National Institute of Standards and Technology

Cybersecurity Framework

Request for Information

February 22, 2016

EY

Building a better
working world

EY
Building a better
workin world

Ernst & Young, LLP
1101 New York Avenue, NW
Washington DC 20005

Tel: +1 202 327 6000
Fax: +1 202 327 6200
www.ey.com

February 22, 2016

Diane Honeycutt
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899

Dear Ms. Honeycutt,

Ernst & Young, LLP (EY) is delighted to have the opportunity to respond to your request for information (RFI) supporting the Cybersecurity Framework (Framework) revision. Our answers to your questions are based on extensive experience in implementing the Framework internally, in addition to helping our public and private clients manage risk by engaging the appropriate people, processes and technology capabilities.

Cybersecurity risk management demands adaptable, scalable, and practical approaches to the prevention, detection, delay, and remediation of breaches faced by enterprises of all sizes. EY commends the National Institute of Standards and Technology (NIST) on its continued work on the Framework, which represents a significant step toward broadly applicable cybersecurity guidance for critical infrastructure organizations and others that seek to improve their cybersecurity policies, practices, and procedures. The Framework's structure and content, particularly their reliance on well-known cybersecurity guidelines, present a baseline for organizations to develop and assess cybersecurity risk management as needed for their business objectives.

EY applauds NIST's grassroots effort to develop and revise the Framework by hosting regional workshops and meeting with stakeholders to solicit feedback. Posting Framework drafts and stakeholder comments for public review also exemplifies NIST's transparent process.

Sincerely,

Ernst & Young LLP

1. **Describe your organization and its interest in the Framework.**

   Ernst & Young, LLP (EY) is a global leader in assurance, tax, transaction, and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders.

   EY is a leader in providing cybersecurity advisory services, and has been recognized by numerous industry analysts for its work in this area. Our Cybersecurity practice helps clients identify and address the risks that impact their business strategies and growth agendas. We leverage industry-leading standards, including the Framework, in our service delivery.

   EY's purpose is to build a better working world, and our interest in supporting revisions to the Framework stems from this purpose. We recognize that strong, foundational standards that are able to adapt to changes in technology, threats and markets help companies improve risk management and respond to breaches.

2. **Indicate whether you are responding as a Framework user/non-user, subject matter expert, or whether you represent multiple organizations that are or are not using the Framework.**

   EY is a Framework user with respect to our own internal operations, and in our capacity as an advisor, we leverage the Framework in delivering our services to clients.

3. **If your organization uses the Framework, how do you use it? (e.g., internal management and communications, vendor management, C-suite communication).**

   Our client-serving practitioners use the Framework as an enabler and guide for designing and implementing sustainable cybersecurity risk management programs. Below are two examples of how we have leveraged the Framework to help clients:

   Client example #1: Health Care Provider

   EY assisted a national health care provider in implementing the Framework. The client wanted to identify a security control framework and perform a Service Organization Control (SOC) 2 assessment for their security controls. The client operates in a regulated environment with multiple standards and requirements, and the Framework was a natural choice with its ability to reference numerous controls, regulations, and guidelines.

EY also used the Framework to map common controls between NIST and SOC2 Trust Services Principles (TSPs), creating common terminology and correlation between the SOC2 requirements and NIST controls implemented by the client.

Client example #2: Financial Institution

EY assisted a global financial institution in using the Framework to conduct a gap analysis and identify improvement opportunities. The client had selected the Framework as the cornerstone for process risk and control mapping. EY supported their decision because of the Framework's completeness and applicability in the client environment.

4. **What has been your organization's experience utilizing specific portions of the Framework (e.g., Core, Profile, Implementation Tiers, Privacy Methodology)?**

   Our primary Framework experience has been centered on use of the Core. The Core is flexible, complements many existing security programs, and allows clients of varying maturities and from diverse sectors to align their security requirements to a common set of controls. Our clients appreciate the Core's flexibility, which allows them to assess risks and apply controls based on their environment. Given the various sectors in which our clients operate, the Framework effectively correlates to many regulatory requirements, enabling each client to align their various needs to a common set of controls.

