5. Which of these practices pose the most significant implementation challenge?

All of the practices listed will have significant challenges to implementation, but Intel believes these three will pose the greatest challenges:

Identification and authorization of users accessing systems—Intel and many other companies and organizations have devoted considerable resources to improving identity and access management systems. Despite this effort, serious technical and policy challenges remain in developing an automated system that can effectively identify a user and grant appropriate access while delivering a positive user experience and respecting the user's privacy rights and civil liberties.

Privacy and civil liberties—New technologies present new challenges and opportunities in the privacy context. Optimizing for both the new and enhanced user experiences and protecting the users' rights is the challenge on which technology companies must focus, especially when there are different interpretations of how that should best be accomplished. The framework NIST develops must comprehend privacy and civil rights not just from a U.S. standpoint but rather from a global viewpoint, based on internationally recognized Fair Information Practice Principles (FIPPS), that contemplates the multinational operations of many companies.

Monitoring and incident detection tools and capabilities—The traditional corporate security perimeter continues to dissolve as an increasing number of intelligent devices become part of the corporate environment through BYOD (Bring Your Own Device) programs and the growing "internet of things." These dramatic changes are creating increasing difficulty in building sensor and telemetry functions capable of detecting, validating, and reporting potential incidents in a timely manner. Even with the progress of big data tools, the amount of sensor data to process in real time could become overwhelming.

6. How are standards or guidelines utilized by organizations in the implementation of these practices?

Generally, Intel tries to align itself to existing standards and best practices for implementing practices such as these. However, multiple factors often lead Intel to create new, internal standards as they are adapted directly to the Intel environment and business needs. For example, existing standards often lack applicability because they are too academic in nature or too generic or impractical to be applied verbatim in the real world. Intel will, however, use components of those standards as the backbone to our internal process. Modifications are made as dictated by internal business needs. Additionally, as described in other answers here, Intel regularly examines the rapidly evolving threat landscape and changes its own security posture to respond to that evolution. This includes modifying standards and best practices as needed, sometimes as often as several times in one year. A good example of where rapid changes have had significant impact is in Intel's BYOD (Bring Your Own Device) program. New devices, new use cases, and new threats are emerging very rapidly in this arena so our standards must also change quickly along with them.

In many cases, however, there are few relevant existing standards because Intel is an early adopter—or even the creator—of leading edge technologies or functions. In those cases, new ones must be created. For example, during Intel's initial implementation of cloud services, a survey of best practices was performed and discovered there were few standards or guidelines for cloud services at that time. Intel developed its own guidelines, and as industry standards evolve we work to both influence and align with emerging standards. In another case, Intel recognized early the need to ensure the security of its outsource vendors such as third-party organizations contracted to perform functions such as payroll, health insurance administration, etc. Again no applicable standards existed, so Intel created its own standards which it has used successfully to align our outsource vendors to uniform security practices.

A third example of collaborative, industry-led dissemination of best practices is Intel's Threat Agent Analysis methods and the supporting Threat Agent Library (TAL). The TAL was created internally to address the lack of consistency in describing the threat posed by human actors. When we discovered others in industry were struggling with the same issue, the TAL and its techniques were published externally for sharing. Subsequently, the TAL has been incorporated as a best practice or standard in various systems such as the IT Sector Risk Assessment [Baseline] by the IT-SCC and Dept. of Homeland Security partnership, and is listed as a Best Practice by international standards organizations such as ENISA. Intel encourages all users of the freely-available TAL to adapt, modify, and most importantly, to evolve it to meet their own industry requirements and the changing demands of their own unique environment.

As demonstrated, Intel has a culture and history of creating and sharing flexible, agile standards and guidelines to support business needs. Often, as a creator or early adopter of technology, Intel will develop initial best practices, and then as there is broader industry adoption, Intel will share its best practices in white papers or briefings, or by participating in external communities developing standards. Intel's objective is always to create a flexible framework that supports and improves business capabilities of our company and of the ecosystem, and allows for responsive evolution of that framework.

7. Do organizations have a methodology in place for the proper allocation of business resources to invest in, create, and maintain IT standards?

Yes. The Intel security community has a culture of sharing and promoting best practices and standards. Support for maintenance of existing standards is typically discussed as part of our internal planning processes. A Subject Matter Expert (SME) or manager may identify standards or best practices effort of interest and will work within the planning process to allocate appropriate resources. Intel may identify gaps in a specific area of external best practice where Intel may have unique expertise. Resources are then allocated to draft a best practice whitepaper and champion it through an external channel or organization. Alternatively Intel may choose to publish as an Intel branded whitepaper. Intel routinely publishes best practices and whitepaper through portals such as IT@Intel (http://www.intel.com/content/www/us/en/it-management/intel-it/intel-it-best-practices.html). Intel is involved in a variety of external IT-related affinity groups and actively participates in these group efforts to update, create and maintain IT standards. One example is Intel's involvement in the FIRST (Forum for Incident Response and Security Teams) Vendor SIG where inputs into updates to the Common Vulnerability Scoring Standard (CVSS) are gathered.

As noted above, Intel has fostered a strong culture of support for external community engagement. Intel management has strongly encouraged continuing cybersecurity education and certification. This culture of community involvement has led to formal and informal best practices sharing and standards influencing efforts.

Intel IT is often an early adopter of technology solutions, and often in such circumstances relevant best practices and standards do not yet exist. When this occurs, Intel IT's cybersecurity-related controls may be foundational and informative to other enterprises, both through formal and informal sharing. For example, Intel IT has been an early adopter of BYOD (Bring Your Own Device) solutions which has resulted in several external whitepapers and sharing of best practices with other companies.

In addition, as a technology developer and manufacturer, Intel Product teams are involved in many IT-related standards efforts. These efforts are tracked through a formal Standards Committee process.

