From: **Stacey Barrack**
Date: Mon, Apr 10, 2017 at 2:22 PM
Subject: ISA/FAIR Institute Cybersecurity Framework 1.1 comments
To: "cyberframework@nist.gov" <cyberframework@nist.gov>
Cc: Larry Clinton, Nick Sanna

To Whom It May Concern,

Thank you for the opportunity to provide feedback on the proposed draft Cybersecurity Framework 1.1. Please find attached comments filed jointly between the Internet Security Alliance and the FAIR Institute.

Thank you in advance for your review and consideration of our comments.

As always, should you need anything, please don't hesitate to reach out – happy to help.

Best,

--
Stacey B Barrack | Internet Security Alliance | Director of Policy and Programs | 2500 Wilson Blvd., Arlington, VA 22201

[Attachment Copied Below]

Edwin Games
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, M.D. 20899

RE: Proposed Update to the Framework for Improving Critical Infrastructure Cybersecurity

Dear Mr. Games,

Thank you for the opportunity to provide joint commentary from the Internet Security Alliance and the FAIR Institute on the proposed version 1.1 update to the Framework for Improving Critical Infrastructure Cybersecurity.

EXECUTIVE SUMMARY

The Internet Security Alliance (ISA) is a multi-sector trade association representing mainly the chief information security officers of Fortune 100 companies. ISA has a long-standing interest in seeing that the Framework achieves its objectives of better private-sector cybersecurity. ISA's Cybersecurity Social Contract, published in 2009, first called for the collaborative industry-government development of standards and practices suitable for voluntary adoption reinforced by market incentives that lead to Executive Order 13636 and the NIST Cybersecurity Framework (CSF). Since the CSF was unveiled in 2013 ISA has worked with the National Association of Corporate Directors (NACD) to integrate models such as CSF successfully into enterprise wide risk management programs.

FAIR Institute is an organization with over 1,200 industry members that promotes a standard analytics risk model (FAIR) for information and operational risk that facilitates an economic analysis of cyber risk. FAIR has already been listed by NIST on the NIST CSF Industry Solution Page as a complementary analytics model for quantifying and prioritizing risk.

NIST's process of private sector outreach and its proven track record of adjusting the Framework according to public input is a model among federal agencies for public-private partnerships. ISA and FAIR believe this process should be extended in a fashion similar to that which resulted in the development of the NIST CSF, but this time focused on implementation. ISA and FAIR believe that their models are complimentary to the CSF and that a useful outcome of the NIST 1.1 effort would include illustration of how these models can be used to create a broader and economically sustainable approach to enterprise-wide cybersecurity.

INTRODUCTION

The need for urgent, comprehensive and effective action to combat our cybersecurity threats has never been greater. The Internet, which is inherently insecure, is becoming even more so with the explosion in mobile devices and the Internet of things. At the same time the system is getting weaker and the attackers are getting ever more sophisticated. In March the NSA acknowledged that nation states are now robbing banks and FireEye reported that the criminals are becoming so sophisticated that there is virtually no difference between them and the nation states. The evolution of the threat raises the bar both with respect to economic loss but also threat to disabling critical infrastructure. At the same time, all the economics of cybersecurity favor the attackers – attack tools are cheap and easy to acquire, and profits are enormous. Meanwhile defenders are protecting an inherently flawed system, are almost always a generation behind the attackers and there is virtually no effective law enforcement deterrent – we prosecute one percent of cyber criminals.

ISA has long maintained that the NIST Cybersecurity Framework (CSF) is a world-leading step toward a better system of cybersecurity. Since its inception it has been the primary model government has advocated for enterprise security. However, the sad and undeniable fact is that we are losing the fight to secure the Internet. It has long been known that doing the same thing and expecting different results is illogical. The CSF alone is not able to create the system of sustainable, long-term cybersecurity that meets our collective economic- and national-security needs. For that, we must evolve a comprehensive risk management process that facilitates efficient use of scarce cybersecurity resources. The CSF, which operates primarily at the operational level, constitutes a critical, but not sufficient, element of this system. As the Framework continues to evolve into its 1.1 version and beyond, it needs to be integrated into a more fully articulated enterprise wide cyber risk management process that builds on and integrates models developed within the private sector since the 1.0 version of CSF was created. ISA and FAIR are advocating that NIST, working in concert with the private sector as well as other agencies of government, convene a program of similar size and scope as that went into development of NIST 1.0 to focused on implementation of the Executive Order that NIST 1.0 was based on.

