Testimony of

Christopher F. Feeney

On behalf of

BITS – Bank Policy Institute

Before the

House Subcommittee on Intergovernmental Affairs

for the

Committee on Oversight and Government Reform

Hearing entitled:

"Regulatory Divergence: Failure of the Administrative State"

July 18, 2018

Chairman Palmer, Ranking Member Raskin, and members of the Subcommittee, thank you for the opportunity to testify before you today.

My name is Christopher F. Feeney, and I am the President of BITS – Business-Innovation-Technology-Security.[1] BITS is the technology policy division of the Bank Policy Institute (BPI). BITS provides an executive level forum to discuss and promote current and emerging technology, foster innovation, reduce fraud and improve cybersecurity and risk management practices for the nation's financial sector.

Led by C-Suite executives, including Chief Executive Officers (CEOs), Chief Information Officers (CIOs), Chief Information Security Officers (CISOs) and other senior leaders, BITS brings together its members, regulators, government agencies and technology firms to advance collaboration in the regulatory and risk environment; address current and emerging policy issues; improve effectiveness of technology programs; promote critical infrastructure resilience; and strengthen cybersecurity and reduce fraud.

With a focus on business, innovation, technology and security, BITS is a leading voice in Washington for information sharing and development of best practices and policies that protect our nation's financial services platforms and the customers they support.

In addition to my role as BITS President, I am also a member of the Financial Services Sector Coordinating Council's (FSSCC) Executive Committee and Co-chair of the Policy Committee. The mission of the FSSCC is to strengthen the resiliency of the financial services sector against attacks and other threats to the nation's critical infrastructure by proactively identifying threats and promoting protection, driving preparedness, collaborating with the U.S. Federal government, and coordinating crisis response for the benefit of the Financial Services sector, consumers and the nation.[2] I also hold leadership positions in several other industry organizations, such as Sheltered Harbor and fTLD Registry Services, LLC, all of which are focused on addressing the security and resiliency of financial institutions.

In these roles, my charge is to advance policies to protect the nation's financial infrastructure, firms' infrastructure and, most importantly, to protect the customers that use and depend on these financial systems every day. On behalf of our member firms, I offer the following testimony regarding the growing challenges financial firms face, putting a particular emphasis on a multi-year process the financial sector undertook to make progress relative to harmonizing cybersecurity regulation in the U.S. and globally. The key areas to cover are:

1) The expanding number of cybersecurity issuances financial firms are being asked to adhere to and the solution industry is proposing for usage by the regulatory community;

[1] For more information, please visit: https://www.bpi.com and https://bpi.com/category/bits/.
[2] For more information, please visit: https://www.fsscc.org/

2) The fast-changing environment to address the issue of privacy as evidenced by recent state and international privacy laws; and

3) The ongoing need for a uniform federal standard for data protection and breach notification.

A. Introduction

Financial firms prioritize preserving customer trust, and make significant investments to protect and secure customers' personal and financial information. As an industry, financial services is one of the most advanced when it comes to cybersecurity protections and regulators regularly oversee and challenge the systems and processes firms have in place to protect information and privacy. The industry is subject to multiple laws – for example, the Gramm-Leach-Bliley Act and the Fair Credit Reporting Act – that include strong cybersecurity requirements, consumer protections and govern the industry's use of data.

On an individual basis, many of the regulatory requirements financial firms must meet are beneficial and have strengthened firms and the industry. The challenge is that collectively, without harmonization and alignment, the regulations are often counterproductive; creating duplication, conflict and confusion, and place a significant burden on firms' ability to improve cybersecurity and innovate to stay ahead of threats.

Cybersecurity regulation is a ready example. Several years ago, as regulators (see Figure 1) began issuing multiple new cybersecurity tools, guidance and requirements, firms became deeply concerned that they were having to divert cybersecurity resources away from the front lines of cyber protection to instead focus on regulatory compliance – an outcome that put firms at risk and most certainly did not meet regulators' intentions of helping protect the industry against threats.

Over the course of the last three years, BITS has worked to address this problem and has coordinated extensively with firms, industry associations, our industry's sector coordinating council, the U.S. Department of the Treasury, our regulators and other federal agencies to develop a path forward that meets regulators' expectations while giving firms the ability to increase focus on improving front line cyber defenses rather than regulatory compliance. The solution we have developed – referred to as the Sector Profile – is described below. We are currently working to have the Sector Profile, which is based on the commonly used and cross sectoral National Institute of Standards and Technology's (NIST) Cybersecurity Framework, adopted across multiple jurisdictions and internationally.

