Introductory Comments

While we will attempt to keep this section to a minimum, we believe it is important in a response such as this to provide some context on the respondent to promote understanding the particular interpretation and viewpoint being brought to the table.

We are a mid-sized organization providing supply chain management services, primarily in the Aerospace and Defense space, though we do have customers in other critical infrastructure sectors. Consequently, our comments are heavily influenced by three factors:

1. Being a small-to-mid size business that will be implementing/employing the Cybersecurity Framework developed through this process.
2. Experience in supplier management and the challenges of managing, coordinating, and assuring a global supply chain.
3. Our history – both as a company and individually – in the Defense sector, with its particular standards, guidelines, and requirements.

Current Risk Management Practices

NIST solicits information about how organizations assess risk; how cybersecurity factors into that risk assessment; the current usage of existing cybersecurity frameworks, standards, and guidelines; and other management practices related to cybersecurity. In addition, NIST is interested in understanding whether particular frameworks, standards, guidelines, and/or best practices are mandated by legal or regulatory requirements and the challenges organizations perceive in meeting such requirements. This will assist in NIST's goal of developing a Framework that includes and identifies common practices across sectors.

What do organizations see as the greatest challenges in improving cybersecurity practices across critical infrastructure?

“Critical infrastructure”, as defined by PPD-21, represents an incredibly broad cross-section of the national economy. Many of these sectors are regulated to various degrees, by different agencies and to different standards. The lack of unifying or universally-acceptable guidelines poses a significant challenge in improving overall cybersecurity maturity.

Another major challenge lies in the supply chains serving the primes/OEMs/principals/etc. in these sectors. Most of these organizations at the top of their respective supply chains have fairly robust cybersecurity programs in place, but the smaller organizations supporting them don’t have the capability, resources, or – in many cases – incentives to implement even basic good security hygiene. Currently, the “best case” scenarios involve those where cybersecurity or information risk management requirements are flowed down through contract clauses; however, because there is no common framework, these companies have to conform to differing requirements for each customer.

What do organizations see as the greatest challenges in developing a cross-sector standards-based Framework for critical infrastructure?

Each of these sectors – and the departments or agencies that oversee them – are "heavyweight" industries in their own right. Some of them (i.e., Defense) have their own information assurance and cybersecurity guidelines and processes which have been developed over years and represent substantial investment from both government and industry. We do not believe a cross-sector framework that is simply a union of these various sector-specific standards can be effective; consequently, individual sectors must be willing to adjust – or abandon – their specific standards. This will be a significant challenge, and the current wording of the Executive Order isn't strong enough to push through this hurdle.

Describe your organization's policies and procedures governing risk generally and cybersecurity risk specifically. How does senior management communicate and oversee these policies and procedures?

We utilize ISO/IEC 27001, and have an information security risk management process consistent with the standard. We can say with relative confidence that our specific policy is pretty "standard" as compared with other companies, and can offer little fresh insight to NIST or other readers in this area.

Where do organizations locate their cybersecurity risk management program/office?

Our organization splits this function between our Business Technology (BT) and Quality and Compliance (Q&C) departments. Business Technology has primary responsibility for cybersecurity policies, procedures, controls, monitoring, etc., while Q&C is ultimately accountable for the enterprise risk management function.

How do organizations define and assess risk generally and cybersecurity risk specifically?

We utilize ISO 27001, and have an information security risk management process consistent with the standard. We can say with relative confidence that our specific policy is pretty "standard" as compared with other companies, and can offer little fresh insight to NIST or other readers in this area.

To what extent is cybersecurity risk incorporated into organizations' overarching enterprise risk management?

Within our organization, cybersecurity is deeply embedded into our overall risk management. The nature of our business involves possessing and managing a large amount of our customers' and their suppliers' data, and as such the protection of that information is a very prominent part of our risk management strategy.

However, in working with small/medium suppliers, or larger suppliers who only peripherally participate in critical infrastructure sectors (i.e. suppliers whose products are leveraged in multiple industries), we frequently find that this is not the case. Many of these organizations do not have a well-developed cybersecurity awareness, culture, or program, and consequently cybersecurity does not play much role in their risk management approach.

What standards, guidelines, best practices, and tools are organizations using to understand, measure, and manage risk at the management, operational, and technical levels?

Nothing unique to offer here.

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?