NIST 1.1 SHOULD BEGIN BY ADRESSING THE EFFECTIVNESS OF NIST 1.0

The Framework in its current condition was never envisioned as the final product of the executive order that led to its creation. Executive Order (EO) 13636 called for the CSF to be at the heart of a program that is voluntary, prioritized, flexible, repeatable, performance-based, and cost-effective.[1] While there have been anecdotal reports of various "uses" of NIST CSF in the past few years the government has not yet produced empirical evidence of the extent to which NIST CSF 1.0 has changed behavior, to what extent such behavior change may have improved cybersecurity nor if these behavior changes are cost effective and therefore sustainable for long term security. For it's effectiveness to be maximized in the context of private sector organizations a greater emphasis needs to be placed on its economics.

---

[1] Executive Order 13636 "Improving Critical Infrastructure Cybersecurity," Section 7(b). https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

Demonstrating cost-effectiveness is particularly important for maintaining the voluntary nature of the Framework.

No organization wants to be the victim of cyber attacks. Nonetheless, for the private sector—owning 80%-90% of cyber infrastructure and operating under a mandate to maximize shareholder value—the cybersecurity risk management calculus is inherently economic. If use of the CSF, with its admirable flexibility, can be demonstrated to be cost effective, regulations will not be required. Organizations naturally do what is cost effective. However, simply asserting that the CSF is cost effective writ large is unlikely to persuade entities currently not using the CSF to adopt it.

As NIST looks to the future of the CSF, it must embrace the totality of E.O. 13636. To that end, we propose NIST deploy its considerable prowess in convening public-private partnerships to being a new process whose result is a methodology that individual entities can use to adapt the Framework in the most cost effective manner to meet their unique cyber-risk profile.

Fundamental to this process would be a consensus methodology for determining cost-effectiveness. ISA and FAIR believe such a methodology can be developed and usefully adapted to industry sectors. We reject the assertion that security can't be measured and hence efforts to determine cost effectiveness are fruitless. If cost effectiveness cannot be measured the only response would be for companies to implement absolutely every possible security measure, thus dooming any pretense of a risk-based approach.

We will concede that just as absolute security will not be achieved, perfect measurements will also be elusive. This lack of perfection, which is endemic to all social sciences, is no excuse for not trying to develop a useful mechanism to assist organizations to apply elements of the Framework most useful and cost effectively for their purposes. Indeed, developing this mechanism is critical for the maintenance of the voluntary model defined in EO 13636.

As with Framework development, which built on previous existing standards and practices, the private sector has already created a basis from which these next steps can proceed. The comments below highlight some of the specific issues ISA and FAIR find with the current NIST draft, outlines the models the private sector has developed since NIST CSF 1.0 was created and points toward a process that will further develop these models and integrate a refined NIST CSF 1.1 into them.

SPECIFIC COMMENTS ABOUT THE NIST DRAFT

In the following comments, we address language from the new proposed Section 4.0 and suggest revisions. A subsequent section discusses the need for increased consideration of small business cybersecurity needs.

1. Replace language in Section 4.0 calling for "external audit" or "conformity assessment". Section 4.0 contains the following proposed language (draft line numbers noted in parenthesis):

> (745) Measuring state and trends over time, internally, through external (746) audit, and through conformity assessment, enables an organization to understand and convey (747) meaningful risk information to dependents, partners, and customers.

No one, certainly not ISA or FAIR, is saying we ought not to have cybersecurity controls. And we acknowledge that discussion here of "external audits" and "compliance" is intended to remain within the context of a voluntary system of cybersecurity, which the ISA and FAIR support.

However, even to suggest that the path to better cybersecurity metrics lies through audits or compliance assessments is to set the private sector on the wrong path. The term "audit" has a long and generally well-understood meaning. The reality is that in most companies they are more afraid of the cybersecurity auditor than they are the cyber attacker. This is in part because audits, based on the long understood financial audit model, are a pass-fail proposition. Everyone needs to have a "clean" audit.

