Specific Responses

This section provides specific answers to the numbered questions posed in the aforementioned RFI.

Question Number	Major Areas of Concern	
1	What do organizations see as the greatest challenges in improving cybersecurity practices across critical infrastructure?	We view the greatest cybersecurity challenges organizations face revolve around these areas: • Technical coverage and architectures (i.e. information, systems, and process architetures) • Keeping up with the pace of technological change • Approaching cybersecurity with tactical, as opposed to strategic, solutions. • Working with impractical methodologies that are "siloed," contain errors, and are not scalable.

2	What do organizations see as the greatest challenges in developing a cross-sector standards-based Framework for critical infrastructure?	In order for cross-sector standards to be effective, they require buy-in and communication between different stakeholders. It is natural that problems would occur due to politics, interpretation of jurisdictions, and defining territories. These issues could make it difficult to reach consensus. Additionally, different personas will require different means of communication. For example, a CISO or ISSO is more likely to require *accurate* information, whereas a Security Analyst or System Administrator is likely to require *precise* information. We also see that many existing frameworks are often written to be too idealistic and rigid (all or nothing) in their approaches. This makes implementation difficult. Finally, we see both a lack of objectivity in evaluation methods combined with the lack of actionable metrics makes progress hard to demonstrate.
3	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?	Tripwire has instituted a Risk and Security Oversight Board responsible for the prioritization and funding for information security related activities across the company. This Board is the governing body for risk management within our organization, and senior management is heavily involved. Our Chief Financial Officer chairs this Board, and our General Counsel leads meetings. Policies and procedures are communicated at all management levels in multiple venues, and progress is reported against specific, measurable targets.

4	Where do organizations locate their cybersecurity risk management program/office?	The Risk and Security Oversight Board at Tripwire is a committee at the highest levels of the organization. The committee meets virtually and physically. Due to its cross-functional nature, this committee works with matrixed resources in the Information Systems department, the Research & Development department, the Security Research team, Legal, Finance, and other areas of the company.
5	How do organizations define and assess risk generally and cybersecurity risk specifically?	Most organizations with which we come into contact do not formally practice risk management in general, or cybersecurity risk management specifically. We often see a more structured approach to risk management as a company matures. Proper Risk Management is an expensive endeavor, and while it has proven to be beneficial on multiple levels within certain organizations, it has not been universally adopted. Of those addressing risk in a formal manner, the most common approaches focus on adapting frameworks such as NIST's RMF, ISACA's Risk Framework, FAIR, or the ISO standard for information risk management. However, many of these organizations are frustrated because their organizations are more focused on documenting that they have used a framework rather than focusing on truly implementing security. Tripwire commissioned The Ponemon Institute for a study called "The State of Risk-Based Security Management," which goes into detail about this. The initial study was performed in 2012, and another will be conducted in mid-2013.

6	To what extent is cybersecurity risk incorporated into organizations' overarching enterprise risk management?	As stated above, formal risk management is rarely practiced in most organizations. Ponemon, in the report mentioned above, states that more than half of organizations say they are "serious" about Risk-based Security Management, but fewer than 1/3 of organizations have a formalized risk program. Other recent reports suggest (though without citing specific data points) that larger the business is, the more likely they are to formally recognize that IT risk management is a piece of operational risk management. Small businesses appear unable or unaware to incorporate IT into their total understanding of operational risk.
7	What standards, guidelines, best practices, and tools are organizations using to understand, measure, and manage risk at the management, operational, and technical levels?	CIS and DISA benchmarks appear to be popular. PCI, NIST 800-53, ISO 27001, and COBIT are popular frameworks. Each specifies some degree of risk management, which is often not actually performed - each is viewed as compliance more than it is to guide operational security. CIS provides measurement guidelines as do frameworks, but all appear to be somewhat different. Internationally, heavy influence is apparent from the Monetary Authority of Singapore's Internet Banking and Technology Risk Management Guidelines, as well as Australian Defence SIgnals Directorate's Information Risk Manual and accompanying "Top 35 Strategies to Mitigate Targeted Cyber Intrusions."

8	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?	We are aware of PCI, NIST 800-53 (per FISMA), HIPAA, GLBA,NERC and SOX at the national level. States have some well-known reporting requirements around breaches as well (i.e. Massachusetts Privacy Law 201 CMR 17.00). All of these appear to have reporting requirements, but such reporting is largely compliance focused and not necessarily results focused.

