**Reponses from Threat Panel for "RFI - Framework for Reducing Cyber Risks to Critical Infrastructure"**

www.threatpanel.com

| ***Questions*** | ***Answers*** |
|---|---|
| 1. Describe your organization and its interest in the Framework. | Threat Panel is pleased to have the opportunity to provide input. Threat Panel ( www.threatpanel.com ) is a private company founded in 2015 by veterans of the cybersecurity industry. The company is focused on providing small, medium, and large organizations with an easy to use product for implementing the Cybersecurity Framework, as part of its offering. |
| 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. | User / Subject Matter Expert |
| 3. If your organization uses the Framework, how do you use it? (*e.g.*, internal management and communications, vendor management, C-suite communication). | All of the above |
| 4. What has been your organization's experience utilizing specific portions of the Framework (*e.g.*, Core, Profile, Implementation Tiers, Privacy Methodology)? | Core is the most actionable / specific. |
| 5. What portions of the Framework are most useful? | Please see #4 |
| 6. What portions of the Framework are least useful? | Implementation Tiers are useful but can be laid out in a more granular manner, i.e. subcategories in each of them. |
| 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)? | N/A |
| 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. | N/A |
| 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? [7] | This is one area which can also use improvement. The specific overlap and mapping of security and privacy regulations such as HIPAA and PCI can be better mapped, as is done with the information references. |

*Possible Framework Updates*

| | |
|---|---|
| 10. Should the Framework be updated? Why or why not? | Yes - but not too often. On one hand the framework needs to adapt to current environment, but on the other hand, too much change can fork or split the community resulting in inefficiencies. |
| 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. | As previously noted in #6 and #9. Also, more metrics across sectors, perhaps with ISAC input. |
| 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? | Any case studies, e.g. Intel case study, should be made centrally available on the resource page or other location. |
| 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? | A sweep of current case studies should be done, and the best practices of each should be brought up for discussion. |
| 14. Should developments made in the nine areas identified by NIST in its Framework-related "Roadmap" [8] be used to inform any updates to the Framework? If so, how? | Yes, as specific guidelines to be added into the respective sub-category. |

| | |
|---|---|
| 15. What is the best way to update the Framework while minimizing disruption for those currently using the Framework? | a) Proper versioning; b) Having a secure, signed autoupdate capability in software to stay current; c) Leveraging best practices from open source and private sector, e.g. diff tools, automatic updates delivered |

*Sharing Information on Using the Framework*

| | |
|---|---|
| 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? | Case studies as noted in #13. Furthermore, tailoring the framework for SMBs, where a dedicated security team might not be available. |
| 17. What, if anything, is inhibiting the sharing of best practices? | N/A |
| 18. What steps could the U.S. government take to increase sharing of best practices? | A 2-pronged approach: a) Promoting sharing of best practices among users of the framework; b) a web-based tool to faciliate the production and consumption of the best practices. |
| 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)? | Leveraging the best practices from the STIX/TAXI effort underway. |

*Private Sector Involvement in the Future Governance of the Framework*

| | |
|---|---|
| 20. What should be the private sector's involvement in the future governance of the Framework? | [Disclosure: Threat Panel is a private organization] There should continue to be a partnership and input, to leverage any innovation and tools produced by the private sector. |
| 21. Should NIST consider transitioning some or even all of the Framework's coordination to another organization? | Too early to tell. NIST has done a really great job thus far. There are different models that can be explored, and it is worth considering approaches that have been adopted in other fields, for example information sharing. |
| 22. If so, what might be transitioned (*e.g.,* all, Core, Profile, Implementation Tiers, Informative References, methodologies)? | Assuming a transition, all of the above should be transitioned. |
| 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? | Ideally, it would be a not-for-profit or the right for-profit. A for-profit can help with insuring it is self-sustaining. Another related idea, is to treat it as an open source project and manage it accordingly. The core committers would include but not limited to members of the entity it is transitioned to. |
| 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 danger is forking the framework resulting in confusion / non-adoption. |
| 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? | The governance structure is critical to ensure forward progress, even in the event of conflicting priorities. |