FEDERAL DETERMINATION OF INDUSTRY BEST PRACTICES

In the Matter of	)	
	)	
NIST; Developing a Framework to	)	Request for Information
Improve Critical Infrastructure	)	
Cybersecurity	)	
Docket Number: 130208119-3119-01	)	

Prepared for the

Cyber Consortium
by
The Center for Regulatory Effectiveness
Multinational Legal Services, PLLC
1601 Connecticut Avenue, NW
Washington, DC 20009
202.265.2383
www.TheCRE.com

April 2013

Center for Regulatory Effectiveness/Multinational Legal Services, PLLC

FEDERAL DETERMINATION OF INDUSTRY BEST PRACTICES

Executive Summary

The Center for Regulatory Effectiveness' (CRE's) comments on the Cybersecurity Framework focus on a single crucial issue:

- Establishing a process for federal determination of what constitutes an Industry Best Practice.

Two components which need to be included in the Framework's process for determining Industry Best Practices are:

1. **Administrative Appeals Process**. NIST needs to establish an administrative process which allows organizations, if needed, to seek and obtain correction of decisions on determining Industry Best Practices.

2. **Conformity Self-Certification**. The Framework needs to include a process by which each critical infrastructure company can determine how best to verify their conformity with Industry Best Practices in lieu of expensive and burdensome third-party certification.

Executive Order 13636 emphasized the importance of the Cybersecurity Framework incorporating industry best practices "to the fullest extent possible...." In order for the Administration's aspirations for the use of Industry Best Practices to be realized, adherence to the following Five Principles which are based on the "Good Government" laws should guide NIST's development of the determination process:

1. **Diversity**. The process should recognize the diversity of cybersecurity Best Practices;

2. **Affordability**. The process for individual companies for determining whether their use of a Best Practice is Framework-compliant should be minimally burdensome;

3. **Reciprocity**. Critical infrastructure cyber-defense measures undertaken at the behest of any federal, state or tribal agency or the European Union should be determined to be an Industry Best Practice for purposes of the Framework;

4. **Clarity**. The best practices determination process needs to clearly define the boundaries of an infrastructure company's responsibilities regarding the facilities to which the best practices are applied; and

5. **Recognition**. The process should culminate, within a specified timeframe, in clear government-wide recognition of a company's voluntary adoption of the Framework.

ESTABLISHING FEDERAL DETERMINATION OF INDUSTRY BEST PRACTICES

President Obama's Executive Order 13636 "Improving Critical Infrastructure Cybersecurity" emphasized that NIST is to incorporate into the Cybersecurity Framework "industry best practices" as well as voluntary consensus standards, "to the fullest extent possible."

NIST is not the only agency directed by the President to support use of industry best practices to protect critical infrastructure. Presidential Policy Directive 21 (PPD-21) "Critical Infrastructure Security and Resilience" directed the State Department, in coordination with other agencies, to engage in international outreach "to facilitate the overall exchange of best practices and lessons learned for promoting the security and resilience of critical infrastructure on which the Nation depends."

Similarly, PPD-21 ordered the Federal Communications Commission (FCC) to work with other agencies in developing and implementing "best practices promoting the security and resilience of critical communications infrastructure on which the Nation depends."

Achieving the President's goals for use of Industry Best Practices will require that NIST develop a process that critical infrastructure companies can use to obtain federal recognition as Framework-compliant for best practices that they are already using.

What Is An Industry Best Practice?

The Executive Order calls for reliance on best practices without defining the term. The EO's lack of a definition for best practices needs to be viewed in light of GAO's recent finding that

> *As we reported in December 2011, DHS and other agencies with responsibilities for specific critical infrastructure sectors have not yet identified cybersecurity guidance applicable to or widely used in each of the sectors.*[1]

Moreover, it is not clear that whether a given example of widely used cybersecurity guidance would be accepted as a best practice under the Framework.

Thus, NIST is in the unenviable position of being directed to ensure maximum possible use of industry best practices without possessing either:

- A definition of Industry Best Practices; or

[1] GAO, Testimony Before the Committee on Commerce, Science, and Transportation and the Committee on Homeland Security and Governmental Affairs, U.S. Senate, Statement of Gregory C. Wilshusen, March 7, 2013, "CYBERSECURITY: A Better Defined and Implemented National Strategy Is Needed to Address Persistent Challenges," p. 15.

- A federal compilation of industry best practices.

