FSSCC YELLOW: The contents of this document are sensitive, and intended only for the recipients and other FSSCC members and partners with a need-to-know.

September 9, 2014

FSSCC Members,

As you know, the FSSCC has been very active in the development of the NIST Cyber Security Framework. NIST is now requesting information via a public RFI from the critical sectors about our level of awareness and initial experiences with the Framework. The FSSCC Policy Committee is assisting in this process by suggesting FSSCC members focus only on those questions that are believed to be the most relevant and that have not been addressed in previous FSSCC contributions. However, firms are welcome to respond to all questions as appropriate within the attached RFI.

Concurrent with this transmission, the FS-ISAC has distributed a survey to its membership, targeted primarily at small/mid-sized institutions, that queries more fundamental aspects of companies' awareness of the Framework and their experience with it, delivered in yes/no and multiple choice format. We hope that these two surveys will provide a snapshot from which we can track and articulate in commonly understood terms the evolving effectiveness of our cyber resiliency programs and the role that the NIST Cybersecurity Framework is playing in that process.

Instructions: This survey is intended for both FSSCC operators (banks, utilities, insurance companies, etc.) and our sector trade associations. For best results please coordinate among all the appropriate SMEs in your organization and where possible submit a unified enterprise set of answers, recognizing that different organizations within your enterprise may have different answers if your risk management programs are decentralized. Trade associations may also assess their own cyber risk management programs against the Framework in addition to discussing their outreach and awareness initiatives.

Please submit answers BY COB FRIDAY SEPTEMBER 19 either in this Word document or in the text of the reply to the RFI email, to the FSSCC Business Operations Manager Clara Fritts: clara.fritts@fsscc.org. This will provide us enough time to compile the answers and draft an approved response for submission to NIST by its October 10 deadline.

9 questions total begin on page 2.

a. **Aetna**
b. **Freddie Mac**
c. **TCH**
d. **BNYMellon**
e. **Wells Fargo**
f. **LCHClearnet**
g. **Credit Union National Association (CUNA)**
h. **State Street**
i. **SIFMA**
j. **US Bank**
k. **FMR Corp.**
l. **Bank of America**
m. **CITI**
n. **FSR**

High Priority Questions from the RFI

1. Is your organization an operator or an association?
   b. **Operator**
   c. **Association**
   d. **Both**
   e. **Operator**
   f. **Operator**
   g. **Association**
   h. **Operator**
   i. **Association**
   j. **Operator**
   k. **Operator**
   l. **Operator**
   m. **Operator**
   n. **Association**

2. Has your organization conducted, or do you plan to conduct, a mapping exercise between your cybersecurity risk management program and the NIST Framework? This work effort was completed last year and it will be updated this year. How would you characterize the extent of alignment or integration between the two?
   a. **Excellent alignment with business drivers for the information security program. Overlap with the policies and control standards in place and our control standards are more comprehensive so we did not change them to align with the Framework controls.**
   b. **Yes and we are in the pilot phase of the implementation.**

c. **We will wait until version 2.0 releases before we perform the mapping.**
d. **Yes, the preliminary high level assessment has been performed and we are currently aligning areas of interest with ongoing mitigation programs such as ISO 27001.**
e. **Yes, closely aligned**
f. **We completed a high-level mapping between the NIST Framework, ISO, internal IS Policy and the 10 Steps to Cyber Security. The NIST Framework itself only provides control objectives - not specific controls but ISO provides us with a comprehensive set of controls which satisfy the control objectives comprising the Framework. At this time we have identified no obvious gaps in terms of this framework and controls in existence which was expected.**
g. **n/a**
h. **Earlier this year, we began the process of mapping our current information security controls based on the ISO 2700 and SANS Critical Security Controls to the NIST Cybersecurity Framework. We plan to complete a full transition to the NIST Cybersecurity Framework early with CY2015. Our analysis has concluded that although there is considerable alignment between our current methodology and the NIST Cybersecurity Framework, efforts remain to precisely map each existing security controls.**
i. **We do not have any plans to do that type of a cross walk within our IT organization. However, they, our senior management and board have been made aware of the NIST-CF and the suggested stance it requires for cybersecurity protections.**
j. **Yes, we have engaged in a "mapping exercise," and have found that there is substantial alignment relative to NIST SP 800-53 controls and other regulatory and guidance documents including PCI, GLBA, HITECH, CSA CCM, *inter alia.***
k. **Our organization uses ISO27001 as the foundation for its information security program. The alignment with the NIST Framework can be reconciled using the "Alternative View" provided by NIST as a supplement to the Cybersecurity Framework. In addition, we have done an independent mapping of individual information security controls to the framework.**
l. **Yes, we have conducted a mapping exercise. There is a high degree of alignment between the NIST Cybersecurity Framework and our existing cybersecurity risk management framework.**
m. **Yes. There is alignment.**
n. **See response to Questions 4, 5, and 6 below.**

