Organizational Information	**Response**
Organization Name	Krypton Brothers
Organization Sector	IT Media and Consulting
Organization Size	10-Jan
Organization Website	http://kryptonbrothers.com
Organization Background	CEO is Cochair of the NIST Big Data WG subgroup on security and privacy
Point of Contact Information	**Response**
POC Name	Mark Underwood
POC E-mail	mark.underwood@kryptonbrothers.com
POC Phone	520-457-7004

#	Question Text	Response Text	References
1	Describe your organization and its interest in the Framework.	Krypton Brothers contributes Mark Underwood as cochair of the security and privacy subgroup of the NIST Big Data public working group. We also participate in the Ontolog Summit, which includes certain topics automated reasoning, classification and interop for security and privacy.	
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.	SME as part of related WGs. The framework has been consulted in our work in the NIST WG cited, as well as in academic writing about complex event processing for cybersecurity in the Internet of Things. We are also responding on half of clients who use the WordPress stack for web hosting.	
3	If your organization uses the Framework, how do you use it? (e.g., internal management and communications, vendor management, C-suite communication).	Used to guide related standards work for Big Data security and privacy. Internal use is limited to guidelines offered to our web hosting clients for their web hosting activities. (Most are small businesses and feel this approach is too burdensome - FYI).	
4	What has been your organization's experience utilizing specific portions of the Framework (e.g., Core, Profile, Implementation Tiers, Privacy Methodology)?	The Core is useful as a standards crosswalk (see References column p. 20), though there are quite a few standards that are not mentioned. The profile has some use for qualitative work, but seems aimed at a nontechnical audience and not connected to current architectures, which limits its usefulness. Ditto "tiers" - seems quite idiosyncratic, even if helpful.	
5	What portions of the Framework are most useful?	Those pertaining to "systems in situ," i.e., live systems after deployment.	
6	What portions of the Framework are least useful?	Those pertaining to architecture, design and the software development process and forensics for remediation and analytics after lapses, failures or disaster recovery walk-throughs. E.g., the "profile" is likely to be seen as unusable by developers who tend to leave these matters to analysts. Analysts are a dwindling breed in the DevOps ecosystem.	
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)?	The lack of an ontology and canonical cross-standard taxonomies is, and has been a hindrance. Lack of awareness is also a challenge, as the NIST message tends to get lost in the blurry of commercial messaging - including certification training, etc.	
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.	No specific metrics available, but we look to insider threat, extortion and response to DDoS as measures. Clients are aware of those after casual exposure to the framework (i.e., we send the PDF to them for review). Cause and effect is difficult to assess, however.	
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?	Ontology, common terminology, and having a funded watchdog position whose role it is to identify those conflicts.	
10	Should the Framework be updated? Why or why not?	Yes. We bellieve big data diversity and mobile data threats are not fully addressed to meet the privacy fears of the public. The framework would be more useful if it had case studies or use cases worked out in more detail. See remarks about technical writing resources.	
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.	Refer to previous remarks about CRISC BoK. There is a tendency to view the process as uni-organizational, which is flawed for Big Data.	

#	Question Text	Response Text	References
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?	The ISACA CRISC Body of Knowledge is sometimes more particular about how to develop a risk profile, yet does not get mentioned here.	
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?	CRISC BoK is a cross-sector approach, but domain-specific language approaches are needed in areas focused on compliance, forensics and risk management. The audience for this framework is IT, but that's probably not who will have to pay for it in some industry sectors.	
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?	Yes. Not sure what's being asked here. The roadmap might also consider: forensics, legal, access to cybersecurity resources during SDLC processes, "nonconformance" testing and self-reporting. Somee of this is touched upon, but it's unclear why a list of only 9 was selected. Why limit? Why group into those? The roadmap seems frozen at 2013 release.	
15	What is the best way to update the Framework while minimizing disruption for those currently using the Framework?	Use online resources with notification to subscribers. This seems like more of a staffing challenge than a true collaboration challenge. Any good collaboration platform will be sufficient if the word can get out. The greater problem is the soft voice inviting engagement, which is lost in the din of new products, systems and capabilities, especially at the intersection of IoT, cloud, big data and mobile.	
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?	Only communications about this framework. If it has been connected to other NIST initiatives, we have failed to connect with those communications.	
17	What, if anything, is inhibiting the sharing of best practices?	The word isn't getting out in industry channels. The effort needs to have the standing of a Github - a place where guidelines and suggestions are grabbed as though an API.	
18	What steps could the U.S. government take to increase sharing of best practices?	Create, nurture, host a Github-like resource that is API friendly.	
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)?	In addition to more tech writers, more promotion through industry trade pub channels, publicize use cases / case studies so that users will "see themselves" in the work. There will be a tendency for this effort to be seen as only for the Fortune 100.	
20	What should be the private sector’s involvement in the future governance of the Framework?	No different than any other segment of the framework.	
21	Should NIST consider transitioning some or even all of the Framework’s coordination to another organization?	No, but with more technical writer support, it could achieve greater penetration within the active subpopulation of NIST users, e.g., Big Data, Cyberphysical Systems, Cloud, etc. Technical writer effort can bridge siloes and foster reuse and common frameworks.	
22	If so, what might be transitioned (e.g., all, Core, Profile, Implementation Tiers, Informative References, methodologies)?	We would have to see to whom the world would get transitioned. Too much of the available resources -- e.g., SANS -- are very expensive and will exclude many shops from participation. The effort should foster zero cost dissemination and transparency.	

#	Question Text	Response Text	References
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?	Some of the standards organizations have proven that they are hindrances to adoption by erecting pay walls on front of the standards, or eschewing reuse of concepts better developed elsewhere. So it's not the profit status of the entity, but its charter and how it goes about execution that matters more. The business models that exist are not compellingly better than the current arrangement at NIST (though see our comments about techical writer resources).	
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?	The work should remain in the public domain, and participation in refinement exercises free or nearly free -- within reason. Host organizations should be required to stage webinar-based meetings that foster wide attendance without self-limiting issues such as proximity to Wash DC greater metro or Silicon Valley.	
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?	Ability to operate with transparency and maximum communication to a broad audience of both technical, managerial and governmental (custodial) readers. If this step is taken, suggest a separate RFI to address this concern. It's too important to leave as a single question, assuming that NIST does not keep this assignment and/or is not able to fund it.	