Although calls for lists of "guidelines, best practices, and tools" used in the cyber defense of critical infrastructure can produce useful information, such lists cannot take the place of a NIST process for determining whether or not to accept various private sector practices as constituting Industry Best Practices meeting specified cyber defense needs under the Framework.

- The Framework should establish the processes to ensure it is living document responsive to the needs of industry and a rapidly changing threat landscape.

Consistent with a process-driven Framework, CRE provides in these comments a set of principles, based on the "Good Government" laws,[2] to guide NIST's development of a process for accepting (or rejecting) proposed best practices. CRE also provides examples of two components, an appeals process and a low-burden conformity verification process, that need to be part of the Framework's best practices acceptance process.

The Five Principles which should be embodied in the Cybersecurity Framework's process for accepting Industry Best Practices are:

Principle 1: Diversity

Industry best practices span a wide range of document types in addition to consensus standards including:

- Market-Driven Consortia (MDC) standards, aka industry standards developed through non-consensus processes; and

- Practices identified through best practices studies.

Although the consensus standards development process offers many benefits, it is also a lengthy and painstaking process. Consensus standards, thus, will often not be able to respond to evolving security needs in the face of the rapidly changing technological and threat landscape. Consistent with OMB Circular A-119, NIST will need to expand their concept of Industry Best Practices beyond consensus standards to embrace other proven corporate approaches to cyber defense.

With respect to consortia standards, a CRE white paper[3] on federal standards policies explained that MDCs "are associations of organizations which develop technical standards without necessarily adhering to ANSI requirements for openness and consensus."

---

[2] http://www.thecre.com/pdf/20110530_Governors_of_the_Regulatory_State.pdf

[3] CRE, "Market-Driven Consortia: Implications for the FCC's Cable Access Proceeding," available at http://www.thecre.com/pdf/whitepaper.pdf.

The CRE paper also explains that OMB Circular A-119

> *explicitly states that there is no federal preference between consensus and non-consensus standards that are developed in the private sector. Therefore, MDC non-consensus standards are accorded equal treatment to consensus standards in matters of regulation and procurement by the Circular.*[4]

Thus, under the OMB Circular, which EO 13636 directs NIST adhere to, industry standards developed through a non-consensus process are accorded equal status with standards developed through a consensus process.

CRE's white paper on federal policies regarding consensus and non-consensus standards has been widely cited by standards authorities, including the European Commission, and in a paper written by NIST and IEEE officials.[5]

It is important for the Framework to recognize, however, that the types of industry best practices recognized by Circular A-119 go well beyond MDC standards. As A-119 explains,

> *this policy allows agencies to select a non-consensus standard developed in the private sector as a means of establishing testing methods in a regulation and to choose among commercial-off-the-shelf products....*[6]

Thus, products as well as processes are recognized by A-119 as potentially eligible for federal use in standards applications even if they are developed through a non-consensus process.

As CRE has demonstrated, in certain cases it is the way a product is used that constitutes a Best Practice. For example, the CRE paper "Federal Cybersecurity Best Practices Study: Information Security Continuous Monitoring" analyzed the continuous monitoring practices using off-the-shelf software tools and identified a set of Best Practices.[7]

---

[4] Ibid., p. 21.

[5] See references to CRE paper in "Beyond Consortia, Beyond Standardisation? New Case Material and Policy Threads – Final Report for the European Commission," http://ec.europa.eu/enterprise/newsroom/cf/_getdocument.cfm?doc_id=4565, "Government Activity to Increase Benefits from the Global Standards System" http://ieeexplore.ieee.org/xpl/articleDetails.jsp?reload=true&arnumber=968568&contentType=Conference+Publications and "Consortium problem redefined: Negotiating 'democracy' in the actor network on standardization," http://www.tbm.tudelft.nl//fileadmin/Faculteit/TBM/Over_de_Faculteit/Afdelingen/Afdeling_Infrastructure_Systems_and_Services/Sectie_Informatie_en_Communicatie_Technologie/medewerkers/tineke_egeydi/publications/doc/Consortia_Egyedi_JITSR.pdf.

[6] OMB, CIRCULAR NO. A-119 Revised, Sec. 6(g). [Emphasis added]

[7] http://www.federalnewsradio.com/494/2606114/Continuous-monitoring-requires-strong-leadership-and-software

Although the study focused on a given federal organization's response using a specific software package, the study's Best Practice Principles and its Lessons Learned are absolutely brand neutral and organization neutral.

- Best practices can be identified through third-party analyses as well through a consensus or non-consensus standards development process.