There are several good resources available to address reporting requirements at the national and state level (public websites). Some sector-specific reporting requirements can be difficult to navigate.

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

Looking at our own business and the companies we work with, the answer to this is – for all intents and purposes – everything.

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

Nothing unique to offer here.

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?

We do not have regular reporting requirements to any regulatory bodies, and fortunately have not had to report any incidents or breaches to date. We are required by many of our customers to provide annual self-attestations of compliance to certain controls, and go participate in customer assessments of our cybersecurity program.

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

In terms of assessing conformity, approaches similar to those used by other international organizations (ISO, etc.) is a proven model. It is important that conformity assessments under this framework are consistent and – through an accreditation process or something similar – universally accepted.

In at least some sector-specific standards (specifically Defense, in this case), certification and accreditation (i.e., going through a conformance assessment) must be initiated by agency or contract and cannot be voluntarily initiated by an organization (except in rare cases). Additionally, because an accreditation is based on acceptable risk for a specific company/program/mission, it is not necessarily valid for other uses or customers. At this point we don't have any concrete recommendation for how this can be addressed, as different risk profiles necessitate different implementations, but would encourage the community developing this framework to tackle the issue of universally-recognized conformity assessments.

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:

What additional approaches already exist?

In the international space, ISO/IEC 27001 of course is (we believe) the most recognizable standard in this space. In the supply chain space, of particular interest at the moment are ISO/IEC 27036 (currently in draft form), and the Aerospace Industries Association (AIA) NAS9924 ("Cyber Security Baseline") was just released in the past few months.

In the government/national security space there's FISMA and NIST guidelines as well as the DoD's DIACAP and NISPOM policies/guidelines.

Although not a formal standard, we are strong advocates of the SANS Top 20 as a baseline for any organization.

Which of these approaches apply across sectors?

There are elements of all the above approaches that have applicability across all or at least most sectors.

Which organizations use these approaches?

Our organization uses ISO/IEC 27001 as our overall information security management framework. At the implementation level, we leverage the SANS Top 20 as well as a subset of the NIST 800-53 controls.

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

The limitations are really in finding the right balance between standards comprised of controls that are highly prescriptive but often place a heavy burden on organizations (especially smaller organizations) and more general standards that are highly scalable (both up and down) but as a consequence don't provide enough in the way of hard standards to give outside entities any real assurance without those entities performing an assessment or audit of their own.

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

A framework that contained elements of both approaches – prescriptive controls with quantifiable, universal definitions of conformity (or, even better, degrees of capability/maturity) as well as scalable information risk management frameworks that can be tailored to the size and business processes of individual organizations.

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

Nothing unique to offer here.

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

While we have to respect that there are fundamental differences in the needs and operating environments of these sectors, there is a deep need within the field at this point to corral the number of differing standards and programs and begin working towards a dominant design in cybersecurity. This is, of course, a daunting proposition but we must try to leverage the momentum generated by this Executive Order to drive the process forward. If we can make headway in developing a universally-applicable framework, the nature of a competitive market will take it from there.

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

The single greatest role these agencies and councils can be is promote cross-sector standards unification to the greatest extent possible. While there are undoubtedly sector-specific requirements that must be addressed by these organizations, they must take the lead in working towards a unified standard wherever possible.

What other outreach efforts would be helpful?

Nothing unique to offer here.

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.*

Are these practices widely used throughout critical infrastructure and industry?

Yes but often to different degrees and not as a holistic effort.

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

Nothing unique to offer here.

Which of these practices do commenters see as being the most critical for the secure operation of critical infrastructure?

There's no easy answer to this, as all the practices listed above are critical to the secure operation of a system. However, at a high level:

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

Are some of these practices not applicable for business or mission needs within particular sectors?

Almost any business in any sector (and, for many of these practices, individual end users) benefit from these practices. In looking at the larger ICT ecosystem, any network open for exploitation can be leveraged for large-scale distributed attacks.

Which of these practices pose the most significant implementation challenge?

Balancing monitoring and incident handling policies and procedures with privacy and civil liberties protection is a tremendous challenge, especially in multi-national organizations. Striking a balance is hard enough from a purely technical perspective, but when factoring in the privacy regulations of the international community can get practically impossible and dramatically increase the cost and complexity of monitoring and auditing. Developing robust monitoring capabilities, policies, and procedures is (relatively speaking) feasible but difficult (see below); incorporating diverse international privacy laws and PII protection requirements while trying to manage a network as a unified whole makes the issue nearly impossible. Some examples from our experiences include working within and between "safe" countries including the U.S., U.K., and Germany.

