ISACA®
Trust in, and value from, information systems

3701 Algonquin Road, Suite 1010
Rolling Meadows, Illinois 60008-3105, USA
Web Site: *www.isaca.org*

Telephone: +1.847.253.1545
Facsimile: +1.847.253.1443
E-mail: *info@isaca.org*

10 October 2014

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

Re: Experience with the Framework for Improving Critical Infrastructure Cybersecurity ("Framework")

Dear Ms. Honeycutt,

I am the international president of ISACA, a worldwide independent professional association providing thought leadership on information and information system security and assurance, enterprise governance and management of IT, and IT-related risk and compliance.

ISACA applauds the US government's steadfast commitment to cybersecurity and NIST's fortitude in creating and delivering a robust and timely framework focused on helping enterprises address and reduce cyber risk. NIST's emphasis on the importance of a framework to help align business, policy and technology risk is particularly insightful and very much needed. Additionally, ensuring the workforce has the proper skills and capabilities continues to be a critical issue for governments as they prepare to move rapidly on their strategies. ISACA shares this vision and has moved aggressively with some solutions to begin addressing this gap and stands ready to assist.

To support ISACA's response to NIST's RFI, we surveyed our US constituents who are chief information security officers (CISOs) and those who hold the Certified in Information Security Management® (CISM®) certification. ISACA received almost 800 responses. Over 75 percent of respondents were aware of the Framework and believe it has definitely helped to elevate the overall importance of cybersecurity. We are encouraged with this level of awareness, but realize more needs to be done on the use and benefit side. We are confident that over time, once the implementation rate increases, the Framework will assist in reducing risk to critical infrastructure entities and protect digital information and infrastructures from the full range of cyber threats. However, with the fast-moving and increasing number and severity of cyber incidents, further work needs to be undertaken to promote use and drive implementation to further assist organizations.

The Framework and its best practice recommendations appear broad enough to address the unique characteristics of enterprises across different market segments while still able to be tailored to specific sector needs. Although the Framework seems to offer the right degree of detail, a resource that is rightsized for small and medium enterprises, drawing on the good practices of the Framework, seems like something that could be of great value—similar to what the UK Government has done with its Cyber Essentials program.

The growing global importance of cybersecurity further necessitates good governance over IT projects and systems. Regrettably, however, the importance of governance and the role it plays in sound cybersecurity strategies and policies is often understated or not addressed at all. This must change if sound cybersecurity practices are to be integrated into business processes.

ISACA appreciates the opportunity to assist where appropriate, and has provided more detailed comments to the applicable questions in the NIST RFI. We stand ready to provide other assistance to ensure NIST and the US government's efforts are successful in supporting and growing a safe, yet reliable and robust, cybersecurity environment for enterprises, through use of the Framework for Improving Critical Infrastructure Cybersecurity.

Respectfully submitted,

Robert E Stroud, CGEIT, CRISC, International President
ISACA (*www.isaca.org*)

About ISACA

With more than 115,000 constituents in 180 countries (50,000 in the US), ISACA constituents have developed, implemented, managed and assessed security controls in leading critical infrastructure organizations and governments on a global basis. ISACA is a leading global provider of knowledge, certifications, community, advocacy and education on information and information systems security and assurance, enterprise governance and management of IT, and IT-related risk and compliance. ISACA offers the Cybersecurity Nexus™, a comprehensive set of resources for cybersecurity professionals and COBIT®, a business framework that helps enterprises govern and manage their information and technology responsibilities, particularly in the areas of security, risk, assurance and control to deliver value to the enterprise. COBIT is used within many governmental departments and regulatory bodies around the world. ISACA also participates in the development of international security and governance standards through our active global Category A liaison status with several working units of the International Organization for Standardization (ISO). Additionally, ISACA enjoys a mutual and collaborative working relationship with the European Network Information Security Agency (ENISA), who has the responsibility and dedication in the EU to preventing and addressing network security and information system failures.

Founded in 1969, the nonprofit, independent ISACA hosts international conferences, publishes the *ISACA® Journal*, and develops international IS auditing and control standards, which help its constituents ensure trust in, and value from, information systems. It also advances and attests IT skills and knowledge through the globally respected Certified Information Systems Auditor® (CISA®), Certified Information Security Manager® (CISM®), Certified in the Governance of Enterprise IT® (CGEIT®) and Certified in Risk and Information Systems Control™ (CRISC™) designations.

Section 1: Questions Regarding Current Awareness of the Cybersecurity Framework

Recognizing the critical importance of widespread voluntary usage of the Framework in order to achieve the goals of the Executive Order, and that usage initially depends upon awareness; NIST solicits information about awareness of the Framework and its intended uses among organizations.

- What is the extent of awareness of the Framework among the Nation's critical infrastructure organizations? Six months after the Framework was issued, has it gained the traction needed to be a factor in how organizations manage cyber risks in the Nation's critical infrastructure?

