recommendations for public companies and their independent auditors to address fraudulent financial reporting, this framework is instructive in the cybersecurity best practices context as well.

Intel's primary means of measuring risk is through a number of risk assessment methodologies, as described in an earlier answer. These methodologies, and the processes Intel has in place supporting them, allow for precise tailoring of the assessment to the type, scale, and scope of the issue for the most effective assessment possible.

Knowing where to look for risks, however, is equally important. Intel employs a number of methods to help identify areas of greatest concern for further examination. One of the most effective means of risk identification in the Intel environment is to carefully study and monitor threats. Cyber threat is the most dynamic variable in the TVC (threat-vulnerability-consequence) risk equation. By constantly monitoring and assessing cyber threat, Intel can quickly identify both emerging trends and areas needing more detailed risk assessments.

Intel has instituted this capability in a number of ongoing programs, such as one that monitors the malware threat environment. This program regularly draws on the expertise of subject matter experts throughout the company to report on changes in the external malware domain, and has developed a sophisticated model for charting the maturity of each threat, which in turn indicates its threat level. The Threat Agent/Analysis Group (TAG) program conducts a similar function, but with the focus on the human activities that create and drive threat. Both programs focus on providing up-to-date threat information and early warnings to affected business units. The Threat Management program deals with malware that has been found internally, analyzing it to relay critical data to internal controls and mitigation teams. The Security Center of Excellence (SeCoE) incorporates information from these programs with its own product information to similarly monitor threats to Intel products.

Intel also conducts regular threat landscape briefings for all cybersecurity stakeholders. Along with the programs already mentioned, other related programs such as Investigations, Physical Security, Security Operations Centers, and others, contribute to the briefings so that the Intel cybersecurity community has inclusive, current and actionable information to use in their own security efforts and assessments.

8. <u>What are the current regulatory and regulatory reporting requirements in the United States (e.g. local, state, national, and other) for organizations relating to cybersecurity?</u>

It is difficult to provide an exhaustive list of regulatory reporting requirements related to cybersecurity. Currently, the most direct impact tends to be from state data breach notification laws although a wide range of sectorial laws dealing with privacy and data security may apply as well, such as those dealing with the protection of health care and financial information. While not all data breach situations are triggered by a cyber intrusion, a breach to Intel's IT infrastructure may trigger an obligation to notify both impacted individuals and state Attorneys General or consumer protection agencies. At the federal level, our reporting is typically voluntary. We may also voluntarily report to federal law enforcement or the Dept. of Homeland Security based on the nature of the incident or threat encountered.

The recent 2013 National Defense Authorization Act Section 941 adds a security breach notification reporting requirement for DoD Contractors who access classified documents. While not directly applicable to Intel, it will likely impact Intel's subsidiary entities.

9. What organizational critical assets are interdependent upon other critical physical and information infrastructures, including telecommunications, energy, financial services, water, and transportation sectors?

Like most large design and manufacturing companies, Intel has a significant dependence on the critical infrastructure surrounding and supporting its world-wide facilities. Intel relies on the dependable operation of almost every critical sector, supporting its 90,000 person organization in more than sixty countries around the world.

10. What performance goals do organizations adopt to ensure their ability to provide essential services while managing cybersecurity risk?

Intel is a data-driven company and uses a wide range of metrics depending on business process and organizational level to set performance goals related to security and risk management. Within the IT cybersecurity organization there is an agreed upon set of metrics measured in a dashboard and reviewed by the management team regularly. Some examples of security domains in which Intel tracks detailed metrics include:

- Infrastructure
- Applications Security
- Data Protection
- Identity and Access Management
- Policy, Training and Awareness
- Security Enclaves Controls
- Investigations

More specific metrics may be tracked by an individual team. The areas listed above are a roll-up of the more specific metrics. Also, Intel has regular threat briefings where specific groups report threat-related metrics out to a broad security audience internally.

11. If your organization is required to report to more than one regulatory body, what information does your organization report and what has been your organization's reporting experience?