Separate from the balancing act described above, robust monitoring and incident handling requires qualified personnel who are in short supply. There are plenty of technologies and tools, but not enough people trained and qualified in their usage and interpretation to determine what an incident is or how incidents can be contained/prevented.

Encryption and key management poses a particular hurdle to smaller businesses, as the cost of entry is relatively high for these organizations. While various sectors have robust PKI platforms in place, there must be a simple and cost-effective way to extend this down the supply chain.

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

Standards help organizations mature from individual controls implemented by (typically) the Security or IT organizations and into the realm of information risk management. Without these high-level standards (i.e. ISO/IEC 27001), implementation of the above practices is more of an undirected "whack-a-mole exercise" rather than an integrated defense based on specific threats to the organization.

With that said, in many cases organizations will push hard to initially demonstrate compliance to these standards but, in the long run, treat it as a "check the box" exercise. An exception is many financial institutions, who (likely due to SOX) seem to put much more effort into long-term sustainment of their cybersecurity investments and risk management programs.

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

In our experience, most small/medium businesses do not. Many such organizations do not have a formal risk management process, and consequently building the business case for investment, creation, and maintenance of IT standards is difficult.

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

Again, in the context of small/medium businesses our experience suggests no.

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

Our business is very focused on field activities, with a large BYOD footprint. Due to the nature of our business, it is very difficult – and sometimes not permitted – for us to supply our personnel with equipment, yet we remain to various extents liable for the protection of information furnished to or generated by them.

In trying to secure equipment we do not own or control, with personal (or sometimes other companies') data, we have encountered numerous cases of potential privacy concerns and have had to scale back on our monitoring efforts to avoid risk. Some guidance on balancing the risks of

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

As a service provider to many of the critical infrastructure sectors, we would seek to be an early adopter of this framework. However, many other countries we do business in are actively developing their own standards and policies around cybersecurity, risk management, and privacy protections. Maintaining compliance with these diverse requirements is an exercise we expect to be extremely difficult.

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

Nothing unique to offer here.

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

While it doesn't quite fit into the list of "core practices" described above, we believe that the framework must address cybersecurity in the supply chain, as this is an area in desperate need of attention. Most primes in the critical infrastructure sectors (typically larger corporations) have implemented the core practices described above (at least in the A&D space); however, their products and systems are only as secure as the hundreds or thousands of suppliers downstream from them, and many of those business do not have the knowledge, resources, or motivation to proactively manage their cybersecurity risk.

At the NIST-sponsored workshop on 3 April, the DHS panel proposed the following high-level goal statement for the framework:

> *"Adoption of the framework will give the entity a high level of confidence that the essential services it provides will continue to be delivered to its critical customers in the face of most cyber incidents directly effecting the entity."*

It is the final part of that statement ("… directly effecting the entity") that concerns us here. While we certainly understand the intent from the perspective of managing liability or understanding accountability, it's also critical that organizations be mindful – and, in some cases, responsible – for the risk posture of their upstream and downstream partners.

The Supply Chain Operations Reference (SCOR) Model developed by the Supply Chain Council can be considered best practice – certainly within the Defense sector, at least, in that DOD 4140.1R (DoD Supply Chain Material Management Regulation) mandates use of the model by DoD Components. The SCOR Model is a large reference – much not relevant to this discussion – but a fundamental aspect of it states that "supply chain management" as a whole encompasses two tiers in both directions of the supply chain from the supply chain manager in question. In other words, a supply chain manager must consider everything from Delivery by a Tier 2 supplier ("supplier's supplier"), through the Source-Make-Deliver processes of a Tier 1 supplier, through their own organization, and then the Source-Make-Deliver processes of their Tier 1 customer and the Source process of Tier 2 customers ("customer's customer"). Traditionally, many standards and frameworks have left the supply chain to the very end, typically addressed through an addendum, bolt-on, or (worst case) yet another complementary standard. We strongly believe supply chain cybersecurity should be baked into this new framework.

Conclusion

Thank you for the opportunity to provide this feedback and be involved in the process. We are extremely excited about the potential for this framework and look forward to contributing in more detail as it matures. Please feel free to contact us at any time for clarification or additional information.