Another example – and the most recent – is in the data privacy arena. While existing law and regulation for financial firms includes privacy and data security measures, the European Union's General Data Protection Regulation (GDPR) as well as the California Consumer Privacy Act (CCPA) create new obligations for firms that will require changes to

technology, policies and procedures. While both laws may create an entirely new set of requirements to enable consumers to control how their data is used across all industries, they also set up a number of duplicative requirements and potential conflicts with existing regulations for financial firms.

For instance, financial firms must fulfill what are referred to as Know-Your-Customer (KYC) requirements to detect and prevent money laundering. To fulfill these obligations, firms must collect and retain certain personal and financial information on customers for a defined period of time (e.g., in the securities area FINRA Rule 17a-4 requires customer record retention for 7 years). Under GDPR and CCPA, a consumer can request that their information be deleted, setting up a potential conflict for firms who must now meet competing and mutually exclusive requests.

A growing concern for financial firms is that GDPR and CCPA may be the start of a new wave of similar but different privacy laws being considered across the country by states as well as cities and warrants consideration of a national standard. If the history of state data breach laws is any indicator, firms may soon face 50 different standards they must comply with and, in some cases, de-conflict with multiple government authorities.

Lastly, the financial industry has been a strong proponent of a single, national data protection and breach notification standard to help firms and consumers protect themselves and recover in the event of a breach. We have testified in support of such legislation, most recently before the House Financial Services Subcommittee on Financial Institutions and Consumer Credit on its "discussion draft" entitled, "Data Acquisition and Technology Accountability and Security Act," calling for a uniform, federal consumer data protection and breach notification law.

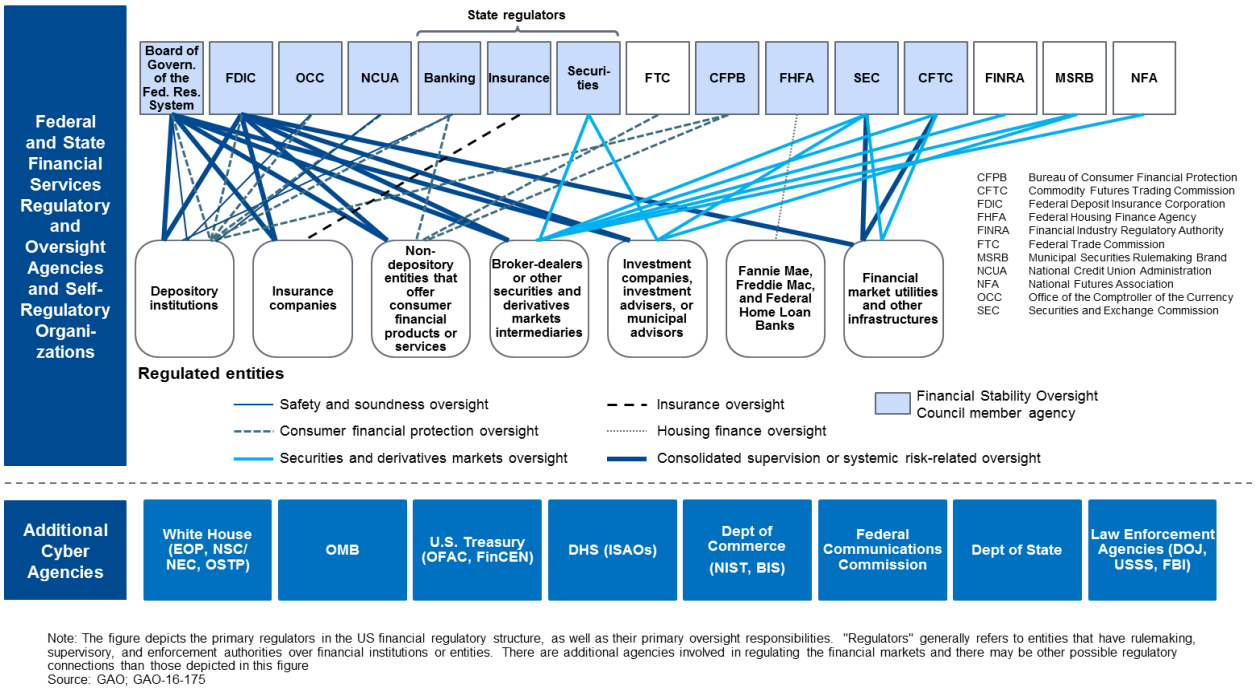
This Committee's support for the regulatory harmonization effort would be welcomed and we encourage you to help ensure competing frameworks and requirements for other aspects of data security, breach notification and privacy can be better aligned under a national standard.