Cybersecurity is not a pass-fail proposition. You are not either secure or not. Cybersecurity is a continuum and not every organization or every asset within an organization needs to be at the same level of cybersecurity. While NIST correctly abandons the traditional binary grading for the CSF, most cyber audits do not. Audits demonstrate what a company has done at point in time. But cybersecurity is how well you do it on a consistent basis, and auditing models are not designed to capture that dimension of company activity.

The suggested language in Section 4 may open the door to mandatory or quasi-mandatory compliance regimes. Should it become final, regulators would likely state that the audits carry an imprimatur of approval by the Framework—and so should be implemented wherever possible. Regulators may easily stop short of issuing a rule with explicit mandates and instead issue "guidance." Such guidance would inevitably become a de facto requirement; such is the importance corporate counsels attach to regulatory "guidance."

Despite the supposedly voluntary model embraced by NIST CSF, ISA member companies across sectors are seeing and explosion in cybersecurity regulations and quasi regulations. Organizations in the financial sector report up to 30 percent of their cybersecurity budget being diverted to compliance costs that not only do not necessarily equate to any security improvements but consume scarce resources and thus exact an opportunity cost in lost time and money to deal with pressing cybersecurity problems.

There is a path forward. The ISA has worked with the Center for Audit Quality (CAQ) and the American Institute for CPAs (AICPA) in the latter's effort to develop an entity-level cybersecurity reporting framework that organizations can use to communicate useful information about their cybersecurity risk management program to a broad range of stakeholders. The AICPA's cybersecurity reporting framework has been developed to provide the market with a common approach to reporting on and evaluating a company's cybersecurity risk management program. The approach will be voluntary, flexible, and comprehensive.

The AICPA plans to adapt and advance the cybersecurity-reporting framework according to feedback from users in the marketplace, with an emphasis on identifying opportunities to enhance efficiency and reduce compliance burdens. This process, which includes outreach to the government, ought to be allowed to play out to develop a more appropriate mechanism to assess cyber risk that reflects an organization specific perspective on cyber risk and embraces the maturity concepts supported by ISA, FAIR and NIST.

2. Rewrite Section 4.1 to emphasize the strategic nature of cybersecurity's effect on business results

This section has an important message to communicate: That cybersecurity is an enterprise-wide risk management issue, not just a technology one. NIST has taken an important step in placing cybersecurity in its proper context. Ultimately, risk acceptance and resource allocation decisions that underpin cybersecurity are business decisions. Information technology is merely the enabler.

However, we are concerned that by advising companies to correlate micro business objectives with their cybersecurity programs, the proposed draft proposes something that is difficult, if not impossible, to achieve and worse, creates a distraction to pursue a new holy grail. Has the NIST concept here even been piloted successfully across critical sectors? This isn't to say that ISA doesn't believe that cybersecurity should be integrated into business objectives, nor that we don't want metrics for cybersecurity. We do. But when we discuss metrics and business objectives, the goal is to track the costs necessary to reduce risk exposure, not the impossible-to-quantify correlation of cybersecurity spending to granular business results. Businesses need the freedom of choice to determine WHAT they do for cybersecurity, WHY they do it, and HOW they get it done. In time, the free market will generally hold business accountable for cyber results where regulators don't. In many sectors, regulators and courts will drive accountability.

The draft itself acknowledges the difficulty of this prospect when it states that in lines 777-778 that "There are a large number and variety of contributing factors to a given business objective." It does so again in line 792 when it states "The effect of cybersecurity outcomes on a business objective may often be unclear."

In the one proffered example, the draft explicitly acknowledges the sheer impossibility of the proposed task at hand. On lines 778 to 783, a hypothetical retail bank implements stronger authentication to increase online banking, but the draft acknowledges that success of the objective— more customers using online banking—is contingent on activities unrelated to cybersecurity. Those include "developing the messages regarding trusted online transactions, targeting specific demographics of consumers, selecting communications channels…and marketing those communications channels over a duration necessary to achieve the objective."