The Framework will also need to recognize that not all best practices are American and may be foreign and/or multinational. EO 13636 cited Executive Order 13609, "Promoting International Regulatory Cooperation" and PPD-21 explicitly recognized the international nature of best practices when it called on the State Department to help facilitate the "exchange of best practices and lessons learned...."

It is important to note that the White House, through the Office of Management and Budget's (OMB's) Office of Information and Regulatory Affairs (OIRA) and the Office of the United States Trade Representative (USTR), has underway international regulatory harmonization talks including the EU-US High Level Regulatory Cooperation Forum and the Transatlantic Trade and Investment Partnership (TTIP). NIST should closely coordinate its Framework development process with EU regulation of cybersecurity through OMB/OIRA.

With respect to acceptance of international standards:

1. Agencies that enforce privacy and security commitments on private sector entities have accepted that non-U.S. federal government standards are appropriate to drive a response and commitment from a security standpoint. For example, the Federal Trade Commission (FTC) recognizes that companies use the ISO 27000 suite of information security as the framework for developing "best practices" for a company's information security program.[8]

2. Although diverse standards should be recognized, the NIST SP 800-53 standards[9] are widely recognized as key security controls and their adoption through a process that aligns with business and private sector processes should be encouraged. One possible option would be for the Framework to include a process for crosswalking between the SP 800-53 and ISO 27002 controls.

In summary, the Diversity Principle means that:

- Industry Best Practices encompass domestic, foreign and multinational non-consensus standards, off-the-shelf-products, and practices identified through third-party studies.

---

[8] See, http://www.27000.org/

[9] See, http://www.thecre.com/fisma/?p=1026

Principle 2: Affordability

The starting point for any discussion of the Affordability of cybersecurity controls needs to be recognition that the basis of the need for security controls in the private sector is different and economically separate from how the approach is addressed in the public sector. Thus, while NIST's Risk Management Framework (RMF)[10] is fundamental to understanding the federal government's approach to cyber risk management, it was not developed with meeting industry needs as its organizing principle.

CRE recommends that the Enterprise Risk Management (ERM)[11] be the basis of recognizing the appropriate structure and practices for the Framework rather than the RMF.

CRE is on the record explaining that cost-effectiveness is the prerequisite for cybersecurity regulation,

> *Cost effectiveness needs to be designed into any plans for critical infrastructure cyberdefense for two reasons. First, if regulations affecting much of the economy are not cost-effective, the regulatory structure will not have lasting viability and will not boost industrial security irrespective of legal requirements. Second, a discussion of cost effectiveness inherently encompasses a review of several issues that are fundamental to any rational regulatory scheme starting which, what is meant by effective cybersecurity?*[12]

Cost control and cost effectiveness are emphasized in the regulatory review Executive Orders which are cited in the cybersecurity EO. Of particular note, EO 12866 and EO 13563 both highlight the importance of agencies taking into account the "costs of cumulative regulations."

There are two types of cyber defense costs which need to be considered within the context of the RFI. Specifically,

- The costs of an infrastructure company obtaining the products/services needed to comply with the Framework's requirements; and

- The costs of a company having their already deployed cyber defense solutions being verified as complying with various specified aspects of the Framework's requirements.

These comments will focus primarily on the latter type of cost. It is essential for overall cost effectiveness that companies be able to leverage, to the greatest extent possible, their existing cyber defense practices, products and services.

---

[10] See, http://csrc.nist.gov/groups/SMA/fisma/framework.html

[11] See, http://en.wikipedia.org/wiki/Enterprise_risk_management

[12] See, http://www.thecre.com/oira/?p=1033.

Thus, the process for individual companies to obtain federal recognition of their use of a company-specific tailored adaptions of Best Practices, individually and/or as part of a suite cybersecurity practices, should be as minimally burdensome as possible.

Similarly, companies need to be able to revise and update their cybersecurity practices without triggering burdensome Framework requirements. The Framework needs to encourage, not penalize, critical infrastructure companies that upgrade their cyber defense practices.

In summary, the Affordability Principle means that:

- The process for a company to have their cybersecurity best practices accepted as complying with the Framework needs to be non-burdensome.