B. Overview and Challenges Inherent in the Financial Services Sector Regulatory Structure

The financial services sector consists of more than 13,000 banks and credit unions, payment companies, insurance companies, wealth and asset managers and financial market utilities that process transactions, payments and move money across domestic and international markets.

The sector is overseen by nine federal regulators (all of which are independent from the executive branch), three self-regulatory organizations, the U.S. Department of the

Treasury (Treasury) as its sector-specific agency,[3] and every state banking, insurance, and securities agency. When agencies tasked with cybersecurity-related authorities are added, the list expands even further (see Figure 1).



Note: The figure depicts the primary regulators in the US financial regulatory structure, as well as their primary oversight responsibilities. "Regulators" generally refers to entities that have rulemaking, supervisory, and enforcement authorities over financial institutions or entities. There are additional agencies involved in regulating the financial markets and there may be other possible regulatory connections than those depicted in this figure
Source: GAO; GAO-16-175

(Figure 1. The current financial services regulatory structure as it relates to cybersecurity)[4]

C. The Financial Services Sector's Commitment to Cybersecurity Advancement

Cybersecurity is a top priority for our member firms. It is a key concern and focus area for CEOs and Boards of Directors, all the way to the frontline defenders sitting at keyboards monitoring network activity and responding to security events. Firms' senior management have made clear that cybersecurity risk is not solely a technology issue, but a business line and enterprise-wide risk that should be considered across all levels of the organization. As such, cybersecurity is a regular agenda item at Board of Directors meetings, often with the Chief

[3] For more information, please visit: https://www.dhs.gov/financial-services-sector

[4] Figure is derived from a nearly identical graphic developed and used by the United States Government Accountability Office in its February 2016 report, entitled, "Financial Regulation: Complex and Fragmented Structure Could be Streamlined to Improve Effectiveness," which was then amended to include the agencies below the dotted line. See: https://www.gao.gov/assets/680/675400.pdf. Those agencies were added because their cybersecurity issuances also can have a direct impact on financial institutions' cybersecurity programs and compliance response.

This exact graphic, however, has been reproduced from the FSSCC and BCG Platinion May 17, 2017 presentation at the NIST Cybersecurity Workshop event:
https://www.nist.gov/sites/default/files/documents/2017/05/18/financial_services_csf.pdf

Information Security Officer or equivalent providing updates on threats to the financial industry and individual firms, specific risks plus risk trends, and strategies for mitigation. With this senior-level support, firms have sharpened priorities and their commitment to cybersecurity.

According to the Cyber Security Market Report "U.S. Financial Services: U.S. Financial Services: Cybersecurity Systems & Services Market – 2016-2020" report, the U.S. financial sector's cybersecurity market is the largest and fastest growing private sector cyber security market. Its cumulative 2016-2020 market size is forecasted to exceed $68 Billion.[5]

Recognizing that cybersecurity affects the entire industry, financial firms also have a long history of significant investment and collaboration to improve cybersecurity preparedness, response and resiliency across the sector. For example, prior to the passage of the Homeland Security Act of 2002 and the Cybersecurity Act of 2015, the financial services sector established the cyber threat information sharing and analysis center known as the FS-ISAC – a gold standard for critical infrastructure cyber threat information sharing organizations.