3. Given that many organizations and most sectors operate globally or rely on the interconnectedness of the global digital infrastructure, what is the level of awareness internationally of the Framework?
    a. **Affiliates in Europe and the Far East are aware of the Framework but regulators and government officials are not aware of it**
    b. **Fully aware**

c. We are a domestic organization. Though, there is a fair amount of coverage internationally about the NIST framework.

d. In EMEA there is marginal awareness, wherein the European cyber initiatives are taking precedence. In APAC the MAS framework is being initiated but we believe that here and in LATAM, further awareness is needed.

e. Not very aware

f. We have been tracking the well publicized President Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," since February 2013. In enacting this policy, the NIST risk-based Cybersecurity Framework was developed but arguably this has been less publicized outside of the US. It is gaining more momentum now through consultancies, press and articles.

g. n/a

h. Our experience is that overall cognizance of the NIST Cybersecurity Framework exists – especially with the European regulatory organizations. However, detailed understanding of the framework is till limited.

i. We have made our foreign partner trades (AFME, ASIFMA and GFMA) aware of the NIST-CF and the benefits of using it in those regions. That being said SIFMA (the US entity) handles IT services for the other three so by default they are getting some benefits and awareness via that mechanism as well.

j. We are not prepared to comment about global awareness, but note that we, along with other FIs, are impacted by international regulation. Other countries (*e.g.,* New Zealand, EU) already have their own requirements.

k. While our organization operates globally, non-US-centric operations are managed by an independent "sister" organization. The answers here reflect the position of the domestic business. Given that, the level of awareness globally is minimal, except in those international locations which directly support US business operations.

l. There is an awareness of the Framework, but international entities continue to develop their own cybersecurity directives, guidances, and frameworks.

m. Very little in Latin America and Asia, but there is more awareness in Europe.

n. With greater frequency, we are hearing anecdotally from our membership that there is a general awareness that the NIST Cybersecurity Framework document exists. Earlier this year, a trade association representing another critical infrastructure sector invit\ed our trade association to represent the financial services sector on a trip to China. NIST was also one of the other invited organizations. During this trip, this delegation that consisted of U.S. based organizations spoke repeatedly about the NIST Cybersecurity Framework, the open and voluntary process by which it was created, and referred to this process and the document's stated goal of harmonization as constructs to follow. More recently, the Financial Times published an article quoting Greg Medcraft, the Chairman of both the Board of the International Organisation of Securities Commissions (Iosco) and Australian Securities & Investments Commission, as stating that international regulators are "looking at producing a global 'toolbox' next year…," and that the "[t]he starting point is to look at

what the Americans have done…and look at those risk-management principles and see how they could translate globally," a clear reference to NIST's Cybersecurity Framework.

4. Is your organization using the Framework to communicate information to key stakeholders - including boards, investors, auditors, and insurers - about your cybersecurity risk management?
    a. **Yes to the Board and Security Steering Committee**
    b. **Yes**
    c. **No, not yet as we are waiting for version 2.0**
    d. **Yes**
    e. **Yes**
    f. **NIST is not the main Framework we utilize at this time but increasingly likely that we will move to it in due course.**
    g. **Yes, we are communicating general information regarding the NIST framework to our member credit unions.**
    h. **Very limited at this time.**
    i. **We are using it as a catalyst to raise general awareness of the issues with those groups, but not at a detailed subcategory level. The goal is to organize our processes and technology along the 5 main categories.**
    j. **Not at this time. The Framework is mapped to our Common Control Framework, and we report via this method as it facilitates generating metrics once to report on multiple regulatory and guidance framework requirements, and is familiar to our key stakeholders.**
    k. **No, the organization is continuing to use ISO27001 as the basis for discussions with the board and outside organizations but is keeping a close eye on the ongoing development and use of the NIST Cybersecurity Framework.**
    l. **We provide stakeholders, including regulators, information on how our cybersecurity risk management processes align to the NIST Cybersecurity Framework.**
    m. **Not at this time.**
    n. As an active participant in past NIST Cybersecurity Framework workshops and an advocate for Framework usage, FSR/BITS is at the forefront of Framework awareness outreach.
        i. ***Member Level***
            1. At the member level, FSR/BITS routinely discusses the NIST Cybersecurity Framework and its attendant risk management principles through a variety of fora. This past month, during its CEO Fall Conference, FSR/BITS briefed its members' Chief Executive Officers and designees on the development of the NIST Cybersecurity Framework, its potential usage as a risk management communication tool to smaller entities and vendors, the goals of the Framework, and this open request for information. On recent working group calls for our information