Principle 3: Reciprocity

Close enforcement of the "good government" laws[13] which "regulate the regulators" is essential for avoiding needless regulatory conflicts, wasted resources and the associated harms to security. Enforcement by OMB of the good government laws is particularly important given the EO 16363's directive that:

> *If current regulatory requirements are deemed to be insufficient, within 90 days of publication of the final Framework, agencies identified in subsection (a) of this section shall propose prioritized, risk-based, efficient, and coordinated actions, consistent with Executive Order 12866 of September 30, 1993 (Regulatory Planning and Review), Executive Order 13563 of January 18, 2011 (Improving Regulation and Regulatory Review), and Executive Order 13609 of May 1, 2012 (Promoting International Regulatory Cooperation), to mitigate cyber risk.*

In short, any cyber defense regulatory/quasi-regulatory action put forth by an agency needs to objectively and substantively demonstrate that:

1. The regulatory action fills an unmet need not addressed by any other mechanism; and

2. The action does not conflict with any existing regulatory requirements.

Moreover, OMB should give strong consideration to revising/amending Circular A-130 "Management of Federal Information Resources" to clarify their long-standing and ample authority to review the cyber security-related information disseminations of regulatory and non-regulatory agencies.

---

[13] http://www.thecre.com/pdf/20110530_Governors_of_the_Regulatory_State.pdf

- OMB, using their authorities under Circular A-130, should require *all* agencies to conduct formal impact analyses on their cyber security-related documents including regulations, frameworks, and implementation/guidance-type documents. Agencies should request public comments on their draft impact analyses and revise them as appropriate.

The cybersecurity Executive Order recognizes that there is the danger that compliance with the Framework could lead to companies being faced with duplicative and/or conflicting cyber-defense requirements. Specifically, EO 13636, citing the President's Executive Orders on regulatory review, calls on owners/operators of critical infrastructure, within two years of the Framework being finalized, to

> *report to OMB on any critical infrastructure subject to ineffective, conflicting, or excessively burdensome cybersecurity requirements.*

Executive Order 12866, which is explicitly reaffirmed in EO 13563:

1. Directs agencies to avoid regulatory and policy conflicts with other agencies; and

2. Directs the Office of Management and Budget's (OMB's) Office of Information and Regulatory Affairs (OIRA) to ensure:

> *that decisions made by one agency do not conflict with the policies or actions taken or planned by another agency.*

EO 12866 also requires that agencies avoid duplicative and/or conflicting regulations:

> *Each agency shall avoid regulations that are inconsistent, incompatible, or duplicative with its other regulations or those of other Federal agencies.*

Given that it is far more expensive, burdensome and harmful to American competitiveness to fix problems after they occur than to prevent them in the first place, it is incumbent on NIST to take steps in developing the Framework to minimize the possibility of the Framework's requirements conflicting with and/or being redundant to the regulatory and guidance critical infrastructure measures of other agencies.

One of the key policies for NIST to adopt to avoid needless conflict in the Cybersecurity Framework is through the Framework's process for determining acceptance of Industry Best Practices.

Specifically, the Framework's process for determining Industry Best Practices should recognize any relevant cyber-defense practice that a critical infrastructure company takes at the formal or informal request of:

- Any federal agency;

- Any State/local regulatory authority;

- Any tribal government; and/or

- The European Union (EU) or the national government of an EU member state.

Simply stated, corporate compliance with any federal/state/tribal or European Union cyber-defense measure to protect critical infrastructure should not trigger non-compliance with any requirement of the Framework.

Similarly, a critical infrastructure company's compliance with the Framework, should not result in any agency taking any action against an infrastructure company for non-compliance with a conflicting/ duplicative cybersecurity requirement.

NIST should work with DHS and OIRA to resolve any potential interagency cyber-defense conflicts before they occur.

- Interagency/Intergovernmental Coordination is Essential. The Framework will not achieve much needed infrastructure protection if compliance means that companies are left to sort out conflicting governmental cyber-defense demands and are faced with increased costs.

In summary, the Reciprocity Principle means that:

- NIST and all other agencies working on cybersecurity-related guidance for industry should conduct formal impact analyses and provide the results in draft for public comment;

- Compliance with the Framework should not create any conflicting and/or duplicative cyber-defense requirements for critical infrastructure companies;

- Compliance with the Framework should not create any conflicting and/or duplicative cyber-defense requirements for critical infrastructure companies; and

- NIST should work with DHS and OIRA to ensure that the Framework does not create conflicts with the regulations, guidance and formal or informal policies of any agency or the EU.

The CFATS Example

Pursuant to statute, DHS has established a Chemical Facility Anti-Terrorism Standards (CFATS) program including an "interim final rule that imposes comprehensive federal security regulations for high-risk chemical facilities."