In addition, BITS has facilitated ten semi-annual CEO-led "Joint Financial Associations Cybersecurity Summits." These summits bring together financial institution CEOs, trade association CEOs, and key Congressional and government leaders to actively address sector resiliency, respond to capability gaps, and encourage coordination and investment. Other sector-wide activities include the initiation of a joint financial services, telecommunications, and electric sector working group to address cyber risks posed to all three sectors; the "Hamilton Series" of cybersecurity response exercises; the establishment of a not-for-profit organization – Sheltered Harbor – an initiative launched by the financial services industry to establish standards for secure data vaulting and rapid recovery of customer balances and assets in the event of a catastrophic cyber incident; fTLD Registry Services, secure website domains for banking and insurance companies; and updates and testing of the sector's cyber response plans, including the "All-Hazards Crisis Response Playbook," which provides guidance on intra-sector and government coordination in the event of a cyber incident.

Much of this collaborative work includes regulators, and our government partners at the Treasury and Department of Homeland Security (DHS). Under the DHS National Infrastructure Protection Plan, Treasury is our sector-specific agency and helps organize regular meetings of the FSSCC along with our government counterparts, referred to as the Financial and Banking Information Infrastructure Committee (FBIIC). These meetings help our industry, our regulators and our government partners work collaboratively to improve resiliency and the policies that enable it.

[5] https://homelandsecurityresearch.com/reports/u-s-financial-services-cyber-security-market/

D. The Issue of Cybersecurity Regulatory Overlap

Industry and our regulators share the same goal: To ensure the financial services sector is safe, sound, strong and secure. We support our regulators' attention to the critical issue of cybersecurity and understand that on a daily basis the nation's businesses and citizens rely on our ability to facilitate the financial transactions of their daily lives. We also understand and embrace the fact that we are the guardians of our customer's data, including sensitive personal and financial information. Accordingly, like the regulatory community that oversees us, we support the advancement of cybersecurity and data protection and understand the need for their regulatory oversight.

With a fragmented regulatory landscape, however, we are now experiencing a proliferation of layered requirements that often are topically similar, but semantically different. Some of these cybersecurity proposals incorporate the NIST Cybersecurity Framework's organizational structure and terminology (a congressionally approved framework supported by both the Obama and Trump Administrations). But many do not, instead opting for novel approaches and different language. For those financial institutions operating internationally, or even servicing international customers within the United States, the number of applicable regulatory schemes only expands.

United States Financial Services Cybersecurity Regulations, Guidance and Supervisory Practices: In 2017, the Financial Stability Board[6] published its "Stocktake of Publicly Released Cybersecurity Regulations, Guidance and Supervisory Practices"[7]. U.S. member agencies self-reported 10 different federal "schemes" of regulation that "address cybersecurity" for the financial services sector and cited 43 different publicly available cybersecurity issuances. The 10 schemes and 43 issuances did not include agency/examiner questionnaires, first-day letters, and other non-public supervisory expectations that financial institutions are also subject to during their examination process, nor does it include the cyber regulatory expectations issued or proposed by each of the fifty states.[8]

---

[6] The Financial Stability Board (FSB) is an international body that monitors and makes recommendations about the global financial system. The FSB, working through its members, seeks to strengthen financial systems and increase the stability of international financial markets. The policies developed in the pursuit of this agenda are implemented by jurisdictions and national authorities.

Members include representatives from financial services regulatory oversight bodies from the following 25 jurisdictions: Argentina, Australia, Brazil, Canada, China, France, Germany, Hong Kong, India, Indonesia, Italy, Japan, Korea, Mexico, Netherlands, Russia, Saudi Arabia, Singapore, South Africa, Spain, Switzerland, Turkey, United Kingdom, United States and the European Union.

For more information, please visit: www.fsb.org.

[7] See: http://www.fsb.org/wp-content/uploads/P131017-2.pdf

[8] In my written testimony before the Senate Homeland Security and Governmental Affairs Committee last year, I supplied charts of the over 30+ issuances that we had been tracking since the release of the NIST Cybersecurity Framework in 2014 that directly impacted firms in the financial services sector. Those charts can be found in

Select International Cybersecurity Regulations, Guidance and Supervisory Practices: The international financial services regulatory community has also been prolific. Indeed, each of the 25 member jurisdictions to the FSB reported that "they have publicly released regulations or guidance that address cybersecurity for at least part of the financial sector, and a majority have also publicly released supervisory practices."

Like the United States, the European Union (EU) self-reported 10 schemes of regulation that pertain to the financial services sector. Additionally, the EU cited to 26 applicable and publicly available cybersecurity issuances. Each overlapping FSB and EU member nation reported that they also had their own nation specific regulatory schemes.

