromised by weaknesses in smaller entities to which they are technologically connected. Given this fact, it is critical for us to create a sustainably secure cyber ecosystem for all entities, large and small.

Section IV. Sector-Critical Systems

As noted in the previous section, the most troubling aspect of this section of the ANPR is the Agencies' contemplated extension of systems-level requirements on so-called "sector critical systems" directly to third-party services providers.

However, other questions are also raised by the Agencies contemplated "sector-critical systems" designation scheme – the first being, who designates what is critical? This seems an open question, as per the ANPR the Agencies contemplate an either/or approach – either the entities will self-designate, or the agencies themselves will designate what are sector-critical systems. Both approaches have their flaws, and raise several questions. Are entities subject to the Enhanced Standards equipped to evaluate their interconnectedness, as well as the sector -criticality of their systems sufficiently? Might these entities have a disincentive to self-identify? From the Agencies' standpoint, what level of access might

be required to proprietary systems and information to make such designations, and do they possess the resources and expertise to capably make such designations?

As a threshold matter - if it is established that designations of critical systems are necessarily a good idea for better protecting such systems - a better approach would be for the entities and agencies to work together, in partnership. For instance, pursuant to EO 13636, DHS was charged with consulting with their critical infrastructure (CI) partners in the private sector to designate critical infrastructure at greatest risk (CIAGR) across the nation's CI sectors, including the finance sector. The initial designations of CIAGR were completed in 2013. Recounting the process for designating CIAGR pursuant to EO 13636 begs the question – hasn't a designation of critical systems as contemplated in the ANPR already been completed for the financial sector?

In any event, ITI believes it is pivotal to continue to replicate this partnership approach in addressing cybersecurity challenges. The NIST Framework provides an overarching structure, grounded in proven international standards and consensus best practices, to address organizational security across all critical infrastructure sectors, while providing adaptability and flexibility to meet the unique needs of each sector and address new threats. The US Government writ large and the Agencies specifically can provide leadership to make certain that efforts to improve cybersecurity leverage public-private partnerships and build upon existing initiatives and resource commitments. The IT industry, along with our peers in other industry sectors including the finance sector, leads and contributes to a range of significant public-private partnerships, including information sharing, analysis, and emergency response with governments and industry peers. Two key examples of public-private partnerships the government can prioritize to ensure greater coordination and collaboration across the government and industry are information sharing and analysis centers (ISACs), and sector coordinating councils (SCCs). Perhaps the Agencies can establish a process with DHS and impacted private sector stakeholders to more fully examine the sufficiency of the CIAGR designations that have already been made, and to determine whether there is utility in doing more work of this sort in the finance sector, from a risk management standpoint.

Section V: Enhanced Cyber Risk Management Standards

If the Enhanced Standards considered by the Agencies are indeed apt for large complex financial institutions – we reserve judgment on this question – this supposition serves to highlight why such standards are likely misplaced in the context of third-party service providers of varying sizes in divergent sectors, who doubtless face different risk profiles, possess different resources, etc., as mentioned above.

However, even with respect to application of the Enhanced Standards to the covered entities to which they were intended to apply, we believe the ANPR raises significant questions as to the viability of implementing many of these standards.

Cyber Risk Management and Workforce. For example, ensuring that business units maintain and have access to resources and staff with the skill sets needed to comply with the business units' cyber responsibilities seems like a noble, aspirational goal. However, it ignores the acknowledged cybersecurity workforce challenges facing the nation, and the reality that the entities the Agencies are

contemplating applying the Enhanced Standards to may not have access to the personnel needed to fully staff these functions.

This weakness is further magnified in the context of contemplated application of the Enhanced Standards to third-party service providers. If large banks can't hire, pay and retain such employees, it seems unrealistic to expect smaller companies with less resources to be able to comply with such requirements. Are there enough qualified personnel to fill all the positions amongst Covered Entities and interconnected ones as contemplated by the ANPR, to ensure the broad array of potentially impacted entities remain in compliance? This question warrants further scrutiny.

Developing strategies to meet acknowledged workforce challenges is a priority of ITI's members, and has been identified as an Administration priority as well. For example, the Cyber Security National Action Plan (CNAP) proposed under the Obama Administration took important steps to reverse the cyber talent shortage with the inclusion of a $62 million increase to the President's Budget to bolster cybersecurity personnel programs. One specific additional step ITI proposes is to establish a CyberCorps Reserve program, providing cyber education scholarships to Americans seeking to serve their country in the federal civilian government. Other steps include the development of a Cybersecurity Core Curriculum, an increase in the number of participating academic institutions in the NSA Centers for Academic Excellence in Information Assurance Education program, and an expansion of student loan forgiveness programs for cyber professionals joining the federal workforce.