  In the six months since the Framework has been issued, there has been a good deal of press coverage and awareness building in the government space. To assist in the response to NIST's RFI, ISACA surveyed our US constituents who are chief information security officers (CISOs) and those who hold the Certified in Information Security Management® (CISM®) certification, to gauge their awareness and use of the Framework. ISACA received almost 800 responses. Of the respondents to the awareness and use survey, over 75 percent were aware of the Framework and believed it has helped to elevate the importance of addressing cybersecurity.

- How have organizations learned about the Framework? Outreach from NIST or another government agency, an association, participation in a NIST workshop, news media? Other source?

  Yes, ISACA has actively communicated to the association's constituents regarding the importance of the Framework as well as its development and availability. At the associations recent European Information Security and Risk Management (ISRM) held in Barcelona, where ISACA hosted the Global CyberLympics, there were attendees from over 20 countries witnessing workshops, a keynote and numerous sessions where the Framework was mentioned and discussed. Additionally, at ISACA's recent Global Leadership conference, over 300 leaders and members of the profession from nearly 80 countries around the world were provided an update of the Framework and its importance in helping manage cybersecurity risk. ISACA plans to continue this active awareness building.

- Are critical infrastructure owners and operators working with sector-specific groups, non-profits, and other organizations that support critical infrastructure to receive information and share lessons learned about the Framework?

  Yes, this is beginning to occur. Since the Framework was completed and issued, ISACA has presented several webinars on the Framework itself, how it was developed and the approaches and benefits from its use, and has provided a platform for users to share any lessons learned. ISACA has also created specific guidance for the Framework, showing how COBIT®, one of the international frameworks included in the Framework's Core component, can help with Framework implementation. In addition to the webinars, ISACA has begun to provide in-

person implementation training using the guidance publication. As this training is carried out, ISACA will be happy to share with NIST any information gathered from the association's interactions with sector-specific Information Sharing and Analysis Centers (ISACs).

- Is there general awareness that the Framework:
  - *Is intended for voluntary use?*

    Yes, it seems well understood that it is intended to be voluntary, and this is a positive outcome. NIST needs to continue to emphasize this, and at the same time ask for others to convey the need to increase overall awareness, use and integration with existing business practices and processes.

  - *Is intended as a cyber risk management tool for all levels of an organization in assessing risk and how cybersecurity factors into risk assessments?*

    This is a point that seems to be well laid out in the Framework. However, it is not known if and how the Framework is communicated inside organizations. Although the Framework states it can be used for all levels of an organization, there is likely a gap between this statement and understanding how this will be done in various organizations. ISACA stands ready to help better convey this important message.

  - *Builds on existing cybersecurity frameworks, standards, and guidelines, and other management practices related to cybersecurity?*

    Yes, there appears to be a fairly solid understanding that the Framework is built on and extends existing frameworks, standards and management practices such as COBIT®.

- What are the greatest challenges and opportunities—for NIST, the Federal government more broadly, and the private sector—to improve awareness of the Framework?

  The greatest opportunity for NIST and the federal government is to get the private sector to see the Framework as something that is relevant to the private sector and will help them better manage, govern and address overall cybersecurity risk. Much progress was made through the many workshops held during the fact-gathering and building of the Framework. Perhaps that same level of vigor and dedication could be continued with industry and professional nonprofit associations like ISACA to help carry the message about use and adoption. ISACA will continue to collaborate with NIST to position NIST speakers at ISACA events whenever possible and appropriate in order to convey the needed messages to industry about the importance and benefits of the Frameworks use and implementation.

- Given that many organizations and most sectors operate globally or rely on the interconnectedness of the global digital infrastructure, what is the level of awareness internationally of the Framework?

ISACA's interactions with its global constituents reveals a fairly healthy level of awareness of the Framework and a base level understanding of how the Framework might help them or affect interactions within other countries. Cybersecurity risks and threats are a global problem, and the more the Framework can be socialized globally, especially among governments and those agencies that deal with cyber issues, the better. ISACA is aware that NIST has made a concerted effort to engage with many governments around the world about the Framework, and the association views this as very positive. As ISACA continues to actively advocate around the world in various venues, the association stands ready and committed to assist NIST in raising global awareness of the Framework. Additionally, as ISACA engages with governments that are actively concerned and inquiring about cybersecurity, ISACA will be sure to educate them about the Framework and its value as they address their own country's needs.

- Is your organization doing any form of outreach or education on cybersecurity risk management (including the Framework)? If so, what kind of outreach and how many entities are you reaching? If not, does your organization plan to do any form of outreach or awareness on the Framework?

