	Organizational Information	Response
	Organization Name	State of Indiana/Indiana Office of Technology (IOT)
	Organization Sector	Public - State Government
	Organization Size	30,000 (State)/300 (IOT)
	Organization Website	http://www.in.gov
	Organization Background	The Office of Technology establishes standards for technology infrastructure of the State and is focused on bringing the most appropriate technology solutions while maintaining the greatest security possible.
	Point of Contact Information	**Response**
	POC Name	Bryan Sacks
#	**Question Text**	**Response Text**
1	Describe your organization and its interest in the Framework.	The State of Indiana is focused on protecting the data that has been entrusted to it by Hoosiers. The framework provides a mechanism to improve and mature cybersecurity.
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.	The State is currently adopting the framework.
3	If your organization uses the Framework, how do you use it? (e.g., internal management and communications, vendor management, C-suite communication).	Having a 'Common Language' is essential for organizations that have multiple business units, agencies, departments, etc. The first step the State of Indiana is taking is to conduct a profile assessment using the Core of the CSF.
4	What has been your organization's experience utilizing specific portions of the Framework (e.g., Core, Profile, Implementation Tiers, Privacy Methodology)?	While many organizations are approaching the Core by mapping Functions, Categories and Subcategories to existing Policies, the State is considering refreshing policy under the CSF taxonomy to increase reporting capability.
5	What portions of the Framework are most useful?	All components play a role in improving cybersecurity for the State. The Core is the most useful, as it is the baseline for the whole approach. However, the value of the current and target profiles are also vital to an operation like State government. With appointed positions, the knowledge of security will differ significantly across agencies. Metrics, such as profile assessments, can provide a good benchmark for agency heads as they move into budgeting for their next fiscal year. Further, an analytical assessment of the profile results may produce items that can be enhanced at an enterprise level, rather than taking a decentralized approach to managing security.
6	What portions of the Framework are least useful?	The concept of Implementation Tiers is ideal, however, this is an area where the State plans to deviate from the content provided in the framework. With diversity in cybersecurity knowledge across agencies, adopting a simpler tiering model may provide more consistent results. Secondly, some of the Subcategories are difficult to grasp without additional context and can be interpreted in different ways. The purpose of the framework is to provide a common language, so if interpretations are different in the Subcategories, a comparison of apples to apples may no longer exist. To drive home interpretation, the State created questions for each Subcategory (i.e. Yes/No format) to validate that each agency is considering the same components when determining the Current and Target profile.
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 State is currently adopting the framework and hasn't been limited at this point.
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 State is not far enough along in adoption to conclude reduction in risk.
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?	NIST should enhance the mapping of 'Informative References' to additional regulations. Providing a comprehensive control crosswalk would be extremely helpful so that users of the framework can track their compliance with multiple regulations or standards through Excel (or GRC tools). The Informative References would be an ancillary document that provides the additional detail and should come in CSV, TXT, and other formats suitable for data import.
10	Should the Framework be updated? Why or why not?	Similar to special publications, there are new versions or revisions to previously posted documents. The framework should be updated, however careful consideration should be taken to keep the framework scalable. Having a defined or target schedule for updates would be beneficial for organizational planning.

#	Question Text	Response Text
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.	A simplified implementation tier definition would make the Framework easier to manage.
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?	A control crosswalk should be created for as many regulations, standards, etc. as possible. This will allow the use of the framework across all industries and sectors. Further, if this information can be in consumable format(s) by GRC tools, this will be extremely valuable for organizations looking to satisfy multiple requirements for similar controls.
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?	It would be useful to have successful use-cases posted for each industry/sector, if organizations are willing to provide this information.
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?	Any advancements should be communicated and shared.
15	What is the best way to update the Framework while minimizing disruption for those currently using the Framework?	The best method to minimize disruption is to allow for scalability. This could be manifested by keeping the Categories the same and modifying Subcategories only, or introducing entirely new Categories, confirming scalability prior to publishing.
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?	Use of presentations and use-cases posted on the NIST website have been helpful, additional use-cases that can be applied to the same industry would be ideal.
17	What, if anything, is inhibiting the sharing of best practices?	It is difficult to determine 'best practice' at the current state of implementation.
18	What steps could the U.S. government take to increase sharing of best practices?	A good sharing tool would be to create an industry-aligned information sharing program.
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)?	Barring using information security maturity as a competitive advantage in some industries, government is typically willing to share information with other government entities. If a secured information sharing program was established for all States (i.e. one representative per state), this may drive sharing of documents, use cases, etc. which may lead to enhanced ability to adopt the framework. Time and resources are major constraints in State government, if a program can reduce the burden, NIST CSF may see increased adoption.
20	What should be the private sector's involvement in the future governance of the Framework?	Key representatives should be involved in the evolution of the framework, whether public or private sector.
21	Should NIST consider transitioning some or even all of the Framework's coordination to another organization?	Possibly, if NIST determines that additional value can be derived. However, the framework should continue to be published by NIST.
22	If so, what might be transitioned (e.g., all, Core, Profile, Implementation Tiers, Informative References, methodologies)?	If any part of the Framework was transferred, the Informative References portion makes the most sense. Adoption may be higher if there is direct alignment with regulations or standards that are followed by an organization. However, the framework should continue to be published by NIST.
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?	All components should be published by NIST, even if a portion is transitioned to another organization.
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?	Organizational capability, knowledge, viability, etc.