#	Question Text	Response Text	References
1	Describe your organization and its interest in the Framework.	Rapid7 is a leading provider of security data and analytics solutions that enable organizations to implement an active, analytics-driven approach to cyber security. We combine our extensive experience in security data and analytics and deep insight into attacker behaviors and techniques to make sense of the wealth of data available to organizations about their IT environments and users. Our solutions empower organizations to prevent attacks by providing visibility into vulnerabilities and to rapidly detect compromises, respond to breaches, and correct the underlying causes of attacks. Rapid7 is trusted by more than 5,100 organizations across 99 countries, including 37% of the Fortune 1000. We work with organizations to help them implement and maintain security programs aligned with the Framework, and we also use the Framework internally ourselves.	
2	Indicate whether you are responding as a Framework user/non-user, subject matter expert, or whether you represent multiple organizations that are or are not using the Framework.	We are responding as both a Framework user, and a security program subject matter expert. Our services teams help organizations both build programs that conform to the Framework, and assess their maturity against it. We also use the Framework internally to inform our own security program. Finally, we offer a number of software, cloud, or services solutions that satisfy many of the requirements outlined in the Framework, including in the Identify, Detect, Respond, and Recover functions.	
3	If your organization uses the Framework, how do you use it? (e.g., internal management and communications, vendor management, C-suite communication).	We believe the Framework sets out a logical and pragmatic approach to building a cybersecurity program, and it very much aligns with how we see security and the approaches we recommend to others and for ourselves. So we use it internally to communicate that vision to stakeholders, and enable us to make key decisions when necessary.	
4	What has been your organization’s experience utilizing specific portions of the Framework (e.g., Core, Profile, Implementation Tiers, Privacy Methodology)?	We use the Framework Core to make sure controls we are implementing for FedRAMP are well aligned with other frameworks and happen in logical progression. This creates a significant reduction in work, allowing us to get things in place in one manner and quickly tie that work back to broader certification efforts. It would be helpful to make sure that all US regulatory obligations are also highlighted in the Core. For example, if a Framework adopter decides to enter the healthcare market, they should be able to rely on the Core to link controls back to components of the HIPAA Security and Privacy rules. As we are proceeding towards FedRAMP, we are using a 'Profile-like' approach. We recommend adding one additional "Profile" to the current method that would allow framework-adopters to have an additional dimension to their story-telling. Our current approach to FedRAMP includes the following Profile's: Current, Minimum, Ideal. This distinction allows us to highlight what we MUST accomplish, versus where we would like to.	
5	What portions of the Framework are most useful?	Core offers the most tactical support and the profile approach helps highlight gaps, but lacks depth by only allowing two dimensions.	

#	Question Text	Response Text	References
6	What portions of the Framework are least useful?	Implementation Tiers are a novel approach and work in the right direction, but can delay tangible risk reduction given how broad they are. We would recommend looking at how BSIMM approaches maturity modeling for Application Security and see if a similar construct could be developed across the Core Functions. The Framework also indicates that establishing a cybersecurity program occurs in a relatively linear function, while this would be ideal, depending on the organization, this approach could inherently delay core controls that we already know are paramount to securing environments.	
7	Has your organization's use of the Framework been limited in any way? If so, what is limiting your use of the Framework (e.g., sector circumstance, organizational factors, Framework features, lack of awareness)?	As a high-growth technology company, our initial focus was immediate tactical risk reduction through the implementation of technical controls. The Framework could benefit from some adjustments that allow it to be immediately practical in organizations of all sizes and maturity levels. Ultimately, two of the single most important controls remain unaddressed in the Framework. NIST should consider asserting itself with a slightly more prescriptive approach to two-factor authentication and patching. We know that fully patched environments and two-factor authentication implementation dramatically reduce the risk of compromise.	
8	To what extent do you believe the Framework has helped reduce your cybersecurity risk? Please cite the metrics you use to track such reductions, if any.	The Framework hasn't added any immediate security risk reduction for our organization, but it has simplified some initiatives we are working on and has saved us some time.	
9	What steps should be taken to "prevent duplication of regulatory processes and prevent conflict with or superseding of regulatory requirements, mandatory standards, and related processes" as required by the Cybersecurity Enhancement Act of 2014?	n/a	

#	Question Text	Response Text	References
10	Should the Framework be updated? Why or why not?	Rapid7 believes the Framework should be updated. In the time since the Framework was released, it has seen impressive adoption and gained a reputation of credibility. It has a solid foundation on which to build, and can be even more impactful as a means of tackling the cybersecurity challenges that face all modern businesses and by extension, national security, the economy, and consumers. In order to increase its effectiveness, it must stay current as technology needs and possibilities evolve, and as the cybersecurity landscape and attacker methodologies change. This will help drive even broader adoption, and also ensure continued use and value for organizations that have already adopted the Framework. In the two years since the Framework was published, we've seen a number of developments both in the threat landscape, and in the security industry. For example, the Sony breach highlighted an attack type that had not previously been a huge focus for most organizations - a breach designed purely to cause major disruption and harm to the business. Similarly, we've seen ransomware emerge as a more virulent threat than previously, and at the same time, it's become apparent that point of sale systems are a huge target for financially-motivated attackers. The prevalence of successful user-based attacks has driven the emergence of a new class of cybersecurity solution: user behavior analytics. We're seeing organizations start to leverage the data in their environments to make more informed security decisions; and we're seeing emerging solutions classes such as deception-based security.	