The DHS CFATS "Risk-Based Performance Standards Guidance" includes a Risk-Based Performance Standard for Cyber (RBPS 8) as well as many non-cyber RBPSs.

Any company which is compliant with the CFATS Cyber standard should be automatically credited as being compliant with the Framework.

Similarly, DHS needs to coordinate with NIST and not revise the CFATS Cyber requirements while Framework development and adoption is underway.

If compliance with both the DHS/CFATS Cyber requirements and the Framework imposes new burdens beyond those already in place, the programs would endanger the ability of chemical facilities to participate in the voluntary Framework.

Principle 4: Clarity

The Framework needs to provide clarity regarding the boundaries of the critical infrastructure to which Industry Best Practices are applied. Clarity on the facility boundaries for which a critical infrastructure owner is responsible under the Framework is needed in light of a critical infrastructure company:

- Owning/operating non-critical infrastructure;
- Using critical infrastructure that is shared/leased/owned by or with a third-party; and/or
- Using cyber-defense products and services that are provided by contractors and third-party vendors.

For example, in event of a hypothetical industrial control system that was manufactured by company 1, operated by company 2 on behalf of critical infrastructure company 3, and was supplied as part of a shared services package by value added integrator/services company 4, which company is responsible for applying any relevant cyber-defense Industry Best Practices to the industrial control system?

It should be noted that DHS is pioneering, in the federal space, provision of continuous monitoring services to federal agencies through the use of contractors. The Department's goal is for government agencies and defense contractors to be able to buy the security service off a federal contract.[14] What is not clear is where responsibility would rest under the Framework for a critical infrastructure analog of DHS model if the monitoring service were determined to be a best practice. Could a critical infrastructure owner incur some type of liability if there were a flaw in their best practice because of an issue with work performed/not-performed by a vendor, co-owner or contractor/sub-contractor?

Clarity in infrastructure responsibility boundaries is a concern under Data Quality Act (DQA)[15] as well as the Framework. The "objectivity" component of quality has been defined on a government-wide basis by OMB to include the disseminated information being "presented in an accurate, clear, complete, and unbiased manner, and as a matter of substance, is accurate, reliable, and unbiased."

The Cybersecurity Framework has the potential to be significantly burdensome and damage American economic competitiveness if it is not developed and implemented correctly. In order for the Framework to secure its crucial cyber protection goals, the burdens imposed on critical infrastructure businesses need to be minimized, consistent with Principles and procedures set forth in Executive Orders 12866 and 13563.

A basic element of any federal effort to minimize burden and speed Framework compliance is providing clarity and certainty to regarding cyber-defense responsibilities to the owners of critical infrastructure.

---

[14] See, http://www.thecre.com/fisma/?p=1768.

[15] See, http://thecre.com/quality/index.html.

Corporate financial, legal and security planning functions all require that the businesses have a clear and detailed understanding of the Framework's responsibilities.

In summary, the Clarity Principle means that the Framework needs to provide clear boundaries defining a critical infrastructure owner's responsibilities regarding:

- Infrastructure for which the owner is responsible for deploying cyber-defenses based on Industry Best Practices or other acceptable means;
- Infrastructure which is the responsibility of a third-party due to sharing, leasing, contracting or other arrangements, and
- Infrastructure not covered by the Framework.

Principle 5: Recognition

The President's cybersecurity Executive Order calls for a carrots-and-sticks approach to encourage voluntary compliance with the Framework. Although, in absence of legislation, the range of possible government benefits that could be offered to complying companies is attenuated, the Order states,

> *The Secretary shall coordinate establishment of a set of incentives designed to promote participation in the Program.*

With respect to sticks, the Order directs that

> *Sector-Specific Agencies shall report annually to the President, through the Secretary, on the extent to which owners and operators notified under section 9 of this order are participating in the Program.*

The Framework's process for determining Industry Best Practices should culminate, within a specified timeframe, in clear and definitive government-wide recognition of a company's voluntary adoption of the Framework.

When a company has complied with the Framework, they should be able to take advantage of the comprehensive set of benefits offered by all agencies. Moreover, Framework-compliant companies should also be automatically eligible for any additional benefits that become available for Framework compliance, including benefits made possible through Executive Branch and/or through Congressional action.

Similarly, Framework-compliant companies should be excluded from any reporting or other actions designed to spur companies to voluntarily adhere to the Framework's cyber-defense program.