5. **What portions of the Framework are most useful?**

   The most useful portion of the Framework is the Core's common language/risk management approach, which has allowed: (1) our firm to implement standard processes throughout EY's global offices, and (2) our engagement teams to assist our clients in implementing similar initiatives. Specifically, the Core simplifies cross-mapping to NIST SP 800-53 (R4) controls, the Risk Management Framework, COBIT, and ISO 270xx frameworks.

6. **What portions of the Framework are least useful?**

   The portions of the Framework that have been least useful include:

   - The sections in the Framework should be re-ordered to improve effectiveness. The current sequence is the Core, Implementation Tiers, and Profiles. While the Core's Identify function addresses many of the larger policy-related concerns, the Framework does not drive organizations to recognize their risks in the context of their business first (e.g., current-state profile). The profile activity should be followed by the Core to allow for appropriate selection policies that set the context for how a company wants to manage its business risks. Once risk tolerance is defined and policies are established, the standards developed can address how the policies can be added consistently and the controls can be implemented.

- Stakeholders possess different frames of reference that should be considered within the Framework, such as:
    - Board – Objectives of controls related to operations, compliance, and reporting
    - Senior Management – Process focus around COSO components of internal control and outcomes of processes to meet the objectives
    - IT Management – Results of processes to meet defined objectives
    - IT Personnel – Asset-focused (protect, detect, respond, and recover)

7. **Has your organization's use of the Framework been limited in any way? If so, what is limiting your use of the Framework (e.g., sector circumstance, organizational factors, Framework features, lack of awareness)?**

   The Framework's tiering structure has caused confusion as the Framework requires additional guidance to assess an organization's implementation tiers.

   Many organizations view the Framework as a *compliance* framework. Clients have been asking EY to utilize the Framework to measure compliance for "a potential Framework audit." Verbiage regarding how the Framework is not a compliance-focused framework should be emphasized.

   Finally, since many organizations currently align themselves with the NIST Risk Management Framework (RMF, 800-53 (R4)), clear guidelines should be provided to help these users concurrently implement the RMF and Framework.

8. **To what extent do you believe the Framework has helped reduce your cybersecurity risk? Please cite the metrics you use to track such reductions, if any.**

   Using the Framework internally (and at our clients) to rationalize monitoring controls has enhanced EY's overall understanding of cybersecurity programs. The Framework aligns with business objectives by building flexible, repeatable processes and procedures to identify, assess, and manage cyber risk.

   EY utilizes a variety of metrics to track reductions by referencing numerous federal cybersecurity guidelines, most notably the *White House Cybersecurity Strategy and Implementation Plan (CSIP),* 2015.

9. **What steps should be taken to "prevent duplication of regulatory processes and prevent conflict with or superseding of regulatory requirements, mandatory standards, and related processes" as required by the Cybersecurity Enhancement Act of 2014?**

   NIST should request feedback annually from all industries regarding the regulatory requirements and mandated standards (e.g., North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP), Health Insurance Portability and Accountability Act (HIPAA), and Payment Card Industry (PCI)) they face from a cybersecurity perspective. With this feedback, NIST should develop, maintain, and publish a mapping that provides a holistic view of all US cybersecurity regulatory requirements and mandated standards across industry sectors. This will prevent duplication between requirements and standards.

10. **Should the Framework be updated? Why or why not?**

    The Framework would be more useful to organizations if it were updated. We believe that supplemental guidance on the application of the implementation tiers and development of target profiles should be added. The Framework provides a good overview of the importance of creating a target profile and takes into consideration acceptable risk thresholds that meet an organization's business goals. However, it lacks a step-by-step approach to develop these profiles based on the Core. The Framework also needs to allow reasonable scaling of procedures based on risk evaluation.

    In addition, many clients have not implemented the Framework because it is not clear how they would assess practices to develop a tier-level rating. By closing the gap between the implementation tiers and the developed practices, clients will be in a better position to understand their current posture and identify areas where they may want to adjust their approach.

    Finally, for several controls within the subcategory field, ambiguity regarding the controls' intent needs to be removed. Some high-level controls have been perceived as duplicative in nature, causing clients to remove them. This weakens the Framework. Each subcategory should be mapped to ISO, COBIT, and 800-53 (R4) controls.