security, privacy, and operations professional members, senior NIST staff described the Framework, its potential uses as a tool, ongoing Framework and Executive Order related activities, and NIST's desire to obtain recommendations on improving the Framework through this RFI process.

2. During one of our working group calls, members shared NIST Cybersecurity Framework anecdotes. One institution suggested a survey, which has been obviated by this RFI. Another several Financial Institutions shared that they had done a crosswalk of the NIST Cybersecurity Framework against their security programs as well as other NIST, ISO, and COBIT standards. CISOs for these particular institutions and others stated that since the Framework's release, their Boards' had increasingly requested their presentations on cybersecurity and cybersecurity risk management related issues facing the organization. One CISO mentioned that a few Board members had even enrolled in all-day seminars to learn more about cybersecurity, cybersecurity risk management, and cybersecurity risk mitigation. Another stated that they were conducting vendor and third party review against both NIST's 800-53 rev 4 and the Framework.

ii. ***Sector Level***

1. At the sector level, FSR/BITS is a member of groups such as the Financial Services Coordinating Council (FSSCC), the Financial Services Information Sharing and Analysis Centers (FS-ISAC), and an informal sector collaboration known as the "Joint Trades," which is composed of FSR/BITS, FSSCC, FS-ISAC, The Clearinghouse, fTLD Registry Services, SIFMA, the American Bankers Association (ABA), and the Independent Community Bankers of America (ICBA).
2. At the most recent "Joint Trades," meeting in September, we hosted a panel on Government Initiatives that included a presentation by NIST on "NIST Framework Implementation." The NIST speaker not only provided an overview of the NIST Cybersecurity Framework itself, but also described its purpose, provided anecdotal use cases, and informed the audience of major financial institution Chief Executive Officers, General Counsels, Chief Risk Officers, and Chief Technology & Operations Officers, among others, of the next steps, including this very RFI and companion October workshop.
3. At the mid-August FSSCC-FBIIC in-person meeting, FSR/BITS updated attendees on NIST Cybersecurity Framework related activities, including the then impending NIST RFI, and suggested that member firms be prepared to provide input for a sector response. This presentation and focus on NIST Cybersecurity

Framework usage was an outgrowth from the regularized FSSCC policy committee teleconferences in which the Framework, usage, concerns, and anecdotes are routinely discussed. Attendees included a whole host of professional security and operations personnel within member companies.

4. Moreover, prior to the release of the NIST Cybersecurity Framework, FSR/BITS coordinated the financial sector's input in the development of the Framework through the Financial Services Sector Coordinating Council (FSSCC). In particular, FSR/BITS served as the policy co-chair of the FSSCC during the Framework development's comment period and attended four of the five NIST workshops around the country. During this development process, FSR/BITS individually and through the FSSCC also gathered policy makers and thought leaders, engaged executives at member companies at additional events, and submitted two substantive comment letters (including one with detailed answers to 32 questions posed by NIST). As evidenced in the Framework 1.0, NIST specifically acted on FSR/BITS - FSSCC concerns, including recommendations to adopt a risk-based methodology and the usage of a privacy schema consistent with the statutory approach that Congress enacted for the financial services sector.

iii. ***Industry-Wide Level***

1. In May, FSR/BITS participated on a webcasted panel composed of representatives from the financial services, telecommunications, information technology, and energy industries to discuss NIST Cybersecurity Framework awareness and usage. During its panel presentation, FSR/BITS shared some of the below member anecdotes and mentioned how the financial services sector is beginning to use it to communicate cybersecurity risk management principles to its vendors, suppliers, and other sectors.
2. Following this presentation, FSR/BITS has continued informal conversations about usage with a loose coalition of trade associations that represent virtually all the sectors of the economy. This group tends to speak informally at least once a month.