In summary, the Recognition Principle means that the Framework's process for determining Industry Best Practices and other standards culminates in clear government-wide recognition of a company's voluntary adoption of the Framework certifying that the complying company is:

- Eligible to receive all benefits/incentives for compliance; and is
- Exempt from any negative measure for non-compliance.

Component 1: Administrative Appeals Process

In any accept/not-accept process, mistakes will inevitably be made. So as to minimize the burden on businesses of implementing the Framework, there needs to be an administrative process allowing critical infrastructure companies to appeal any rejections of applications to have their cyber-defense practices accepted as Industry Best Practices for the purpose of complying with specified elements of the Framework.

The ability of company's to seek and obtain speedy redress of any errors in acceptance of Industry Best Practices will be important for company's needing to minimize the burden of voluntary compliance with the Framework. Given that the Framework is a new and highly ambitious program, the possibility of initial glitches is substantial. Although glitches cannot always be prevented, NIST does have the opportunity to ensure that errant decisions are rectified as soon as possible by establishing an administrative appeals process. There are three attributes which should be included as part of the process:

- The appeals process is handled by officials who were not involved in the original decision;
- The process includes a date-certain for agency action; and
- Any negative sanctions/reporting for non-compliance with the Framework would be suspended while the appeal is underway.

The administrative appeals process that OMB established for the DQA provides a model of an effective, low-burden appeals process. The process set by OMB and operated by agencies under OMB's supervision is described in OMB's government-wide Guidelines for Ensuring and Maximizing the Quality, Objectivity, Utility, and Integrity of Information Disseminated by Federal Agencies.[16] It should be noted that even though the Cybersecurity Framework is a voluntary/non-regulatory program, NIST's information disseminations, including the Framework itself, are subject to the DQA.

In summary, NIST needs to establish an Administrative Appeals Process. The appeals process should:

[16] See, p. 8459, http://www.whitehouse.gov/sites/default/files/omb/assets/omb/fedreg/reproducible2.pdf

- Allow companies to seek and obtain correction of any errant agency decisions on whether to accept a given example of an Industry Best Practice; and

- Exempt the appellant from any non-compliance reporting as long as the appeal is underway.

Component 2: Conformity Self-Certification

Once it has been determined that a given cyber-defense practice constitutes an Industry Best Practice for purposes of Framework compliance, the next step is for company's to be able to verify that they are utilizing the Best Practice. NIST's RFI states,

> *It is anticipated that the Framework will: (i) include consideration of sustainable approaches for assessing conformity to identified standards and guidelines; (ii) assist in the selection and development of an optimal conformity assessment approach; and (iii) facilitate the implementation of selected approach(es) that could cover technology varying in scope from individual devices or components to large-scale organizational operations.*

"Sustainable approaches" to conformity assessment mean that they have to be minimally burdensome. Any requirement for intrusive, burdensome third-party auditing/verification procedures could well doom the Framework, as important as it is, because costs would be driven too high.

The conformity assessment process also needs to take into account that companies may use varying combinations of a wide range of Industry Best Practices and other accepted cyber-defense compliance procedures. Companies need to be able to obtain approval for their entire package of compliance procedures. If critical infrastructure companies are faced with hiring a bewildering and expensive array of third-party auditors and assessment organizations and/or be responsible for completing/revising redundant sets of government forms, the program won't work. Businesses need to be able to have a simple means of demonstrating their compliance with the Framework's requirements.

Thus, a sustainable approach to Framework conformity assessment would be a combination of:

- Self-assessment;

- Recordkeeping; and

- Certification to NIST that the company is in compliance with the specified Framework provisions using accepted Industry Best Practices or other accepted means of compliance such as consensus standards.

In summary, NIST needs to establish a Conformity Self-Certification process that allows:

- Companies to demonstrate Framework compliance without the need for third-party auditing/ assessment organizations.

Recommendations

- The Framework should include a minimally burdensome process, with a built-in appeals process, for determining which Industry Best Practices are Framework-compliant. Framework compliance verification should be through conformity self-certification.

- NIST should coordinate with OIRA and DHS to prevent conflict between existing CFATS Cyber requirements the Framework and to ensure that the CFATS Cyber requirements are not revised while the Framework development and adoption process is underway.

- OMB should:

  - Review agency actions taken under the Framework and EO 13636 to ensure that they comply with the Good Government laws; and

  - Require under Circular A-130 that NIST and all other agencies developing cyber security-related regulations and guidance documents conduct formal impact analyses of their planed actions and provide them in draft for public comment.