8. Do organizations have a formal escalation process to address cybersecurity risks that suddenly increase in severity?

Yes. Intel's normal incident response processes comprehend rapid changes in the cybersecurity risks and threat landscape. Within the IT incident response process there is a triage process which allows for a risk management-based escalation in response to changes in threat severity. In cases where escalation is necessary, escalations rise to the appropriate level of management and may trigger corporate emergency operations, as appropriate. Similar processes are mirrored in our Product Security Incident Response Team, which also has an escalation path to senior business unit and corporate management. Intel has dedicated Threat Management and Threat Intelligence teams chartered to monitor and respond to changes in the threat landscape. Regular threat briefings occur with security and management stakeholders to increase awareness of the emerging threat landscape and to adjust our internal controls to address such changes. Intel has an internal cross-organizational team that maintains our Threat Agent Library and monitors for actor-based threats, and is a resource for internal risk management and security personnel. Intel tests and exercises its enterprise and product security escalation and response processes and makes continuous improvement adjustments as a result.

9. What risks to privacy and civil liberties do commenters perceive in the application of these practices?

Intel supports the adoption of appropriate practices with regard to critical infrastructure, based on the level of risk and sensitivity of the components to be protected. Care should be taken to minimize the potential impact to privacy and civil liberties, as the overzealous application of some of the proposed practices may potentially lead to the unwarranted collection of personal information or monitoring of individuals.

10. What are the international implications of this framework on your global business or in policymaking in other countries?

This framework will likely become a global reference for cybersecurity policymaking. Intel operates in over 60 countries and has customers using our products all over the world. It is important that the U.S. set a positive example regarding the essential role that global standards play for both industry and government. This framework presents an important opportunity to develop a product that many other countries can replicate and use in their policy environments. The U.S. could encourage global acceptance of this framework by seeking comments and support from other countries during its development. This adoption would be beneficial by creating consistent and cohesive approaches across those geographies as well as a commitment to the global standardization process.

Intel also recognizes there is a risk in developing this framework. 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 approaches based on voluntary, global standards.

11. How should any risks to privacy and civil liberties be managed?

Intel privacy and security policies support the privacy rights of individuals, as well as the legitimate need for the company to protect itself and its assets from harm. While Intel has discrete

functional groups supporting threat intelligence, cybersecurity and privacy, these organizations share common management and report to the CSO. This close relationship allows review and resolution of potential conflicts that may arise.

Any legislative or regulatory approach taken by the government should encourage adoption of practices in compliance with Fair Information Practice Principles (FIPPS), including adequate notice to impacted individuals and consideration of "proportionality" in developing a cybersecurity framework. Proportionality is the balancing of the intended activity with the potential impact on an individual's privacy rights and related civil liberties. For example, policymakers are currently considering various approaches to enabling more effective sharing of cyber threat information between government and industry, in a manner that balances the essential need to share as much cyber threat information as quickly as possible with as many stakeholders as possible, while also optimizing for the privacy and civil liberties of citizens and the needs of businesses for strong liability protections to incentivize such sharing. In this and all contexts, including under the Framework, the question should always be asked whether there is a less intrusive manner to implement a specific regulatory cybersecurity solution that will minimize the impact on an individual's rights.

12. In addition to the practices noted above, are there other core practices that should be considered for inclusion in the framework?

- *Outsource and Vendor Management*—Few companies are entirely autonomous these days. Most are highly matrixed, with relationships with various vendors who manage corporate assets and employee personal information, such as payroll and health insurance information. A company must have assurance that such vendors have security at least equal to their own to ensure their assets are not at elevated risk.
- *Fostering a Strong Security Culture*—Building and maintaining a strong security culture across the entire organization is essential to effective cybersecurity. Without it, even the best security technologies and polices will fail. A company serious about security will continually work to ensure every employee is engaged and trained to protect the company's assets, at every level of the company.
- *Secure Product Assurance Processes*—Given the nature of our business as a developer and manufacturer of both building block technologies and security technologies and services, Intel also has a clear cybersecurity need—and powerful business incentive—to build trusted products. Intel has been working for years to build trust in technology into our internal policies and procedures, by examining the various elements associated with trust to ensure we take them into account as we invest in, innovate, develop and design new products and services.
- *Hardware Foundation of Trust*—Intel is investing in and innovating solutions to the difficult challenge of building trust directly into technology platforms, whether PCs, Servers, smart phones, or networking equipment. As hardware is more difficult to compromise than software, trusted hardware is the foundation upon which the global market will build trusted operating systems, applications, networks, and services.
- *Security Lifecycle Management Processes*—Intel implements security lifecycle management processes for our technology products to better address challenges posed by product complexity and platformization. To demonstrate development and manufacturing accountability, Intel is focused on security and has undertaken significant initiatives aimed at increasing security processes across the company, including establishing the Security Center of Excellence (SeCoE). One SeCoE-led initiative is "Design for Security," which is focused on building a capability in each and every engineering team to integrate security into products from the outset. A central aspect of this initiative is educating engineers to design for security and

privacy. Another example is the Intel Secure Development Lifecycle, which defines the actions, deliverables and checkpoints a project team follows to engineer in security and privacy to meet the expectations of the product and market.

Thank you again for the opportunity to provide our views on the Cybersecurity Framework. Now more than ever, we must find ways to leverage the expertise of both the federal government and the private sector to solve the important and complex problem of better securing our critical infrastructure in a way that harnesses innovation to address the cybersecurity needs of governments, businesses and citizens. We welcome the opportunity to participate in the workshops NIST will be hosting over the coming months to continue this constructive dialogue.

Best Regards,

Peter M Cleveland

Peter M. Cleveland
Vice President, Legal and Corporate Affairs
Director, Global Public Policy