In the Asia-Pacific region, Japan reported 4 publicly available supervisory documents, China 11, and Australia 11 as well.

Future Cybersecurity Regulatory Issuances: According to the Stocktake, 72% of the member jurisdictions self-reported that they also intend to issue more cybersecurity expectations in the near future. Items listed, included: new regulations, "guidance and strategy for the financial sector; a self-assessment exercise to gauge the cyber resilience of FMIs; guidance on conducting threat intelligence based testing of cyber resilience; developing a set of standards for industry on Information Technology Risk (including cyber) and updating existing guidance in this area; and establishment of a computer emergency response team (together with computer security incident response team referred to hereinafter as CERT) for the financial sector."

E. The Impact of Cybersecurity Regulatory Overlap

The current fragmented approach to cybersecurity regulation causes firms to expend substantial personnel and resources reconciling notionally similar, but semantically different cybersecurity proposals and agency expectations. More specifically, it introduces inefficiencies by requiring institutions to identify, draft, and compile functionally equivalent sets of data from and for the same systems to satisfy each different regulator and each different regulatory standard. As a result, institutions are forced to create single-use compliance data, rather than focusing their time on developing security and mitigation techniques that improve a firm's cybersecurity program and protects customers.

When the sector surveyed its information security teams approximately two years ago, one firm estimated that 40% of its cyber team's time was spent on compliance related

---

Appendix A and can be accessed here: https://www.hsgac.senate.gov/imo/media/doc/Testimony-Feeney-2017-06-21.pdf.

Since that time, we have not resumed the tracking because of the volume of proposals at the State and International level.

matters, not on cybersecurity. That multinational's experience was not unique. Due to one framework issuance, in particular, the reconciliation process delayed another firm's implementation of a security event monitoring tool intended to better detect and respond to cyber-attacks by 3-6 months.

While each agency proposal or set of requirements may have its own merit, when continuously layered, the added complexity is unsustainable as there are simply not enough cybersecurity professionals available to perform the necessary work. According to the 2017 jointly issued Cybersecurity Ventures – Herjavec Group report, there were an estimated 350,000 unfilled cybersecurity jobs in the United States for 2017. This trend is only expected to continue, with the global shortfall reaching 2 million by next year, and by as much as 3.5 million by 2021.

The lack of harmonization also complicates efforts to coordinate across critical infrastructure sectors and with the federal government for cyber incident response. A key focus for the federal government and DHS, in particular, has been to foster a "whole of nation" approach to cybersecurity. This effort to foster greater public-private partnership is critical if we are to effectively protect our economy, our customers, and our citizens from cyber threats. As regulations pull financial institutions away from using the more recognized and widely deployed NIST-based approaches, this could endanger not only our sector, but other critical infrastructure sectors if a coordinated response is needed.

F. A Proposed Cybersecurity Solution and the Regulatory Community's Response to Date

There is a solution, however: the Sector Profile, a meta-framework for financial services based on the organizational structures of the National Institute of Standards and Technology "Framework for Improving Critical Infrastructure Cybersecurity" (NIST Framework)

The industry first suggested regulators align their efforts more closely to the NIST Cybersecurity Framework in a September 21, 2015 submission[9] to the Federal Financial Institutions Examination Council, a coordinative body for the banking-specific agencies and organizations[10]. This suggestion included a request that regulators work collaboratively with