  Yes, to help address the growing worldwide need of addressing cybersecurity risk management, ISACA worked with chief information security officers and cybersecurity experts from leading organizations around the world to create the Cybersecurity Nexus (CSX™) initiative, which is designed to fill an unmet need for a single, central location where security professionals and their enterprises can find cybersecurity research, good practice guidance, certificates and certifications, education, mentoring and community. All CSX materials are built to provide security-related information within the larger business context. ISACA is initiating collaborative discussions with the Association of Computing Machinery (ACM) and the National Cyber Watch Center around existing cybersecurity training and personnel development programs in US colleges, to further determine how and to what degree the CSX program could be of assistance in the classroom. Additionally, ISACA has begun to reach out to its constituents about the Framework, how it can help in management of cybersecurity risk and how the issue of cybersecurity necessitates good governance over IT projects, systems and applications. As noted previously, ISACA has created webinars on the topic and implementation guidance and will continue to raise awareness of the issue.

  Since the Framework provides a risk-based approach that enables a platform for success and offers steps to increasingly improve cybersecurity maturity, and because these values closely mirror the governance and management principles that ISACA has fostered for many years, it was a natural fit for ISACA to build off the Framework's road map to develop its own Framework implementation guidance - using COBIT®, to assist organizations and governments.

- What more can and should be done to raise awareness?

ISACA believes that the creation of customized guidance on use cases and a formal method of sharing experiences and good practices around the use of the Framework would be valuable in raising awareness. Given recent discussion about the use of incentives for organizations, one possible incentive could be the enterprise's ability to promote to its stakeholders, both internal and external, its adoption and use of the Framework as tangible evidence of its adherence to good cybersecurity practices.

Section 2: Questions Regarding Experiences with the Cybersecurity Framework

NIST is seeking information on the experiences with, including but not limited to early implementation and usage of, the Framework throughout the Nation's critical infrastructure. NIST seeks information from and about organizations that have had direct experience with the Framework. Please provide information related to the following:

- Has the Framework helped organizations understand the importance of managing cyber risk?

  Yes, the Framework has helped to raise the level of awareness and importance of cybersecurity and associated risk (78 percent of the respondents to ISACA's Framework awareness and use survey indicated the Framework has elevated the topic of cybersecurity in their organization). The top five sectors represented in the survey responses were financial services, healthcare, retail manufacturing and government. Additionally organizations and governments worldwide are seeking to understand the Framework's direct applicability to their overall management of risk.

- What benefits have been realized by early experiences with the Framework?

  Some of the experiences that have been shared with ISACA include an overall increase in awareness of cybersecurity threats, better strategic alignment of security with enterprise objectives, greater support from senior management and a sense of improved overall governance of cybersecurity.

- Do organizations in some sectors require some type of sector specific guidance prior to use?

  There does appear to be a need among a subset of those who replied to ISACA's Framework awareness survey: 50 percent of respondents were looking for sector-specific guidance, but they realize there can only be one overall framework. This may indicate there is room for further explanatory guidance or use cases.

- Have organizations that are using the Framework integrated it with their broader enterprise risk management program?

  Organizations are reevaluating their cyber risk management approaches and processes since the release of the Framework. While those who say they have "implemented" the Framework remain in the minority, many organizations are reviewing their processes to see if and how well they are aligned with the Framework. While it likely is too early to tell to what degree organizations will integrate the Framework entirely into their existing enterprise risk management approach, ISACA will continue to monitor and encourage the adoption of these good practices.

- Is the Framework's approach of major components—Core, Profile, and Implementation Tiers—reasonable and helpful?

  ISACA believes NIST's approach and components are sound, and constituents have commented on the awareness and value of the Core component of the Framework. Regarding the use of profiles and implementation tiers, this is an area that likely deserves more awareness building. In the ISACA workshops and the implementation guidance, helpful direction is given on the core as well as how to use profiles and tiers for the as-is and target states.

- Section 3.0 of the Framework ("How to Use the Framework") presents a variety of ways in which organizations can use the Framework

  - Are organizations changing their cybersecurity governance as a result of the Framework?

    Yes, according to ISACA's Framework awareness survey, nearly 50 percent of those who are using the Framework reported an increased overall level of governance of cybersecurity in their organization. While more gains still need to be made, this level of focus at the governance layer is encouraging.

  - Are organizations using the Framework to communicate information about their cybersecurity risk management programs—including the effectiveness of those programs—to stakeholders, including boards, investors, auditors, and insurers?

    Yes, ISACA's Framework awareness survey found that 82 percent of those who are using the Framework are using it to communicate the importance of cybersecurity risk to internal stakeholders.

  - Are organizations using the Framework to specifically express cybersecurity requirements to their partners, suppliers, and other third parties?

    Yes, but organizations appear to be less mature when using the Framework to communicate and deal with their external stakeholders. Of those who are using the Framework, 56 percent reported embracing it for use with their partners, suppliers and other third parties.

- Have organizations developed practices to assist in use of the Framework?

  Yes, as mentioned earlier in this RFI response, ISACA has provided several webinars on the Framework, how it was developed and how to go about using and implementing it. The association has also gone a step further and created implementation guidance on how to use the Framework and how COBIT®, one of the international sources of good guidance and practices included in the Framework Core component, can help with implementation and promote good governance. Where appropriate and feasible, ISACA will continue to offer

webinars and in-person implementation training, helping enterprises with the use and adoption of the Framework.