#	Question Text	Response Text	References
11	What portions of the Framework (if any) should be changed, or removed? What elements (if any) should be added to the Framework? Please be as specific as possible.	We have not identified any sections that should be removed. In terms of changing current elements, we recommend shifting away from the emphasis on critical infrastructure. We understand the EO that initially mandated the creation of the Framework was focused on the Critical Infrastructure sectors specifically, but adoption of the Framework over the past two years has gone well beyond that, and it has proven to be relevant more broadly. It's hard to nail down a meaningful definition of critical infrastructure and draw stark lines around those industries in any case, and even if we could, it is not only those industries that are affected by cybersecurity threats and challenges - all are, and with very real negative implications for the economy and consumer well-being. We would also like to suggest some additions for the Framework, detailed below. These suggestions are additional to the recommendations made in the Roadmap published by NIST in Feb 2014, as we comment on those in response to question 14 below. * User behavior analytics. Since the initial development of the Framework, it has become increasingly well-established that malicious use of compromised credentials is a factor in the vast majority of compromises, and users make for easy targets for attackers. As a result, user behavior analytics has emerged as a quickly growing class of security solution. Some of the subcategories in the "Detect" function point at pieces of UBA functionality (DE.AE-1,2,5 and DE.CM1,3,6,7); however, there is little in the way of standard established testing or benchmarks for organizations looking to deploy these technologies. This is an area where NIST could add more informative references. It could also revisit these areas with a closer focus on detecting the malicious use of compromised credentials and lateral movement on the network specifically. * Vulnerability disclosure and handling. Due to its complexity, all technology	For vulnerability disclosure and handling: ISO/IEC 30111:2013 and ISO/IEC 29147:2014
12	Are there additions, updates or changes to the Framework's references to cybersecurity standards, guidelines, and practices that should be considered for the update to the Framework?	As proposed for questions 11, 13, 14.	
13	Are there approaches undertaken by organizations – including those documented in sector-wide implementation guides – that could help other sectors or organizations if they were incorporated into the Framework?	In October 2015, the FS-ISAC issued guidance on "control types to incorporate with vendor governance programs in order to improve information protection capabilities when using third party services and products in the supply chain for financial institutions' customers and employees." This report was created with a view that modern organizations are increasingly reliant on third party software, and this may represent significant risk, so it is important to consider this in the procurement process for any technology. This principle is true for all sectors, not only the financial services sector.	https://www.fsisac.com/sites/default/files/news/Appropriate%20Software%20Security%20Control%20Types%20for%20Third%20Party%20Service%20and%20Product%20Providers.pdf

#	Question Text	Response Text	References
14	Should developments made in the nine areas identified by NIST in its Framework-related “Roadmap” be used to inform any updates to the Framework? If so, how?	Rapid7 believes a number of significant developments have been made in the areas identified by the Roadmap, and that as a result, there are several valuable updates that should be made to the Framework: *4.1 Authentication As the Roadmap notes, compromised credentials frequently play a role in successful cyberattacks. Deploying multi-factor authentication is a straightforward way of reducing this risk and in the two years since the Roadmap was written, options for MFA have improved greatly. So too has adoption, but there is still a long way to go and Rapid7 believes NIST can play a valuable role in encouraging technology operators to offer or enforce the use of MFA. *4.2 Automated Indicator Sharing. In December 2015, Congress passed the Cybersecurity Act, which focused on improving cybersecurity information sharing. Many organizations want to participate in this, and those in the critical infrastructure sphere are particularly encouraged to do so by the Government. There has traditionally been a few barriers to adoption of this; concerns over legal ramifications was one, and was addressed in the Cybersecurity Act. Others have been the need for skilled labor and the delay in sharing timely information. Automating this process can address both challenges - reducing the burden on resources and improving the speed and efficiency of the process. NIST can help establish best practices and encourage productive automated indicator sharing in a numbers of ways: i) facilitating alignment amongst the private sector and the numerous Government agencies that are looking at or participating in information sharing. ii) better defining types of threat intelligence and how they can help organizations inform prevention/detection/response decisions. iii) defining better guidance on tagging and classifying sources of threat intelligence (e.g.: tell me what threat the intelligence is meant to find, when it	
15	What is the best way to update the Framework while minimizing disruption for those currently using the Framework?	n/a	
16	Has information that has been shared by NIST or others affected your use the Framework? If so, please describe briefly what those resources are and what the effect has been on your use of the Framework. What resources, if any, have been most useful?	n/a	
17	What, if anything, is inhibiting the sharing of best practices?	Anecdotally it often seems that awareness is the biggest challenge in driving adoption of best practices.	
18	What steps could the U.S. government take to increase sharing of best practices?	Drive increased awareness and understanding of the challenges and potential solutions, including benefits and relatively straightforward recommendations for overcoming challenges.	

#	Question Text	Response Text	References
19	What kind of program would help increase the likelihood that organizations would share information about their experiences, or the depth and breadth of information sharing (e.g., peer-recognition, trade association, consortia, federal agency)?	n/a	
20	What should be the private sector's involvement in the future governance of the Framework?	n/a	
21	Should NIST consider transitioning some or even all of the Framework's coordination to another organization?	n/a	
22	If so, what might be transitioned (e.g., all, Core, Profile, Implementation Tiers, Informative References, methodologies)?	n/a	
23	If so, to what kind of organization (e.g., not-for-profit, for-profit; U.S. organization, multinational organization) could it be transitioned, and could it be self-sustaining?	n/a	
24	How might any potential transition affect those currently using the Framework? In the event of a transition, what steps might be taken to minimize or prevent disruption for those currently using the Framework?	n/a	
25	What factors should be used to evaluate whether the transition partner (or partners) has the capacity to work closely and effectively with domestic and international organizations and governments, in light of the importance of aligning cybersecurity standards, guidelines, and practices within the United States and globally?	n/a	