These education and workforce investments will make a vital down payment to help close the cybersecurity skills gaps in government and the private sector. With more than 209,000 cybersecurity jobs in the U.S. unfilled last year, and predictions of 1.5 million more cyber jobs than takers by 2019, ITI is committed to supporting the CNAP's cyber workforce efforts and expanding initiatives like the CyberCorps Reserve program. The CNAP is a great step forward, but to remedy our alarming cyber talent deficit, we must recruit more than a million Americans trained in cybersecurity and information assurance. Only the federal government can lead response recruiting effort on the scale required. By offering young STEM graduates immediate employment protecting government and other critical assets, the government could stand up a Cyber National Guard that would quickly produce a trained workforce with practical experience and security clearances. After serving their country for five years in the public sector, Cyber National Guard veterans would find private companies such as those in ITI eager to hire them – and pay them what they are worth.

If the Agencies truly want to take steps to help improve the cybersecurity risk management of financial institutions, initiatives geared toward workforce development for the financial sector are foundational and a great place to start.

Cyber Risk Governance. Another dimension of the workforce challenge implicates the proposed application of the Enhanced Standards to third-parties. As mentioned above, financial institutions and other entities often seek to avail themselves of managed/shared cybersecurity services to bridge the cybersecurity workforce shortfall. Leveraging such solutions should be encouraged – not disincentivized. Yet, as mentioned above, application of an onerous regulatory compliance scheme to such entities will make it less likely that large financial institutions will be able to avail themselves of such services.

Another example of the Enhanced Standards perhaps trying to do too much are the requirements for Board-level approvals of dynamic yet detailed cybersecurity plans, which again seem potentially onerous. While it is doubtless a good idea to have board-level awareness of and involvement in managing entities' cybersecurity risk, it likely does not make a lot of sense to require board-level micromanagement of cybersecurity risk management plans and activities that the Agencies acknowledge must be dynamic and constantly evolving. Moreover, as the NYS Department of Financial Services has also proposed cybersecurity regulations that call for increased involvement by boards of directors, the ANPR may again prove somewhat redundant in this regard.

Further, requiring comprehensive audits may involve a level of invasiveness that is both onerous and inefficient – likely requiring a level of access, for instance, that could jeopardize proprietary systems and information.

Internal and External Dependency Management. With respect to internal management as described in the ANPR – what is striking is how much of the section is already comprehensively addressed in multiple sets of existing guidance. For instance, asset management is addressed at length in the Framework, FFIEC Cybersecurity Assessment Tool, and CPMI-IOSCO Guidance. As stated at the outset of this comment, the Agencies fail to offer any evidence that asset management is not being adequately addressed under current authorities and guidance. Much of the internal dependency management proposals are thus redundant.

External dependency management implicates the global supply chains of the third-parties to which the Agencies contemplate extending the Enhanced Standards. As stated above, the Agencies correctly highlight the interconnectedness of large financial institutions in the ANPR. Yet the Agencies contemplate extending the proposed Enhanced Standards even to *non-critical* external parties. This overreach ignores the importance of prioritization in risk management – if everything is critical, then nothing is critical. Further, the companies primarily targeted by the ANPR are already managing their external dependencies as part of a sound risk management program. Most large financial institutions already have an enterprise risk management program that includes vendor risk management.

Board-level micromanagement of such plans again seems an onerous obligation, and one ill-suited to the expertise of a typical board of directors, of any size entity.The Agencies acknowledge the rapidly changing and complex threat landscape in the ANPR, and state that the contemplated solution should be continuous evaluation of controls, including external dependencies. While this makes sense, it does not to the extent the ANPR would seem to require near continuous Board-level review of external dependencies.

Incident Response, Cyber Resilience and Situational Awareness. Incident response is addressed at length in existing financial sector regulatory frameworks. So again, the detailed sections on this topic in the ANPR appear redundant.

One of the Agencies' primary concerns is articulated as "preventing cyber contagion" across an interconnected financial ecosystem. Static requirements seem ill-suited to preventing cyber contagion in a threat environment acknowledged to be interconnected, rapidly changing and complex.

The ANPR contemplates an obligation on financial sector entities to implement strategies to manage risks in anticipation of interconnected CI – for instance, energy and telecommunications. Is it practical to expect Covered Entities to create cybersecurity programs that fully account for dynamic, sector-wide external dependencies?

The ANPR also contemplates "testing requirements," without a clear explanation of what, exactly, the Agencies propose to test, though there is some discussion of testing for "any" potential cyber event that could affect the ability of regulated entities to service clients in the ANPR. Much additional explanation is needed with regards to contemplated testing of any and all cyber events.

Finally, the Enhanced Standards contain requirements to "pre-empt" cyber events. Adopting a prevention mindset will be beneficial to covered entities, and complements any detection and remediation capabilities they have. Thus, policies that encourage prevention are important. The Agencies must understand, however, that there are limitations to pre-empting, or preventing, 100% of all cybersecurity attacks from being successful—some will always succeed—so any requirements in this regard must be realistic.

Section VIII. Considerations for Implementation of the Enhanced Standards

The Agencies do not try to hide the fact that they are considering a prescriptive approach in the ANPR, including contemplating "regulations that impose specific cyber risk management standards" (ANPR 44). "[T]he regulation would include details on the specific objectives and practices a firm would be required to achieve in each area of concern in order to demonstrate that its cyber risk management program can adapt to changes in a firm's operations and to the evolving cyber environment." (ANPR 45). These proposed requirements contradict existing cybersecurity public policy - such as that embedded in the Framework and much of the other guidance cited in the ANPR - that risk management is a continuous process demanding flexibility to provide reasonable protections in light of the nature and scope of the activities of a given company, including the sensitivity of the data it handles, its threat profile, and the size and complexity of the relevant data operations of the company.