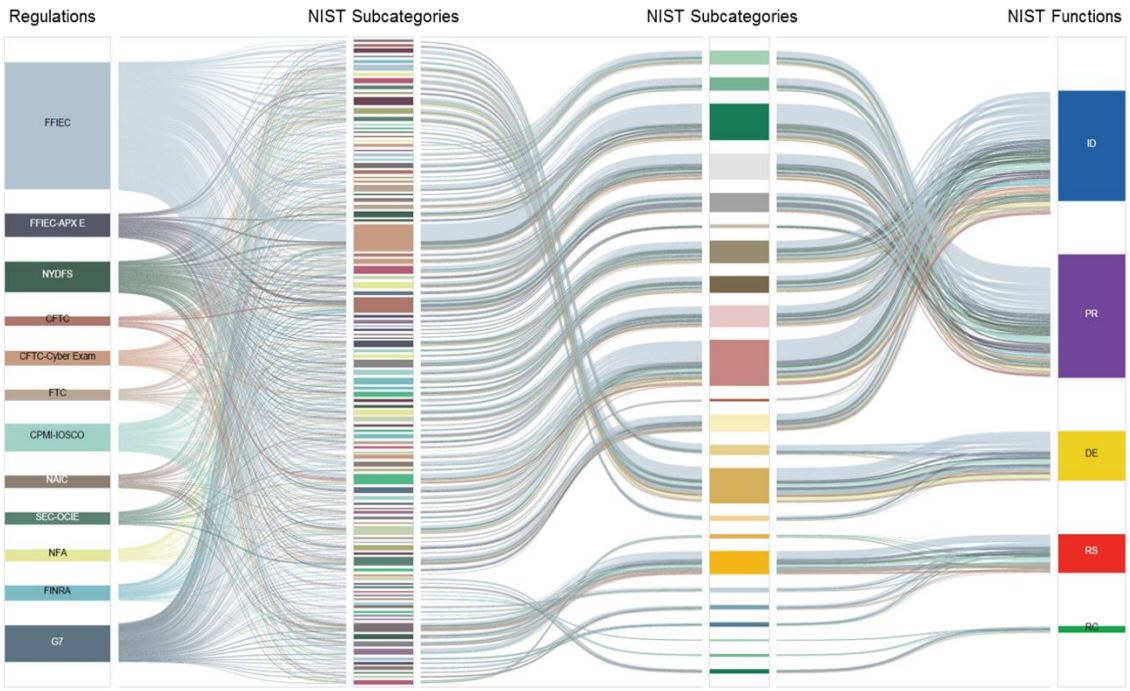
[9] See: https://www.fsscc.org/files/galleries/FSSCC_FFIEC_Cybersecurity_Assessment_Comment_Letter_(FR_2015-17907).pdf

[10] For more information on the FFIEC, including its membership and statutory authorities, please see: https://www.ffiec.gov/. Chaired by the U.S. Department of Treasury's Assistant Secretary for Financial Institutions, members include representatives from the 2) American Council of State Savings Supervisors, 3) Commodity Futures Trading Commission, 4) Conference of State Bank Supervisors, 5) Consumer Financial Protection Bureau, 6) Farm Credit Administration, 7) Federal Deposit Insurance Corporation, 8) Federal Housing Finance Agency, 9) Federal Reserve Bank of Chicago, 10) Federal Reserve Bank of New York, 11) Federal Reserve Board, 12) National Association of Insurance Commissioners, 13) National Association of State Credit Union Supervisors, 14) National Credit Union Administration, 15) North American Securities Administrators Association,

industry to find a solution that would allow regulators to fulfill their responsibilities while better allowing firms to focus on critical cybersecurity activities.

In October 2016, industry (through the FSSCC) and our government coordinating council, the FBIIC, agreed to a joint working group to discuss opportunities to better harmonize cybersecurity related requirements and expectations. When it became clear that the FBIIC would be unable to meet on an ongoing basis, the sector moved ahead on its own with regular individualized outreach to the various regulatory agencies, all of which expressed some level of support for the industry initiative.

To start, the sector began mapping multiple cybersecurity related issuances and proposals against both the NIST Framework and importantly standards from the International Standards Organization (ISO). With the initial mappings complete, a clear pattern emerged: Over 80% of the mappings were topically identical, but semantically different. (See Figure 2. below).



(Figure 2. Regulatory Overlap and Complexity in Reconciling Select Proposals to the NIST CSF).

To reduce the time cybersecurity personnel allotted to reconciling semantic differences, the industry then chose to fund an effort to use these mappings to develop the Sector Profile. Based on the mappings and the widely accepted use of the NIST Framework, the Sector Profile was architected around the NIST Framework's five functions, categories, and

16) Office of the Comptroller of the Currency, 17) Securities and Exchange Commission, and 18) Securities Investor Protection Corporation.

subcategories, and extended to include two new functions – Governance and Supply/Dependency Management – which emerged as distinct areas of (appropriate) regulatory focus. The architecture also extended the NIST-based structure so that it could function as a compliance assessment tool. Borrowing from the Federal Financial Institutions Examination Council Cybersecurity Assessment Tool's "Declarative Statements," the Profile added a series of Diagnostic Statements, which synthesize overlapping expectations from multiple regulatory organizations into a more singular, standardized set of assessment-ready diagnostics.