11. **What portions of the Framework (if any) should be changed or removed? What elements (if any) should be added to the Framework? Please be as specific as possible.**

    The Framework should incorporate additional security controls and definitions from the NIST Special Publication 800-Series, such as:

    - 800-82, *Guide to Industrial Control Systems (ICS) Security*, 2011

- 800-171, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*, 2015

EY also recommends greater incorporation of international standards. As an example, the European Union has different standards regarding data privacy, and NIST should make an effort to cross-map to these standards. This would encourage more trans-Atlantic adoption of the Framework.

EY routinely leverages these guidelines as reference tools to further support client communications regarding capability maturity, help build programs to identify and protect sensitive/critical assets, and improve alignment of risk management programs to business goals. We feel that incorporating these principles and terms would add to and further develop a compendium of common language tools and industry cooperation.

EY further recommends and emphasizes that additional mapping to both NIST guidelines and international references would provide a solid foundation to prevent duplication or misrepresentation of common control alignment.

12. Are there additions, updates or changes to the Framework's references to cybersecurity standards, guidelines, and practices that should be considered for the update to the Framework?

The current Framework is primarily focused on monitoring preventive controls. We recommend that additional attention be given to monitoring activities to detect potential breaches, as well as the follow-up activities necessary to investigate, respond, and if necessary, repel attacks.

The Framework's implementation tier methodology should include priority framework assignments, similar to how 800-53 (R4) identifies control priorities for each control family. This would assist industry practitioners with developing strategies to assess the current-state and implement controls in the Core to adjust an organization's overall approach to risk. The order of priorities should be parallel to 800-53 (R4) P0, P1, P2, and P3 to maintain consistency with process flows and language.

The profile activity could be improved by leveraging content and concepts from existing NIST guideline references (e.g., NIST SP 800-30, 800-37, 800-39). Currently, the Framework references only 800-39, but does not offer guidance on how to effectively conduct a risk assessment. The Framework could further enhance this effort to create a common language by providing clear guidance on conducting risk assessment activities, not just managing information security risk.

The Framework could be improved by providing guidance on how an organization should appropriately use the practices to develop a tier-level rating. This would enable those implementing the Framework to better understand their current approach to cybersecurity risk and identify areas where they may want to make adjustments.

The overall market acceptance of the Framework could be further enhanced by integrating it with an existing enterprise-wide framework such as COSO, which has been widely adopted by the markplace.

Finally, as noted previously, while the Framework was never intended to be utilized as a compliance framework, various stakeholders in the marketplace (e.g., boards, senior management, business partners, investors, regulators) are looking for a comprehensive baseline against which to measure the adequacy of a company's risk management program. Given this growing market demand, we recommend that consideration be given to developing companion materials that could be used for this purpose.

13. **Are there approaches undertaken by organizations – including those documented in sector-wide implementation guides – that could help other sectors or organizations if they were incorporated into the Framework?**

Approaches and best practices should be identified based on leading individuals, sector groups, industry regulators, and information sharing analysis centers (ISACs). For example, a defense contractor could provide guidance on how to protect systems that are involved in the engineering of International Traffic in Arms Regulations (ITAR) products. Subcontracting is a common occurrence in the defense industry and in public agencies, and a subcontractor could implement the Framework based on defense contractor best practices.

The Framework is also aligned to sector regulatory standards, such as the NERC CIP and HIPAA.

14. **Should developments made in the nine areas identified by NIST in its Framework-related "Roadmap" be used to inform any updates to the Framework? If so, how?**

We recommend that the developments identified in the *NIST Roadmap for Improving Critical Infrastructure Cybersecurity* (2014) be incorporated into Framework revisions, specifically "Federal Agency Cybersecurity Alignment." We also recommend that NIST integrate the Federal Information Security Modernization Act (FISMA) controls identified in 800-53 (R4) with the Framework.

15. **What is the best way to update the Framework while minimizing disruption for those currently using the Framework?**

The method NIST used to engage with the public during the development of the Framework in 2012 set the standard for future iterations of Framework updates. We hope NIST repeats this effort by issuing public drafts, seeking comments, and hosting stakeholder workshops for future iterations of the Framework. This transparent method, which has been effectively used by COSO and similar organizations, will improve the adoption of changes and minimize disruption for those currently using the Framework.

16. Has information that has been shared by NIST or others affected your use of the Framework? If so, please describe briefly what those resources are and what the effect has been on your use of the Framework.