In short, this draft section aims in the right direction, in that companies looking to demonstrate that cybersecurity matters must describe cybersecurity through the language of business objectives. But draft section 4.1 gets quickly bogged down in the thicket of all the inputs that go into business decisions, of which cybersecurity is just one of many. It asks the impossible of already over-burdened cybersecurity organizations, and that is to quantify their effect on the success of business objectives.

Rather than directing users of the NIST Cybersecurity Framework to wade into this morass, ISA believes it is better to advise them to approach cybersecurity strategically as part of any significant business decision. We present an alternative model for linking cyber risk management to business goals and objectives, based on an existing and independently verified program below.

3. Section 4.2 should be changed to focus on independent validation of effectiveness

The proposed Section 4.2 essentially seeks to fill the gap in knowledge about the effectiveness of cybersecurity practices by proposing implementation of the Framework as the means to measure increased cybersecurity. Line 829 to 831 states that "the cybersecurity outcomes of the Framework Core

are the basis for a comprehensive set of cybersecurity management metrics. The aggregate of these metrics equals a reduction (or not) of cybersecurity risk."

The draft language then suggests metrics. Lines 847 to 848 state that a "leading way" to measure an outcome within the Data Security Category of the Protection Function would be "implementing protective mechanisms."

What's missing is any independent way to measure how implementation of a control (or set of controls) has reduced a company's risk exposure in a cost-effective manner.

This amounts to a self-referential loop, by which security is measured by implementation of the control, which is then judged by if it was implemented.

What companies truly need is a way, by example and case study, to observe how a control (or set of controls) diminishes risk exposure and the costs associated with that diminishment across multiple sectors for small, medium, large entities. For that, companies need a way to quantify cyber-risk and observe the effect of controls on their risk exposure. They need a frame of reference that lies outside of the Framework or process-based measurement that loops back to implementation of controls.

In short, an effective metric is not whether controls have been implemented, but on whether the controls are reducing risk—and just as importantly, is risk being reduced in a cost-effective fashion.

The proposed draft also misses an opportunity to discuss cost-effectiveness, when in lines 852 to 862, it discusses informative references. The example includes encryption of media storage, which is a well-known way to protect data-at-rest. But not all data is the same. Companies confronted with a decision about paying for encryption software must answer the question of how much to spend. Should the company encrypt all its hard drives? Should it pay for an immediate rollout of encryption software, or should laptop and desktop hard drives be upgraded with encryption capabilities per a schedule dictated by the normal refresh rate of such equipment (i.e., as old computers become obsolete and are replaced with newer ones)? These are real-world questions faced by companies in the position of making spending decisions about cybersecurity. Any discussion of metrics must consider the cost dimension—something, again, that is only possible with a way to measure quantifiable reductions in risk exposure.

Again, we will present below an alternative model to achieving the goals we believe NIST aspires to.

<u>METRICS: WHAT DO WE NEED TO MEASURE?</u>

We are greatly encouraged that NIST is proposing the addition of a new section on cybersecurity measurement to the Framework (Section 4) titled "Measuring and Demonstrating Cybersecurity." Since the NIST CSF was initially launched ISA has campaigned for the Framework to be tested to demonstrate what aspects of the model are most effective, and cost effective for varying elements of industry.

Developing adequate metrics for the Framework is difficult, yet essential for many reasons including the need to maintain the voluntary nature of the program. In addition, even large companies are unlikely to deploy the CSF in its entirety and will need a practical way to allocate scarce resources. Smaller companies represent one of the Internet's most vulnerable elements. The CSF is literally already overwhelming for many of them. Measurement that indicates what elements or aspects of the NIST CSF are most effective can lead to prioritization and greater adoption of characteristics that are most useful to these organizations.

While we applaud NIST's foray into metrics we remain mindful of the traditional statistical caution - garbage in, and garbage out.

What is measured, and what these measurements are taken to mean, is of critical import as this effort is launched. The need to develop a consensus nomenclature is fundamental to any valid measurement system. The NIST CSF has long suffered from the lack of clear definitions. For example, the terms "adopt' and "comply" have been displaced in discussions by the undefined term "use." While the verbiage use has benign impact as a euphemism for adopt, it must not be taken as a synonym for security. Perhaps even more critical is not to equate the term compliance with security. As the program to develop metrics for the NIST CSF is launched it is vital that security be clearly defined from the users' – not the government's – perspective.