5. Is your organization using the Framework to specifically express cybersecurity requirements to your partners, suppliers, and other third parties?
   a. **No- we use other NIST standards like 800-53 and 63 for that purpose**
   b. **No we are using the Shared Assessments tool SIGv7**
   c. **No, as 3rd party attestation e.g. AUP/SOC2/SOC3 or Self-Identified questionnaire e.g. SIG are not aligned to the NIST framework.**

d. **No but portions of the Framework are included in the Vendor Risk Management Program.**
e. **No**
f. **NIST is not the main Framework we utilize at this time but increasingly likely that we will move to it in due course.**
g. **n/a**
h. **No**
i. **No. To my knowledge we have not used it externally as of yet.**
j. **No, we are primarily using NIST SP 800-53, as it is more specific, comprehensive, and discrete in terms of controls.**
k. **No**
l. **Our organization already has a very mature vendor risk management program in place that addresses cybersecurity requirements.**
m. **Not at this time.**
n. **See response to Questions 4.**

6. Is your organization doing any form of general outreach or education on cybersecurity risk management (including the Framework)? If so, what kind of outreach and how many entities are you reaching? If not, does your organization plan to do any form of outreach or awareness on the Framework?
   a. **We introduced it to our Affiliates (subsidiaries) through an internal ISAC we run for them. No**
   b. **Internally only at this stage.**
   c. **Yes, through publications**
   d. **Yes, internally with key stakeholder and senior management.**
   e. **Yes**
   f. **We have a number of different risk management and Operational Risk activities that provide us with an assessment mechanism to enable us to determine current cybersecurity capabilities, set individual goals for a target state, and establish plans for improving and maintaining the cybersecurity programme.**
   g. **CUNA continues to reach out to all our member credit unions, including with general cybersecurity risk management; the NIST framework; National Credit Union Administration (NCUA), FFIEC, regulatory, and FSSCC developments.**
   h. **Current education is based on our existing framework. As we incorporate NIST, we expect our training to change accordingly.**
   i. **On March 18th we organized a ½ day session for our membership on the topic with representatives from Treasury, NIST and the sector to discuss it, about 120 people attended. We are also embedding it within our legislative and regulatory outreach with the goal of driving further use of it by the regulators as a standard way of approaching cybersecurity. We have also done webinars with our clearing member firms to introduce and explain the framework to their clients (introducing brokers). Lastly, we provided our board with a primer on the NIST-CF to ensure awareness as well. Lastly we have developed a**

cybersecurity guide for small broker dealers (<100 employees) and have made the NIST-CF and the need for an assessment as the central tenants of the document for how to organize a firm's protection posture.

j. **Internal awareness within information security and key partners.**
k. **The organization has an ongoing set of initiatives revolving around cybersecurity that are driven by both strategic and tactical needs. This includes general awareness to all associates as well as targeted training to those with particular needs. At present, we are not planning to develop or deliver any outreach specific to the Framework, either within the firm or to outside parties such as vendors/suppliers.**
l. **Yes, we conduct outreach to client groups and employees on cybersecurity risk management.**
m. **We use many opportunities to educate our customers and business partners, but have not incorporated the framework into those communications.**
n. **See response to Questions 4.**

7. How would you characterize your regulator's awareness and use of the Framework in their assessments of your cybersecurity risk management - helpful, flexible, inconsistent, strict, etc.?
    a. **Helpful**
    b. **Unknown**
    c. **Our regulators are aware of it. Though, we haven't seen them referencing / using it as part of their assessment of us.**
    d. **Implicit – feedback or guidance on asset scope would be welcome.**
    e. **Aware—but not aware of them using it**
    f. **Regulator is aware but we cannot respond on behalf of the regulator in terms of their assessment.**
    g. **n/a**
    h. **One regulator did use portions of the framework to assess us. Other have not done so yet.**
    i. **In our discussions we fine they are aware, but it is not clear how they will apply it in practice for exams or in guidance that we expect will be forthcoming. Opposite of the NIST-CF process they have not engaged in any type of partnership on this.**
    j. **We have not yet experienced any direct Framework references by regulators, with the exception of FISMA (our role as a Government contractor), but have read numerous media reports and allusions by representatives of the regulatory agencies regarding the same.**
    k. **Outreach by and discussions with our primary regulator would indicate it is very aware of the Framework and have included it into their information**

requests as well as their examination protocol. However, they do not appear to be using the Framework as delivered, but are tailoring the evaluation criteria including modification of the scope and nature of various functions and sub-functions. We believe maintaining consistency with the framework core would allow for greater consistency in its application promote better cross-sector communication. It is too early to tell whether the regulator's assessments using the framework are consistently applied across organizations under their purview. However, their public articulation of expectations have been helpful in ensuring organizations are adequately prepared for examinations when they occur.