9	What organizational critical assets are interdependent upon other critical physical and information infrastructures, including telecommunications, energy, financial services, water, and transportation sectors?	We take an "organizational critical asset" as an organization-owned asset, the failure of which would be catastrophic to the operation of the organization for some period of time. Given that definition, then organizationally critical assets are integrated with the community critical infrastructure at various points. For example, many companies would not function were it not for a fully-functional and resilient power supply, Internet, and public services. Additionally, many organizations would fail if the transportation industry suddenly came to a halt or were severely disrupted - recall the post 9/11 grounding of airlines and what that did to the economy. A similar event in a tangential transportation sector (i.e. rail, trucking, sea) would have similar results. The more connected an organization is, the more dependent upon power and Internet. It could be reasonable to suggest that nearly all businesses of any size would be adversely affected by disruptions to those and other sectors.

10	What performance goals do organizations adopt to ensure their ability to provide essential services while managing cybersecurity risk?	Measuring performance is a critical aspect of any cybersecurity program. When possible, we align cybersecurity with service performance. Providing secure, resilient software to our customers is paramount to our success, so we tend to focus more on typical performance indicators across the Software Development Lifecycle, in addition to those services we deem as being critical to our customers (i.e. support and our community portal).
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?	Our organization is not required to report to any regulatory body at this time.
12	What role(s) do or should national/international standards and organizations that develop national/ international standards play in critical infrastructure cybersecurity conformity assessment?	Some organized body needs to act as the checking balance in the system. Assuming the defined and required system (the framework) is 1) reasonable, 2) effective, and 3) minimally burdensome, and then a validation body should be able to perform routine assessments on an ad hoc and/or periodic basis. Such assessment is requisite to ensuring that the spirit of the framework is being met. Meeting the spirit of the framework is much different from meeting the letter of the law with the more abstract and verbose frameworks.

	Applicability of Existing Publications	
1	What additional approaches already exist?	There are generally three approaches: 1) Legal/regulatory, 2) contractual, 3) voluntary. We have copious examples of each category of framework, but all generally take the same approach based on a Plan/Do/Check/Act cycle. The implementation of these approaches typically suffer from a failure to adequately address specific aspects of risk management, which is to say that they do not provide enough guidance/prescription for an organization to effectively carry out risk assessment and make trade-off-based decisions.
2	Which of these approaches apply across sectors?	It is equally possible to apply any of the existing control frameworks across any sector. As the Unified Compliance Framework, and other sources of similar content (i.e. from product vendors such as Tripwire), adequately demonstrates, most (if not all) cybersecurity frameworks are ultimately equivalent.
3	Which organizations use these approaches?	Whether they realize it or not, all organizations use the same general approach to managing risk, including cybersecurity risk. The truth of the matter is that they are simply more or less aware (and presumably more or less formal) about it.

4	What, if any, are the limitations of using such approaches?	The major limitation is demonstrated in the verbosity of the selected framework. Control frameworks today do very little to describe or characterize the organizational processes each control objective and control necessarily effects.
5	What, if any, modifications could make these approaches more useful?	Rather than alluding to organizational processes, provide explicit links from controls to these processes. Make expected roles explicit. Make inputs to and outputs from processes explicit. Use diagramming to its fullest extent, thus reserving verbose instruction for step-by-step explanation of the process being described.

6	How do these approaches take into account sector-specific needs?	Are there really sector-specific needs? At the most abstract level, there are no special needs at the control framework level. Instead, there are special needs at the technical control and tool level. Platforms requiring coverage, for example, in the defense industrial base are going to be different than the platforms covered in the energy sector (i.e. SCADA systems). The overall approach should not be different. That said, the approaches in use today seem to take the exact opposite approach by making each control framework different or, the term is often used, "special." The overall risk management system should not be different between sectors. We believe these differences exist because of the verbosity of frameworks and a lack of concentration on organizational role and process abstractions.

7	When using an existing framework, should there be a related sector-specific standards development process or voluntary program?	There may be sector-specific standards in certain cases. If we choose to leave control frameworks at the abstract level, then we can apply standards at various levels within the overall risk management system. There may be a standard for representing the control framework in a human and machine-readable manner. There may additionally be standards for specific configuration settings, log formats, etc.

8	What can the role of sector-specific agencies and related sector coordinating councils be in developing and promoting the use of these approaches?	For an encompassing risk management effort to be useful, sector-specific agencies and coordinating councils must agree on a common vision of the problem domain. For example, if they all can agree that the ultimate purpose of these activities is to manage operational loss, that control frameworks are used to provide guidance on such minimization, that IT-related control frameworks allude to specific organizational processes, and that these all are intended to substantiate controls, then we can get off to a clean start. The "specialness" of each sector does not come before the control level, but rather exists below that and, perhaps, to the side where policy, process, and procedures are implemented as a result. We expect most differences to be in precise implementation of process and in specific procedures, which will pull in specific standards.