We are concerned the current draft's proposed approach to metrics and measurement is self-referential and may lead toward an inappropriate checklist compliance regime that is counterproductive to sustainable cybersecurity.[2]

AN ENTERPRISE WIDE APPROACH TO METRICS THAT INTEGRATES NIST CSF AT THE RIGHT LEVEL
To develop a sustainable and cost effective model for cybersecurity, one needs to begin with understanding the uniqueness of the cyber threat. Cybersecurity is not like traditional consumer product safety, which can be managed by articulating a reliable set of minimum standards or controls that constitute safe operation. Cyber threats are dynamic ever changing with technological and attack method innovation.

Rather than basing a security methodology on a list of controls, the key issue is how can we put leadership in position to best make informed cyber risk decisions?
Research by the Conference Board conceptualizes a digitally secure organization as a pyramid wherein a strategic entity, such as a board of directors, operates at the pinnacle.[3] Beneath that is a management structure charged with defining and managing a process to carry out the organization's strategy (in this case a cybersecurity strategy) and finally an operational layer charged with implementation.

THE PINNACLE OF THE PYRAMID: STRATEGY

In 2014 The National Association of Corporate Directors (NACD), in conjunction with the ISA, published the "Cyber-Risk Oversight Handbook." (Updated in 2017)[4] The NACD Handbook differs from most previous work in the field. Rather than attempting to teach the boards more about IT, (most boards don't talk about ISO standards and NIST Frameworks) the Handbook contextualizes cybersecurity within issues boards are comfortable with (mergers/acquisitions, PE Ratios, innovation, strategic partnerships). The Handbook encourages boards to approach cybersecurity through the perspective of making sound business decisions. The Handbook defines five key principles that boards should use in developing organizational strategy for cybersecurity. These principles are:

---

[2] Internet Security Alliance. "The Cybersecurity Social Contract: Implementing a Market-Based Model for Cybersecurity," pp.3-19.
[3] Andrea Bonime-Blanc. "A Strategic Cyber-Roadmap for the Board." https://www.conference-board.org/publications/publicationdetail.cfm?publicationid=7346&centerId=1
[4] Cyber-Risk Oversight Handbook https://www.nacdonline.org/Store/ProductDetail.cfm?ItemNumber=10687

- Cybersecurity is not an “IT” Issue;
- Boards must understand their unique legal obligations for cybersecurity;
- Boards must have access to appropriate levels of cybersecurity expertise;
- Boards must demand that management define a clear cybersecurity framework that they will follow;
- Boards must understand organizational cyber risk and what risks they are accepting, mitigating or transferring.
-

The Handbook has not only proven to be extremely popular with industry, but both the Department of Homeland Security and the Department of Justice have endorsed it.

More importantly, the positive impact of the Cyber-Risk Oversight Handbook on consensus security outcomes has been highlighted by PricewaterhouseCoopers. PWC’s 2016 Global Information Security Survey reported, "Guidelines from the National Association for Corporate Directors (NACD) advise that Boards should view cyber-risks from an enterprise-wide standpoint and understand the potential legal impacts. … Boards appear to be listening to this guidance. This year we saw a double-digit uptick in Board participation in most aspects of information security. Respondents said this deepening Board involvement has helped improve cybersecurity practices in numerous ways. It may be no coincidence that, as more Boards participate in cybersecurity budget discussions, we saw a 24% boost in security spending. Other key outcomes cited by survey respondents include identification of key risks, fostering an organizational culture of security and better alignment of cybersecurity with overall risk management and business goals. Perhaps more than anything board participation opened the lines of communication between the cybersecurity function and top executives and directors.”

ISA recommends that an element of the metrics process NIST should launch as part of NIST CSF 1.1 include examination of methods boards can use to determine how best to address the NACD principles and coordinate with senior management regarding their implementation.

THE SECOND LEVEL: APPLYING AN ANALYTICAL MODEL

The second level of the Conference Board pyramid consists of senior management. They, too, need to consider cybersecurity in the language of business, albeit at a greater level of detail than the directors who oversee them. For this level of corporate leadership, cybersecurity is best viewed within the confines of a risk management strategy that describes decisions in terms of cost (rather than the operational language of pure technology). It is at this level that the NIST CSF functions, Identify, Protect, Detect, Respond, and Recover is best integrated.