l. **We have a seen a number of regulators using the Framework, or components of the Framework, in their engagements with our organization. We would encourage our regulators to use the Framework as a guideline – rather than some type of prescriptive set of "expectations". This will enable a more robust review of an organization's cyber risk management practices in a more effective, risk-based manner, as opposed to a "check the box" compliance exercise.**

m. **We characterize regulatory awareness as very high. However, we have not seen our regulators use the Framework in their cybersecurity risk management assessment process within our institution.**

n. **Because of the highly regulated nature of our sector and because of FSR's membership composition, our member regulators include the Securities and Exchange Commission (SEC), the Office of the Comptroller of the Currency (OCC), the Federal Reserve Board (FRB), the Federal Depositors Insurance Corporation (FDIC), FINRA, and the Consumer Financial Protection Board (CFPB) amongst others. In April, the SEC's Office of Compliance Inspections and Examinations announced that it would be conducting examinations of approximately 50 registered broker-dealers and investment advisors to assess cybersecurity preparedness. As part of that announcement, the SEC listed a set of potential questions that it might ask during the examinations and stated that "some" of the questions tracked information contained within the Framework. A FSR/BITS member compared the two documents and confirmed this, stating in sum that quite a few, if not most, tracked the controls expressed within the NIST Cybersecurity Framework. More recently, when asked, representatives of the FFIEC and FFIEC member agencies have stated "that they are aware of the NIST Cybersecurity Framework and that it is a useful tool."**

8. What expectations have not been met by the Framework and why? Specifically, what about the Framework is most helpful and why? What is least helpful and why?

a. **The integration of policies and specifically control standards with specific practices is labor intensive and not worthwhile for mature programs. Business Drivers and Tiers/Profiles**
b. **I don't understand why the framework dropped several of the NIST Controls. We have decide to implement them all.**
c. **Framework and related components are not directly measurable. We like to see more of a measurable framework.**
d. **We believe no significant areas have been left out of the Framework. The organization and hierarchy of categories and subcategories, along with the specific references. The lack of metrics surrounding adherence or "compliance" to the Framework is the least helpful.**
e. **n/a**
f. **There is no one-size-fits-all answer for cybersecurity, and governments cannot provide comprehensive, prescriptive guidelines for all entities across industries. While the Framework offers worthwhile standards for improving cybersecurity, it does not fully address all critical areas such as privacy.**
g. **n/a**
h. **State Street is not yet using the framework in its entirety, but is using some parts. For instance, State Street has pulled out specific security controls from NIST SP 800-53, and is using NIST SP 800-30 to help to develop and create a Risk Assessment template process. We are still in the process of evaluating the NIST Framework to assess integration and applicability to our specific environment.**
i. **At this point we have not heard or discovered any major issues with the NIST-CF from our work or in discussions with our membership. In our mind it is still early days in the use of the NIST-CF and many more uses and inclusions should be forthcoming as the market begins to develop around it. The opportunity to have one standard for all sectors with minor modifications is a key selling point for further use in the third-party risk management space. It is our hope that NIST will continue to own the Framework and improve upon it and enhance it. This leadership and participation has been critical to its success.**
j. **Expectations were met; however, implementation or adoption of the Framework, and incorporating Framework parlance into our lexicon, does present potential challenges. These may include that regulators could measure against differently relative to the preexisting framework. (This was noted in prior feedback to NIST specifically citing the existence of NIST SP 800-53 and the ISO/IEC 27000 series).**
k. **While the core structure of the Framework is solid, having been built using various existing standards and models, the "hype" associated with the Framework may have set expectations of something more groundbreaking. Furthermore, while the notion of implementation tiers provides for a more flexible approach in the application of the Framework, the lack of practical examples or reference models through sample profiles either at a broad or**

sector level make it difficult to understand the expectations of external entities such as regulators.