Intel, as a multinational company, has a wide range of regulatory reporting obligations ranging from financial to product safety to occupational health. In the cybersecurity area, our reporting obligations typically are triggered by specific events, usually a data breach with some exfiltration. Depending upon the scope of the incident—whether it involves residents of multiple states, what is the exact nature of the information breached, etc.—the reporting may be very complex. Inconsistencies in varying state regulations exacerbate the difficulty in regulatory reporting because of different response periods, governmental organizations and standards. In each instance, Intel must evaluate each breach on the specific facts and determine the actual nature of the breach, how to seal the breach and whether a reporting obligation is triggered. Communications to impacted individuals must be drafted and in many cases state regulators such as the relevant attorneys general or consumer protection agencies must be informed. Having a common set of regulatory reporting obligations for a data breach would significantly simplify the analysis of a given incident and more easily allow for the provision of timely responses.

We may also voluntarily report to federal law enforcement or the Dept. of Homeland Security based on the nature of the incident or threat encountered.

Under the 2013 National Defense Authorization Act Section 941, DoD Contractors dealing with classified material must report intrusions and provide governmental access to corporate systems in

instances of security breach. While this does not currently apply to Intel, when the implementing regulations are complete, they will likely impact Intel's subsidiary entities. Until the regulations are finalized, Intel cannot speculate on the actual impact. However, while the logic of a reporting obligation related to classified materials makes sense, we do have some concerns regarding the extent of the reporting and potential for government employees to access our confidential IT infrastructure. And, while this may not apply directly to Intel, if we provide IT services to subsidiary organizations that have access to classified material, these obligations may also potentially impact Intel.

12. What role(s) do or should national/international standards and organizations that develop national/international standards play in critical infrastructure cybersecurity conformity assessment?

International standards organizations are critical to ensuring global interoperability and harmonization. Efforts to develop standards and conformity assessment requirements for cybersecurity and critical infrastructure should be pursued within global standards bodies that allow for the broadest input and ultimately the greatest adoption. Conformity assessment is generally understood to refer to a process used to demonstrate that a product or service meets specified requirements. The specification of the requirements is primarily the work of global standards organizations while assessing conformance is the work of separate organizations authorized to certify, inspect and test products against the specifications. When conformance assessment is deemed necessary, independent, private laboratories usually conduct it. The purpose of this arrangement is to separate the duty of developing the specification from evaluating against it in order to increase the probability of achieving an objective evaluation. For example, ISO develops security standards such as ISO 27001 but is not involved in certification to the standards it develops. For an entity to certify to an ISO standard, they much employ a private lab to conduct the evaluation. It is important to note that there are standards for how to appropriately conduct conformity assessment that are based on global consensus and are globally deployed.

Intel believes the separation between standards development and conducting conformity assessment (testing, certification etc.) is extremely important from the perspectives of both security and innovation. From a security perspective, it is important to companies that their IP is protected and that the integrity of the product is preserved. The company will always be in the best place to determine the appropriate way to manage such evaluations. From an innovation perspective, this separation is important because it allows the conformance assessment industry to move at a pace more closely tied to the pace that industry designs and develops products. While it is true that conformity assessment often adds time delays and additional costs to product deployments, additional requirements on where, how and when such evaluations were made would further exacerbate those issues. Many standards bodies are working on issues that will impact critical infrastructure such as cloud computing security, identity management and security assurance. To the extent that compliance with these standards is required for critical infrastructure owners and operators, independent labs should carry out these assessments.

Section 2: Use of Frameworks, Standards, Guidelines and Best Practices

As set forth in the Executive Order, the Framework will consist of standards, guidelines, and/or best practices that promote the protection of information and information systems supporting organizational missions and business functions.

NIST seeks comments on the applicability of existing publications to address cybersecurity needs, including, but not limited to the documents developed by: international standards organizations; U.S. Government Agencies and organizations; State regulators or Public Utility Commissions; Industry and industry associations; other Governments, and non-profits and other non-government organizations.