In our view, establishing standards through policy statements and/or guidance is far superior to establishing a rigid regulatory regime, as already illustrated by much of the foregoing. This is particularly the case where the contemplated standards are prescriptive, inflexible, and misaligned with both industry approaches and federal cybersecurity policies.

From ITI's perspective, any effort to mandate minimum security standards is problematic, in that it is difficult for a minimum standards approach to allow for the flexibility for best security practices to evolve as technology advances, or to fully take into account the necessary risk management processes at the heart of cybersecurity. ITI thus routinely cautions all governments not to set compulsory security standards for the commercial market – whether they are standards vendors must follow as they build their products or services, or standards that would guide consumers when purchasing ICT products and services or conducting business with companies. Such an approach could encourage some firms to invest only in meeting static standards or best practices that are outmoded before they can even be published or cause organizations to divert scarce resources away from areas requiring greater investment towards areas with lower priority. To maintain (rather than restrain) innovation and to

prevent the development of single points of failure, any standards should be purely indicative, their use entirely voluntary, and they should allow organizations to adopt alternative solutions. Defining new, financial sector specific standards has many downsides as they may conflict with global standards currently in use, interfering with global interoperability.

The more resources institutions are required to spend on compliance activities, the less resources they will have available to identify threats to critical assets, and to protect, detect, respond and recover from cybersecurity threats. As stated above, we recommend efforts to reduce redundancy across existing regulations, rather than the creation of new regulations.

In our view, orienting financial sector risk management efforts around the Cybersecurity Framework represents a superior approach to that espoused in the ANPR. ITI has previously commended NIST's continuing work, in cooperation with the private sector and other stakeholders, to further the development of the Framework. The Framework leverages public-private partnerships, is grounded in sound risk management principles, and helps foster innovation due to its flexibility and basis in global standards. We believe the Framework has already helped and will continue to help improve cybersecurity, and that the Framework has had and continues to have an important, valuable impact on organizations' understanding of cyber risks. The Framework has allowed organizations to have useful conversations about cybersecurity risk management both internally (e.g. with our senior management) and externally (e.g. with boards of directors, partners, suppliers, and customers), allowing these parties to better understand the importance of managing cyber risks. The Framework's common terminology (identify, prevent, detect, respond, recover) provides a flexible, common, standardized language to enable these discussions.

However, it's clear that the common language of the Framework can also be promoted and better used to provide a common language or taxonomy for policymakers globally and domestically, at all levels of government. Amongst other benefits, doing so can help prevent duplication of regulatory efforts. The FFIEC used the Framework in precisely this way, in devising its Tool.

As NIST pointed out in the Framework document, "Executive Order [13636] called for the development of a voluntary, risk-based Framework – a set of industry standards and best practices to manage cybersecurity risks." That is exactly what NIST produced, with significant input from industry, in the Framework, and we do not suggest that NIST or other stakeholders lose sight of the inherent "voluntariness" of the Framework, or stop promoting it as such. However, this is not to say that we should ignore the reality that government policymakers and regulators, including the Agencies as acknowledged in the ANPR, are increasingly looking to the Framework for inspiration as they consider whether and how to exercise their regulatory authorities to help improve cybersecurity.

We believe more can and should be done to reinforce the Framework as voluntary, while at the same time embracing its sensible use by regulators such as the Agencies to streamline and on a net basis reduce cybersecurity regulations. How can we accomplish this? The key is that the Framework should not serve as the impetus or rationale for extra layers of regulation, as apparently was the case in the ANPR. That's not regulatory streamlining, it's regulatory redundancy, and multiple layers of redundant regulations will not create better cybersecurity for anyone, including regulated entities themselves. Rather, the Framework can still be held up as a voluntary risk-management based tool, while also

serving as a beacon around which policymakers at every level – including the Agencies – should orient their efforts to improve cybersecurity. Doing so in turn will help reduce regulatory redundancy, thus making it easier for financial services institutions to manage cybersecurity risk.

CONCLUSION

ITI would like to again thank Agencies for demonstrating a commitment to utilizing transparent processes and partnering with the private sector to advance our shared cybersecurity goals.

While we won't recap all our recommendations here, we will reiterate the importance of furthering risk-management and flexible approaches grounded in international standards that leverage public-private partnerships – all of which are hallmarks of the Cybersecurity Framework. We urge the Agencies to embrace the Framework, around which they can orient their ongoing worthwhile efforts to improve cybersecurity across the financial system.

ITI and our member companies look forward to continuing to work with the Agencies and other USG stakeholders on this and other initiatives to improve our cybersecurity posture. Please continue to consider ITI as a resource on cybersecurity issues moving forward, and do not hesitate to contact us with any questions regarding this submission.

Sincerely,

John Miller
Vice President for Global Policy and Law
Cybersecurity and Privacy