NIST has made a major effort to share information with the public and EY has used this information to enhance the Framework's implementation internally and with clients. The following additional legislation and work products have also encouraged Framework use:

- *The NIST Roadmap for Improving Critical Infrastructure Cybersecurity* (2014) examines NIST's next steps with the Framework and identifies key areas of development, alignment, and collaboration. Areas of improvement include authentication; automated indicator sharing; conformity assessment; cybersecurity workforce; federal agency cybersecurity alignment; international aspects, impacts and alignment; supply chain risk management; and technical privacy standards.
  - Through these identified areas of improvement, EY has incorporated related 800-53 (R4) and ISO 270xx controls into its own cybersecurity methodologies.
- *The Cybersecurity Information Sharing Act (CISA)* (2015) is designed to "… improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats."
  - The law allows the sharing of cyber threat information between the US government and private industry; which directly complements the Framework, specifically PR.IP-8, "Effectiveness of protection technologies is shared with appropriate parties."
- *The Critical Infrastructure Cyber Community (C^3) Voluntary Program* (2014) is an innovative public-private partnership led by the US Department of Homeland Security (DHS). C^3 helps align critical infrastructure owners and operators with existing resources to assist in using the Framework to manage their cyber risks.
  - The C^3 Voluntary Program encourages feedback from stakeholder organizations about their experience using C^3 Voluntary Program resources to implement the Framework. Feedback about the Framework is also shared with NIST to help guide the development of the next version of the Framework and similar efforts.

- *The DHS Cybersecurity Evaluation Tool (CSET)* (2011) is a no-cost, voluntary technical assessment that provides a snapshot of an organization's cybersecurity posture.
  - CSET helps asset owners and operators assess cybersecurity strengths and weaknesses within their environments. It can also be used to assess traditional IT infrastructure to complement Framework gap analyses.
- *The Cyber Resilience Review (CRR)* (2009, revised 2014) is another DHS assessment method. It is a voluntary examination of operational resilience and cybersecurity practices offered at no cost to the operators of critical infrastructure and state, local, tribal, and territorial governments.
  - The Framework's profile system complements the CRR's operational resilience by identifying gaps.

While the CSET and CRR predate the Framework, the inherent principles and recommended practices within the CSET and CRR align closely with the central tenets of the Framework.

Additionally, federal and state regulatory guidance regarding financial services is being developed around the Framework.

17. What, if anything, is inhibiting the sharing of best practices?

Notwithstanding the passage of CISA, the sharing of best practices and cybersecurity information may remain a challenge. Although some liability and privacy issues when sharing information may be allayed, the underlying lack of resources and time for many entities has not changed. Businesses, especially those that are small and medium-sized, often have limited in-house IT resources and even fewer resources focused on cybersecurity. In such a constrained environment, companies may be challenged to prioritize voluntary information sharing.

18. What steps could the US government take to increase sharing of best practices?

We recommend that the US government (specifically NIST) make a concerted effort to work with the following information sharing programs:

- *National Cybersecurity and Communications Integration Center (NCCIC)* serves as the DHS hub of information sharing activities to increase awareness of vulnerabilities, incidents, and mitigations.
- Within the NCCIC, the *Cyber Information Sharing and Collaboration Program (CISCP)* is DHS's flagship program for public-private information sharing and complements ongoing DHS information sharing efforts. In

CISCP, DHS and participating companies share information about cyber threats, incidents, and vulnerabilities.

- *Enhanced Cybersecurity Services (ECS)* is an intrusion prevention capability that helps US-based companies protect their computer systems against unauthorized access, exploitation, and data exfiltration. ECS works by sharing sensitive and classified cyber threat information with accredited Commercial Service Providers (CSPs).
- *Sector-Specific Agencies (SSAs)* leverage existing relationships with critical infrastructure entities to expand and improve ECS. SSAs are also responsible for sharing best practices in their respective sectors.
- *Information Sharing and Analysis Centers (ISACs)* are non-profit, member-driven organizations formed by critical infrastructure owners and operators to share information between government and industry.
- *Information Sharing and Analysis Organizations (ISAOs)* are similar to ISACs — they gather, analyze, and disseminate cyber threat information — but they are not sector-affiliated. Executive Order 13691, *Promoting Private Sector Cybersecurity Information Sharing* (2015), calls for ISAO development to improve cybersecurity information sharing between the private sector and government, and enhance collaboration and information sharing within the private sector.