NIST is seeking information on the current usage of these existing approaches throughout industry, the robustness and applicability of these frameworks and standards, and what would encourage their increased usage. Please provide information related to the following:

1. What additional approaches already exist?

   Dozens of well-defined and carefully developed standards exist to cover multiple aspects of cybersecurity and adjacent fields, from cryptographic primitives to IT governance. Today, most technology standards include elements of security and privacy. There are numerous broadly defined approaches, such as Common Criteria, included as an international standard in JTC1 (Joint Technical Committee of ISO and IEC) and ISO/IEC 27000 series, focusing on process and security management. These standards and approaches are designed to work across diverse fields. At the same time, there are industry-specific standards and best practices that work within the bounds of an industry utilizing a vertical model. The Payment Card Industry (PCI) standard developed for the financial industry, standardized numerical identification for prescription drug packages, 3GPP's LTE security standards, or Aerospace Quality Management Standard (AS9100 based on IS0 9901) belong to this group.

   It would be inadvisable and unrealistic to recommend one approach for different contexts of use. However, some level of generalization for best practices that are broadly and globally applicable is useful because of the diverse but connected technological environment in existence today. A group of experts could study best practices and standards developed for specific industry segments and use contexts to assess if the knowledge already developed in other areas, such as aerospace, computer hardware or software, healthcare, smart cards, RFID, or financial services could fill the gaps in other cybersecurity standards and best practices.

2. Which of these approaches apply across sectors?

   Intel can only speak to the practices used internally; other organizations such as trade associations or public-private partnerships can provide more useful information for this question.

3. Which organizations use these approaches?

   Intel can only speak to the practices used internally; other organizations such as trade associations or public-private partnerships can provide more useful information for this question.

4. What, if any, are the limitations of using such approaches?

   Standards are necessarily adapted to specific technology contexts. However, even within a body of standards associated with the same technology, a lack of coordination and interoperability may be a problem, especially when subcomponents have been adopted to fill the gaps in areas where

standardization and the development of best practices have been slow to mature. Large-scale efforts to ensure cohesiveness and interoperability illustrate this need. By way of example, a few years ago, a global RFID interoperability forum for standards (GRIFS) was created in Europe. This was driven by the great incongruence of existing RFID standards, including in security, with dozens of ISO/EIC standards and standards developed by other groups. In another example, the Continua Alliance was created to promote interoperability and cooperation in healthcare-related standards, including their security and privacy aspects. The NIST Framework could include an effort in to bring more coherence and interoperability to standards and best practices associated with cybersecurity.

5. What, if any, modifications could make these approaches more useful?

Specifications and standards, even when developed in a narrowly focused standards consortium, must evolve to keep pace with technology innovation. For example, the Trusted Computing Group extended the Trusted Platform Module from PC-only to other computing environments as those new environments developed. JTC1's Subcommittee (SC) 27 is now working on privacy, a standardization topic that was non-existent 10 years ago. Because the standards development process is typically lengthy, the framework should capture adjustment processes and best practices associated with the technology evolution during standards development. This can help technologists working on cybersecurity standards to build in awareness of technology evolution and ensure that the new or updated standards not only reflect the latest state of technology, but also have embedded controls for continued evolution based on the technology innovations.

Successful adoption of standards has multiple dependencies going beyond technology aspects of the standards. This is especially true in security and cybersecurity. Broad adoption of technologically viable standards depends on factors such as usability or the economic impacts of their deployment. All too frequently, these aspects are overlooked during the standards development processes. Doing so creates the risk that the resulting approaches lack viable business or economic models necessary for their successful introduction. The cybersecurity framework discussed here needs to include considerations of these non-technological aspects. It will also benefit from the development of efficient collaboration models involving all the stakeholders. A forum bridging diverse stakeholders together would be an instrumental component of building such a framework. Another part of the framework could include a series of testbeds for new standards to test them in near real world conditions and create adaptations prior to broad deployment, in order to ensure seamless and swift adoption of new standards approaches and best practices.

6. How- do these approaches take into account sector-specific needs?

Trade associations, sector coordinating councils, and sector affinity groups are best situated to provide meaningful insights in response to this question.