9	What other outreach efforts would be helpful?	Looking to the international community for guidance is critical to the overall success of this endeavor. This is a global problem requiring a global solution, and while we may have the most immediate effect in the United States, providing a reasonably well-thought framework applicable across sectors (not necessarily limited to critical-infrastructure) will go a long way toward engaging the international community.
	On Adoption Of Practices (listed in first cell)	
	• 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.	NA

1	Are these practices widely used throughout critical infrastructure and industry?	It is our experience that organizations are beginning to leverage network segmentation to keep various systems separated (i.e. business and operational). User I&A has also been increasing, but good, up-to-date asset management and incident detection and response are still getting up to speed.
2	How do these practices relate to existing international standards and practices?	Automation is a huge requirement looming in front of this effort. We MUST provide reasonably simple, but powerful, mechanisms that can be used to automate the processes affected by the to-be-proposed framework. The framework must start with a precise definition for all the concepts used in the domain. These definitions can be drawn from existing sources, but need to be reconciled in some manner to become THE source for information security and risk management terminology.
3	Which of these practices do commenters see as being the most critical for the secure operation of critical infrastructure?	The list provided is a perfect example of how we tend to slice the world in the wrong way. What does it take, for example, to suitably manage assets? To manage the asset lifecycle, you're going to need pieces of each of the other capabilities listed. Properly managed assets imply that they are properly configured, periodically checked, and that deviations from the expectations of "normal" prompt investigation (i.e. monitoring and response exist).

4	Are some of these practices not applicable for business or mission needs within particular sectors?	No. These practices are requisite for any organization in any sector having some asset they wish to protect. If there were a candidate for this answer, it might be that which requires resiliency. We can, however, speak of resiliency across any type of system, but this seems to be that concept which may be the most varied across system categories.
5	Which of these practices pose the most significant implementation challenge?	Security engineering, asset management, and key management are, historically, the most difficult to implement. This is true either because it is often difficult to get right (i.e. key management asset management), or requires humans to care and be trained (i.e. security engineering).
6	How are standards or guidelines utilized by organizations in the implementation of these practices?	Standard control frameworks are used less frequently than benchmark guidelines. Even then they are used somewhat sparingly. This is likely due to control framework complexity. The most often we see control frameworks used are under circumstances of compliance (i.e. PCI DSS 2.0, COBIT 5, NERC, and so on). Otherwise, an organization is more likely to have a set of organizationally-specific policies from which processes, procedures are derived and to which standards are applied.

7	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, the answer to this question will depend on the particular industry sector in which the organization operates. The financial, energy, health, and defense sectors appear to be the most mature and often have mechanisms of organizing IT-related business processes.
8	Do organizations have a formal escalation process to address cybersecurity risks that suddenly increase in severity?	The area where this comes into play is in specific IT processes, such as vulnerability management. At regular, frequent intervals systems in the enterprise are scanned for vulnerabilities, the severity of which may have changed at a given point. If the change in severity crosses a pre-defined threshold, then that particular vulnerability is treated differently. This in-built escalation may exist for misconfigurations, and perhaps other vulnerability classes as well.

9	What risks to privacy and civil liberties do commenters perceive in the application of these practices?	The risk to privacy and civil liberty is an important consideration. The biggest risk, however, will not exist in the framework, but outside in the legal system. Additionally, in some cases certain practices may be at odds with privacy and/or civil liberties. Consider encrypted e-mail as one example. If an organization closes off access to the world via typical personal communication means (i.e. personal access to IM, e-mail, Facebook and other similar sites), then the organization should expect that organizational-e-mail to be used for personal communication. What right the organization then has to inspect personal e-mail needs to be dictated in the legal system.

10	What are the international implications of this Framework on your global business or in policymaking in other countries?	As we have learned in the security automation standards space, international perception is critically important for global adoption. Historically, if a standardization effort is viewed as a U.S. Government effort, it is less likely to be well-received, much less adopted, internationally. If a goal of this framework is to be multi-national, then the framework is best developed by a non-partisan, non-government-sponsored, internationally recognized non-profit organization. Global adoption would be advantageous to multi-national corporations on several levels.
11	How should any risks to privacy and civil liberties be managed?	They should be noted, but not necessarily explicitly addressed. Again, the legal system needs to accommodate the answers.

12	In addition to the practices noted above, are there other core practices that should be considered for inclusion in the Framework?	Yes. Security Configuration Management is critically important to the success of any resilient and defensible system. This may fall under the purview of Asset Management, but without a solid take on the integrity of the system in question, it's going to be difficult to make any risk-based assertions that can properly substantiate a given control. Security Configuration Management properly includes configuration assessment and remediation, file integrity monitoring and change management, vulnerability assessment and remediation (i.e. patching). We are also assuming that a proper Incident Detection and Response program will appropriately monitor events (therefore affect standard configuration settings) using centralized log aggregation and inspection with SIEM or SIEM-like constructs such as correlation rules.