Since the initial release of the CSF the private sector has developed models that can be adapted to the CSF and be used to extend the CSF allowing senior management to assess risk in a fashion that reflects the economic impact of the risk and thus better prioritize and implement strategies to manage it. One example of such a process is articulated by the Factor Analysis of Information Risk (FAIR) approach.

At its core the NIST CSF is essentially a checklist of various standards and practices. Even if an organization “uses” the CSF there will virtually always be gaps in that use. In addition, check lists generally simply set lowest common denominators levels of controls and so even if an organization “complied” with CSF we still wouldn’t know if that was sufficient to achieve the needed level of security.

FAIR can assist in extending the analysis an organization can make to better prioritize the operational efforts based on the cost factors that are endemic to a private sector entity.

FAIR is an analytic model that enables an organization to evaluate and measure the significance of gaps or the sufficiency of compliance so that it can make well-informed choices about where to apply its limited resources. Because FAIR enables true quantitative measurement in economic terms (versus more common ordinal measurements), its results are inherently meaningful to business executives.

FAIR seeks to replace qualitative assessments of risk often driven by high-anxiety keywords by a quantitative assessment of risk, as characterized by two main factors: loss event frequency and loss magnitude. This "decomposition" approach toward risk replaces assumptions about risk with probabilistic assessments. The resulting quantitative data allows companies to make informed resource allocation decisions. Proponents of the model acknowledge that some amount of estimation goes into creating a FAIR model. However, the fidelity of the models will increase over time with the accrual of experience and additional data. At a minimum, and at no cost, FAIR introduces a new lexicon of terms leaders can adopt to begin having meaningful deeper more granular conversations around components of cyber risk. Words precede dialogue and words matter.

The Framework provides a needed universe of security controls. Unfortunately, that universe, while not infinite, is still so large that without a risk management methodology such as FAIR, companies are mostly at a loss on how to practically apply the Framework. When combined with an analytic method like FAIR, the value proposition of proposed improvements becomes much clearer allowing organizations to prioritize more effectively and gain stakeholder support more easily

Methodologies such as FAIR can combine with the Framework to present companies with an actionable, cost-driven program of cybersecurity.

That's the case despite language in the framework directing them to construct as-is and to-be Framework Profiles guided by a desired Tier maturity level. With methodologies, such as FAIR, companies can attach cost figures to risk and to controls. For senior level management, cost is basic data for decision-making.

There may be limitations to the FAIR model. Loss magnitude is difficult to quantify in cybersecurity, particularly when it comes to matters such as reputation. The model works best when there is data at hand allowing companies to quantify losses, making it an easier fit for some sectors over others.

Moreover, the cost data of FAIR will need to be supplemented by a menu of incentives in cases where national security considerations outweigh pure cost considerations when it comes to allocating cybersecurity resources in some sectors. For example, pure cost data might suggest under investments into cybersecurity in areas such as utilities, where the loss event frequencies to date have been zero, at least within the United States. However, from a national security perspective, such an under investment would be intolerable, suggesting the need for incentives such as rate recovery and other mechanisms.

Thus, FAIR is complementary to good practice frameworks like NIST and fills an important gap from which all such frameworks suffer.

ISA and FAIR propose NIST should launch a program for better extending and implementing the CSF similar in size and scope to the process that went into developing NIST CSF 1.0. One goal of this work

could be a unifying document, or set of documents, that addresses all levels of a company that we've mentioned: boards, senior management, and operations, and describes how entities from various sectors and sizes can adapt the integrated model we have outlined to their unique characteristics.

4. References to supply chain risk management should explicitly take into consideration small business concerns

The evolution of the modern extended, often global, supply chain has largely been a result of modern economics. The cost and speed to market advantages of offshore supply are so overwhelming in many cases that it is a practical competitive necessity to use this technique. Notwithstanding the compelling economics, cybersecurity issues raised by the modern supply chain are equally large.

As NIST wades into this area as it extends the CSF it must be careful not to apply industrial age thinking to a digital age issue. As with issues discussed above, supply chain must be addressed with a full understanding of the economics of the problem. In an enterprise-wide risk management fashion less well-intentioned initiatives may generate counterproductive results.