l. **The Framework is helpful by creating a common lexicon regarding cybersecurity risk management, particularly among those entities whose cybersecurity risk management practices are in the early phases of development and implementation. The Framework could be a useful tool among regulators, provided there is agreement among regulators on use of the Framework within existing regulatory regimes. It could also be helpful to harmonize cybersecurity regulations among regulators, particularly for those firms who are regulated by more than one regulatory agency and/or type of regulator (i.e. sector specific or non-sector specific).**

m. **We expected that the Framework addresses all industries indiscriminately. This expectation was met, and the Framework now helps us communicate the need for strong cybersecurity risk management requirements to our business partners, as well as the need for incident and vulnerability information sharing. What may not be helpful is that we have made good progress in the Financial Industry public-private partnership in support of the National Infrastructure Protection Plan, and we would be concerned if the Framework were presented as a required approach as we are very far along already. We would not find it helpful if it were to require resources to demonstrate compliance, as these are better spent on the risk management process itself.**

n. **In discussing the NIST Cybersecurity Framework, members have stated that the Framework is helpful in that it provides a common lexicon that is accessible not only to various functions within a given organization, but across sectors as well. It has also been helpful in that it has raised the profile and importance of cybersecurity risk management across sectors and across many more C-suites. As noted, one member is even introducing it into the organization's vendor management process. Areas for improvement and further investigation are discussed below in the response to Question 9.**

9. What improvements do you suggest for the next version of the Framework?

a. **Integrate it with eGRC solutions**

b. **Align with the NIST framework to the fullest, minus those things that are inherently government such as Certification and Accreditation with Designated accrediting authority.**

c. **Making it Measurable**

d. **As stated earlier, metrics for adherence and or/completion; further information on maturity levels; alignment with international standards and/or applicable regulations.**

e. **Risk Prioritization Concept**

f. **An improvement would be to include the requirement to implement processes to identify and understand threat actors' (nation state, hacker groups and individuals), their motivations, their capabilities, and the data they seek. Good**

practice is to understand and anticipate threat actors through intelligence gathering, and then apply adequate safeguards.

g. **More information targeted towards how small financial institutions can incorporate the voluntary NIST framework could be helpful.**
h. **None at the moment.**
i. **More fully developed maturity model, metrics to baseline and measure certain aspects of the framework, a tempered approach to enhancing privacy understanding the main goal is to improve protections, the development of a set of controls and tests to determine achievement of the outcomes or pointing back into the standards for that, and for small firms a more perspective or prioritized set of outcomes to start on**
j. **The framework is only six months old and should be allowed to "steep" and be adopted by many organization across all critical infrastructure sectors prior to being modified and revised. Additional time and use should guide any revisions.**
k. **The next version of the Framework should focus on building supplemental collateral to make it more actionable by a broad constituency. This focus should take into account organizations at various levels of maturity along the cybersecurity spectrum. NIST should continue to bring consistency through ongoing awareness, practical examples and collaborative opportunities.**
l. **NIST should begin development of the next version of the Framework only after there has been sufficient time for entities to determine how to incorporate it into their risk management processes. This will take time, and NIST should not rush to issue the next version of the Framework if it is not going to include improvements that reflect the lessons learned from Framework implementation. There should be a next version to address gaps and areas of improvement that have substantial agreement among the government and the private sector. One specific recommendation is to include cross-references to selected non-US frameworks – such as ISF – as a foundation for harmonization across global firms.**
m. **To the extent that this document is used in assessments, we would require more guidance for the Assessor to recognize compliance with the Framework.**
n. **Several of the FSR member CISOs that mentioned that they had done a crosswalk of the NIST Cybersecurity Framework and their own security programs and/or the NIST, ISO, and COBIT standards also mentioned that this was an extremely resource intensive process. One CISO said that he had "locked 2 senior security professionals in a room to do this comparison using a detailed self-assessment and that it had taken 4 weeks." Others answered similarly. One other member, in particular, stated that her organization had devoted as much as 4 people (some from information security and some from legal and compliance) to do a similar task of assessing against the Framework and that after six weeks, they had only completed an initial Framework "tiering." These professionals expressed their concern that for institutions that did not have similar size and resource allocation, they would find it very**

difficult to do such a walk through. They stated that although they understand that every institution has different systems and different threat profiles, they suggested that NIST nonetheless provide some examples of security controls that when implemented would provide the most benefit for the least cost. These security professionals said that otherwise smaller institutions will have real trouble in best allocating resources and in elevating their security posture. One FSR/BITS member and information security professional strongly suggested that NIST could help improve usage by developing some way for institutions to benchmark within and across sectors.

##