7. When using an existing framework, should there be a related sector-specific standards development process or voluntary program?

Successful sector-specific efforts in cybersecurity and related fields already exist. Some of these efforts, e.g., in the financial sector or aerospace, were mentioned above. Sector-based approaches are necessary because the operational environments and contexts vary significantly across sectors. The need to align context-specific building blocks to create a coherent end-to-end system of best practices and standards in cybersecurity is strongly recognized in the technology community and needs to be associated with sector-specific efforts. As the Framework is developed, NIST should consider including a mechanism to bring experts together in a cross-sector setting in order to

identify gaps, exchange knowledge, reuse approaches that have been proven viable, ensuing a broader understanding of cybersecurity needs is taken into consideration as context-specific standards and best practices are developed.

8. What can the role of sector-specific agencies and related sector coordinating councils be in developing and promoting the use of these approaches?

Intel supports the industry engagement in the public-private partnership model as outlined in the National Infrastructure Protection Plan (NIPP). Intel recommends direct engagement with the sector coordinating councils to develop and promote the use of these approaches.

9. What other outreach efforts would be helpful?

As noted elsewhere in this document, Intel believes some governments might misunderstand the role of the Framework and see its development as a sign that regulatory action is both necessary and warranted. To avoid this scenario, the U.S. government should conduct extensive outreach to educate other governments about the purpose and role of the framework and encourage similar approached based on voluntary, global standards.

Additionally, there are numerous cybersecurity affinity groups already in existence. NIST should engage broadly to understand that the Framework should be built upon existing voluntary and consensus based cybersecurity standards and best practices, as called for by the EO. There is no shortage of such existing standards and best practices. One of the goals of the Framework should be to spread foundational security standards and best practices out more broadly across the CI/KR community.

Section 3: Specific Industry Practices

In addition to the approaches above, NIST is interested in identifying core practices that are broadly applicable across sectors and throughout industry.

NIST is interested in information on the adoption of the following practices as they pertain to critical infrastructure components:

- *Separation of business from operational systems;*
- *Use of encryption and key management;*
- *Identification and authorization of users accessing systems;*
- *Asset identification and management;*
- *Monitoring and incident detection tools and capabilities;*
- *Incident handling policies and procedures;*
- *Mission/system resiliency practices; Security engineering practices;*
- *Privacy and civil liberties protection*

1. Are these practices widely used throughout critical infrastructure and industry?

   Intel can only speak to practices used internally; other organizations such as trade associations or public-private partnerships can provide more useful information for this question.

2. How do these practices relate to existing international standards and practices?

   All of these practices are currently embodied in the work of a variety of global standards bodies. An extensive gap analysis should be completed before developing additional standards so as not to create unnecessary duplication. In some cases, concepts like how to separate business from operational systems are embodied in general IT management standards and are only one of many good practices recommended in a given standard, e.g., ISO 27001. In other cases, there are specific standards initiatives on a given practice. For example, in ISO/IEC SC27 alone there are 46 unique standards efforts involving the use of encryption and key management, but other organizations such as the Trusted Computing Group and 3GPP also work on encryption-related topics.

   Of the practices listed, there appears to be less directed activity in the areas of asset management and privacy and civil liberties and these should be evaluated for completeness. However, Intel stresses the importance of conducting a comprehensive gap analysis before launching new standards initiatives, even if the subject appears under-represented. For example, there is a wealth of extremely important and useful work on privacy practices that is widely understood, accepted and deployed, e.g., the Fair Information Practice Principles, OECD guidelines, APEC privacy principles.

3. Which of these practices do commenters see as being the most critical for the secure operation of critical infrastructure? —AND—
4. Are some of these practices not applicable for business or mission needs within particular sectors?

   In answer to both questions 3 and 4, all of the practices listed are essential to an effective cybersecurity defense, and are equally critical. They are important not only independently, but must be well-integrated to establish effective defense-in-depth security. While it may be possible to de-emphasize one or prioritize one over the others, that prioritization could properly be done only after a careful and comprehensive analysis of the organization's or sector's unique risk profile.