Because of its NIST basis, NIST asked the sector to preview that work at it NIST Cybersecurity Framework Workshop in May 2017. In the months that followed, the sector met individually with each of its federal regulatory agencies, the various self-regulatory organizations, and associations for state-based regulators. The feedback collectively was that it was a productive body of work and that we should continue to refine it, adding risk tiers so that it would be usable and applicable to the most sophisticated firms and the least sophisticated firms. In April 2018, NIST sponsored a one-day, open-to-the-public event at the Department of Commerce specific to the latest round of tailoring work. Again, the Sector Profile was seemingly well-received by all in attendance, including representatives from the various regulatory agencies.

G. Benefits to Regulators, Financial Firms and the Financial Infrastructure

As of today, the tailoring work continues, and is near complete. The sector anticipates releasing a fully developed Sector Profile "Version 1.0" around September. While the agencies have voiced support for its development, we will also be seeking acceptance for its usage. If used by the regulators, the benefits to the regulators, the financial services sector, and those citizens and customers that depend on the financial system would be manifold.

With its usage, the regulatory community will be able to:

- Tailor examinations to institutional complexity and conduct "deeper dives" in those areas of greater importance to that particular regulatory agency;
- Better discern the sector's systemic risk, affording more agency time for specialization, testing and validation;
- Create the ability to take collective action to better address identified risks;
- Compare and better analyze data from other agencies and other jurisdictions;
- Enhance regulators visibility into non-sector and third party risks.

For financial institutions, the benefits are likewise numerous:

- Optimization of cybersecurity professionals' time "at the keyboard" and defending against current and next generation attacks (e.g., calibrating risk identification, automating controls, cyber range testing, instrumenting monitoring systems,);

- Improved Boardroom and Executive engagement, understanding and prioritization;
- Enhanced internal and external oversight and due diligence;
- Greater innovation as technology companies, FinTech firms, startups, etc., are able to meet requirements expectations more efficiently;
- More efficient third-party vendor management review and oversight; and
- Greater intra-sector, cross-sector and international cybersecurity collaboration and understanding.

H. Conclusion and Congressional Request

Congress has an important role to play in –

(1) publicly supporting cyber regulatory harmonization and cyber regulation consistency by encouraging regulators to use and adopt the Sector Profile;
(2) in offsetting the potential proliferation of state and local privacy laws and enhancing consumers' rights to privacy before a patchwork of inconsistent and potentially incongruous privacy requirements are developed; and
(3) in legislating uniform standards for data breach reporting by developing clear, concise and effective notification standards.

With respect to cybersecurity, the financial services sector shares the same goals with the regulatory community: advancing the safety, soundness, and resilience of the financial system by protecting financial institutions and the financial sector from increasing cybersecurity risks. Given the complexity of our regulatory environment, a lack of harmonization negatively impacts the ability of financial institutions to devote resources to security activities, and this is exacerbated by the shortage of cybersecurity professionals. We hope all would agree that those professionals that are available should be able to devote more time to security rather than interpreting notionally similar, but semantically different regulatory expectations.

As discussed, the Sector Profile, if supported, will provide a mechanism for alignment to current regulatory expectations, requirements, and authorities. Additionally, and perhaps more importantly, the Profile provides a clear path forward to streamline existing and future cybersecurity regulatory expectations around a common structure and vocabulary. Accordingly, we request that Congress continue to encourage regulators in their harmonization efforts and suggest public support and future alignment with the Sector Profile.

The same holds true for providing consumers and businesses with a clear expectation for how their data and privacy will be protected and what level of information, transparency and timing for notification they should expect if ever their information is improperly accessed and would result in risk of harm. Multiple standards with slightly different timeframes, definitions or other specific requirements will not benefit consumers and requires firms to sift through a myriad of different notification requirements when they would be better served

helping their businesses better protect information and privacy and attending to customers should a breach occur.