For example, in the defense sector we have seen the evolution of two distinct providers' markets, one driven by the major defense suppliers and the other by a cadre of smaller, but often-critical players. While controls mandated in publications such as SP 800-171 may be fully appropriate for the prime contractors, applying these same requirements to the smaller player who lack the economies of scope and scale drives up company costs without a corresponding increase in cybersecurity.

Although at one time access to a defense contract was the brass ring for most providers (and still is for the majors) many smaller companies (often the best ones) can now find markets for their services that don't entail the dramatic new compliance costs that are associated with SP 800-171. Estimates are that as many as 25 percent of these smaller players will choose to leave the market if forced to comply. Thus, these well-intentioned supply chain requirements may weaken defense by depriving the primes – and our government -- of access to the best small company suppliers.

Moreover, many of these smaller suppliers may not truly need to provide the same level of security as the major contractors. Instead of a traditional industrial age compliance regime a thoughtful, risk-based approach to cybersecurity and the cost-effective improvements targeted at the specific threats they face, might well be a sufficient, and even preferable method to provide adequate security given their specific role in the supply chain. We address small business concerns more fully in the next section.

5. Small businesses need a prioritized set of cybersecurity controls

As helpful as the Framework is on an operational level, it was largely designed by and for larger companies. It's multiple tiers and ninety-plus subcategories make it unsuitable for the clear majority of small companies. This is not to say the Framework can't be used by smaller companies (some do). However, the multiple assessments smaller firms would have to undertake to locate what parts of the framework offer the most cost effective way to spend their next marginal dollar on cybersecurity is too great a burden for small firms operating on thin margins.

If we want small companies to become more secure, we need to make cybersecurity easier and cheaper for them. ISA recently examined five documents that prioritize cybersecurity controls to reveal the areas

of agreement.[5] Our survey revealed seven common security controls contained within all five examined frameworks: NIST ought to support the next step, which is targeted research to prioritize the framework by industry sector and identify the best places for classes of smaller corporations and nonprofits to spend their marginal dollar on cybersecurity.

By undertaking systematic testing of the framework under controlled conditions small businesses can obtain the desperately needed prioritizations of cybersecurity controls they need.

This testing should leverage the existing system of public-private collaboration as defined by the National Infrastructure Protection Plan. Each Sector Coordinating Council (SCC), in conjunction with its sibling Government Coordinating Council (GUCCI) and in collaboration with NIST, would design an appropriate testing plan for the Framework for small businesses within their sector. Once a research-based prioritized list of actions is developed from the NIST framework, multiple industry trade associations are ready, willing, and able to partner with government on outreach. Government should be using these private-sector organizations as their primary leverage vehicle for small-company outreach as opposed to setting up and running their own programs.

6. NIST CSF v1.1 should immediately prioritize and prepare to become the harmonizing document that trade associations are lobbying for on the hill, and with regulators.

A panel composed of OCC, FDIC, and The FED regulators closed the Risk Management Association's (RMA) GCOR Conference in Boston on April 5, 2017. Backed by 50+ ANPR comments, panelists indicated that they are hearing from the White House and regulators the need for harmonization. Industry generally views NIST CSF as "an anchor", a place to begin a common approach that can illuminate redundancies, duplication and counterproductive regulations even within traditionally regulated industries such as financial services.

The NIST CSF v1.1 agenda should not become a distraction to take away from the much larger opportunity to solidify NIST CSF as the anchoring Harmonization framework. Changes needed in CSF v1.1 to ensure this harmonization should be given top priority. Many of these changes are already being prepared by the financial sector through ISA friendly trade associations FSSCC and FSR/BITS. ISA has long held harmonization as a priority and will lead to a rational and economically sustainable

Sincerely,

Larry Clinton
President/CEO
Internet Security Alliance

Nick Sanna
President/CEO
FAIR Institute

---

[5] David Perera. "SEVEN BASIC CYBERSECURITY MEASURES AS REVEALED BY WISDOM OF THE CROWD." http://www.isalliance.org/seven-basic-cybersecurity-measures-as-revealed-by-wisdom-of-the-crowd/