19. What kind of program would help increase the likelihood that organizations would share information about their experiences, or the depth and breadth of information sharing (e.g., peer-recognition, trade association, consortia, federal agency)?

The standards outlined in CISA (2015) encourage organizations to share information among themselves and with the federal government.

Highlights include:

- The Director of National Intelligence and the Departments of Homeland Security, Defense, and Justice are required to develop procedures to share cybersecurity threat information with private entities, non-federal government agencies, state and local governments, the public, and entities under threats.
- Liability protections are provided to entities that voluntarily share and receive cyber threat indicators/defensive measures with other entities or the government.
- A sharing process must be developed within DHS for the federal government to: (1) receive indicators and defensive measures that are

shared by any entity, and (2) ensure that appropriate federal entities receive shared indicators in an automated, real-time manner.

- The law limits how the government may use shared information to certain cybersecurity purposes and responses to imminent threats or serious threats to a minor.
- DHS must also deploy a system to: (1) detect cybersecurity risks in network traffic transiting or traveling to or from an agency information system, and (2) prevent or modify such traffic to remove cybersecurity risks.
- The DHS Secretary may: (1) issue emergency directives to agencies in response to a substantial information security threat, vulnerability, or incident; or (2) authorize intrusion detection and prevention capabilities to secure agency information systems in the case of an imminent threat.
- The National Cybersecurity and Communications Integration Center (NCCIC) must establish a process for statewide interoperability coordinators to report risks or incidents involving networks used by emergency response providers.
- The Department of Health and Human Services (HHS) must convene a task force to: (1) plan a single system for the federal government to share intelligence regarding cybersecurity threats to the health care industry, and (2) recommend protections for networked medical devices and electronic health records.

20. What should be the private sector's involvement in the future governance of the Framework?

NIST should establish an advisory council composed of domestic and international public and private organizations, including consulting/advisory firms. The role of the advisory council would be to contribute to the Framework's continued development, review feedback, and make decisions on future enhancements. NIST should also provide additional avenues (e.g., open workshops) to encourage real-time Framework feedback, where suggestions and improvements can be captured for consideration for future updates. NIST should also encourage private individuals with strong, validated security and risk management credentials to participate and to contribute to improving the Framework's maturity.

21. Should NIST consider transitioning some or even all of the Framework's coordination to another organization?

We believe such a transition, if it were to occur in any measure, would be significant and warrant careful consideration and socialization.

22. **If so, what might be transitioned (e.g., all, Core, Profile, Implementation Tiers, Informative References, methodologies)?**

    If a transition were to occur to an appropriate entity, we would recommend that all of the Framework be transitioned. The Framework's strength is in the cohesion and interplay of its parts. Transitioning only a few parts would likely weaken the Framework, in our view.

23. **If so, to what kind of organization (e.g., not-for-profit, for-profit; US organization, multinational organization) could it be transitioned, and could it be self-sustaining?**

    Should such a transition occur, we recommend that the selected organization have adequate credibility, experience, knowledge, objectivity, and resources to ensure the Framework's continued evolution with the benefit of connectivity with and input from NIST.

24. **How might any potential transition affect those currently using the Framework? In the event of a transition, what steps might be taken to minimize or prevent disruption for those currently using the Framework?**

    In the event of a transition, NIST could develop a detailed transition plan, including frequent and clear communications on key players, milestones, and timeline, to facilitate the transition. Further, the organization that receives the Framework will need to make a continuous effort to ensure that the Framework controls mapped to 800-53 (R4) remained accurate.

25. **What factors should be used to evaluate whether the transition partner (or partners) has the capacity to work closely and effectively with domestic and international organizations and governments, in light of the importance of aligning cybersecurity standards, guidelines, and practices within the United States and globally?**

    NIST should consider the following factors when evaluating a transition partner(s):

    - Objectivity
    - Resources (knowledge and experience, personnel availability, finances)
    - Reputation in managing similar frameworks, offering training, and encouraging ongoing maturity/evolution
    - Respect in domestic and global public and private sectors

EY | Assurance | Tax | Transactions | Advisory

About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, or other professional advice. Please refer to your advisors for specific advice.

ey.com