Lastly, the implementation of GDPR and the passing of the California Privacy Legislation both have the same objective to protect the privacy of individuals while offering choices for how individuals want to manage their personal information. The financial industry supports privacy advances and has been a strong advocate for protecting customer information for decades. We can forecast, however, that a proliferation of multiple privacy standards with multiple, and in certain cases conflicting criteria relative to existing laws, can lead to a negative outcome. As noted above, current law has provisions for handling sensitive customer information while also requiring retention of client information for seven years. These provisions are inconsistent with requirements in some of the new privacy issuances and puts a firm in the midst of a jurisdictional dilemma while a firms' interest is to ensure the protection of their customer. Working on a common federal standard for privacy protection that can complement existing requirements is a chance to get ahead of more disparate laws. We would ask Congress to develop a uniform privacy standard that the financial services industry and other industries who hold sensitive customer information could adopt and adhere to in a collective way.

In short, we stand ready to work with Congress on data breach and privacy standards and we will continue to work actively with our regulatory community on this more rationalized approach to cybersecurity regulation. As we do so, Congressional encouragement is welcome. Indeed, it is needed.

Committee on Oversight and Government Reform
Witness Disclosure Requirement — "Truth in Testimony"

Pursuant to House Rule XI, clause 2(g)(5) and Committee Rule 16(a), non-governmental witnesses are required to provide the Committee with the information requested below in advance of testifying before the Committee. You may attach additional sheets if you need more space.

Name:

1. Please list any entity you are representing in your testimony before the Committee and briefly describe your relationship with each entity.

Name of Entity	Your relationship with the entity
Bank Policy Institute - BITS	Executive Vice President, President of BITS

2. Please list any federal grants or contracts (including subgrants or subcontracts) you or the entity or entities listed above have received since January 1, 2015, that are related to the subject of the hearing.

Recipient of the grant or contact (you or entity above)	Grant or Contract Name	Agency	Program	Source	Amount

3. Please list any payments or contracts (including subcontracts) you or the entity or entities listed above have received since January 1, 2015 from a foreign government, that are related to the subject of the hearing.

Recipient of the grant or contact (you or entity above)	Grant or Contract Name	Agency	Program	Source	Amount

I certify that the information above and attached is true and correct to the best of my knowledge.

Signature _____ Date: 7/13/18

bpi Business Innovation Technology Security
BITS

Christopher F. Feeney
BITS President

Chris Feeney is the President of BITS, the technology policy division of the Bank Policy Institute (BPI), where he collaborates with the nation's largest financial institutions, the administration, regulators and policymakers to promote effective cybersecurity and operating practices and to develop and shape the industry's use of emerging technologies.

BITS is a thought leader for the industry on innovation, policy, cybersecurity technology and practices, fraud reduction and risk management, representing CEO's, CIO's, CISO's and operating executives from the nation's leading financial institutions.

Feeney has over 30 years of experience in executive management, technology, business/sales management and operating roles at software companies, banks, broker dealers and investment management firms. His background includes founding a strategic advisory firm; consulting on behalf of boards, CEOs and leadership teams; and serving as managing director and CIO at LPL Financial. Over his career he has developed a keen ability to lead transformations and establish firms for success. He has served as CEO, President, and in executive roles at Thomson Financial, Bank of America, Telerate, Multex and Broadridge Financial.

Chris is currently a Board and Operating Management member of fTLD Registry Services, a Board Member of Sheltered Harbor, a Board Advisor at Quovo, Inc. and an Executive Committee Member of the Financial Services Sector Coordinating Council (FSSCC) and Co-Chair of its Policy Committee. Mr. Feeney was recently a Board Director at Scottrade, Inc. and Scottrade Bank, prior to its sale to TD Ameritrade and TD Bank, where he was the Risk Committee Chair. Mr. Feeney is a National Association of Corporate Directors (NACD) Governance Fellow.

ABOUT BITS

BITS is the technology policy division of the Bank Policy Institute. BITS provides an executive level forum to discuss and promote current and emerging technology, foster innovation, reduce fraud and improve cybersecurity and risk management practices for the nation's financial sector.

Led by C-Suite executives including CEO's, CIO's, CISO's and senior leaders, BITS brings together its members, regulators, government agencies and technology firms to; advance collaboration in the regulatory and risk environment; address current and emerging policy issues; improve effectiveness of technology programs; promote critical infrastructure resilience; and strengthen cybersecurity and reduce fraud.

With a focus on business, innovation, technology and security BITS is a leading voice in Washington for information sharing and development of best practices and policies that protect our nation's financial services platforms and the customers they support.