Organizational Information	Response
Organization Name	**Novant Health**
Organization Sector	Health and Public Health
Organization Size	30k + Team Members, 13+ Acute Care Facilities, 400+ Ambulatory Facilities
Organization Website	novanthealth.org
Organization Background	Novant Health began as a partnership between two acute care facilities in piedmont of North Carolina and has seen rapid growth over the past decade, expanding coverage to 5 states in the southeast.
Point of Contact Information	**Response**
POC Name	Jeremiah Grant Edward Russell
POC E-mail	iso@novanthealth.org
POC Phone	704 316 0083

#	Question Text	Response Text	References
1	Describe your organization and its interest in the Framework.	Novant Health is a health care provider in the southeast. We are interested in the Framework as we are a part of one of the 16 critical infrastructure sectors (H&PH).	
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.	Although Novant Health is primarily a user of the Framework, after 1.5 years of use, we would also consider ourselves to be subject matter experts.	
3	If your organization uses the Framework, how do you use it? (e.g., internal management and communications, vendor management, C-suite communication).	Novant Health primarily uses the Framework as a as a tool to align disparate regulatory, compliance, and industry standards into a cohesive and holistic control framework. The Framework is also used to coordinate cybersecurity efforts of the organization into a coordinated and aligned security program. The Framework is used as a "translation" layer allowing us to view our environment from multiple vantage points - including regulatory, compliance, and other leading practice informational references. The Framework has been used as the basis and foundation for reporting current state, Tier I cybersecurity residual risk, and Cybersecurity Program maturity.	
4	What has been your organization's experience utilizing specific portions of the Framework (e.g., Core, Profile, Implementation Tiers, Privacy Methodology)?	Our organization primarily uses the Core of the Framework. Our experience, thus far, has been excellent. The cyber resiliency of the organization has been positively impacted by the implementation of the Framework Core.	
5	What portions of the Framework are most useful?	The Core is the most useful.	
6	What portions of the Framework are least useful?	The Implementation Tiers do not align with our business. Instead, we use a Capabilities Maturity Model based on COBIT to define our current state and target state across the cybersecurity functional areas.	
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)?	We have been fortunate to have full support organizationally for the implementation of the Framework. Our limitations are mostly in the form of external partners and staff augmentation that does not command the same level of working knowledge in the Framework.	
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.	Our organization attempted to use the CSET tool, and found it to be inadequate for our environment. We created an assessment tool based upon the Framework and have used that tool to conduct a gap analysis of our environment. This work has been extremely helpful in identifying and prioritizing our efforts to improve our cyber resiliency. We have, or are developing, metrics from 1300 areas that align to the 98 subcategories, 22 categories, and 5 functions.	
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?	The Frameworks primary strength is its ability to be used as a translation layer to align and coordinate disparate control sets. We have used it to align seemingly siloed efforts/compliance objectives into a cohesive program. In short, no steps are necessary to prevent duplication - the Framework is assisting us with doing so!	
10	Should the Framework be updated? Why or why not?	It is necessary to update the Framework - but given that we use it as the over-arching control set, reduced frequency of updates would be helpful, as these updates would have cascading effects on all controls we have mapped downstream.	

#	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.	ID.BE could contain more practical steps to accomplish. PR.DS-3 should really be a part of asset management and rolled up under ID.AM-1. PR.IP-5 is really saying; "Did you do everything you said you would do in ID.GV?" As such, we feel it belongs as an evaluation/audit under ID.GV. PR.PT-5 seems to be a catch-all for any protective technology that has not been called out in other sub-categories and could contain more detail as to what is needed to protect C2 communications. DE and RS are a slim on content and could be informed by NIST 800-61r2. RC is mostly business-focused and could contain more content that aids IT departments on how to enable the business to be cyber-resilient.	
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 mapping to PCI/DSS would be helpful. A mapping to NIST 800-53r4 control enhancements would be helpful (for advancing up the capability maturity model, or implementation tiers).	
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?	We are not aware of any other approaches.	
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?	Our organization has not evaluated the nine areas in the roadmap under section 4.	
15	What is the best way to update the Framework while minimizing disruption for those currently using the Framework?	If any changes are made, they should not be more frequent than annual (at most), and they should be published in parallel with a guide to what the changes were and tips on how to migrate the delta to the new guidance.	
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?	The National Cybersecurity Workforce Framework has aided with roles and responsibilities and the assignment of duties in the functional areas of the NIST CSF.	
17	What, if anything, is inhibiting the sharing of best practices?	We have not encountered any limiting factors yet.	
18	What steps could the U.S. government take to increase sharing of best practices?	An open-source community/forum where users could anonymously share mappings and successes could be very useful.	
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)?	Adoption of the cybersecurity framework for critical infrastructure should continue to be a voluntary, community-driven program, but it should also have incentives (either monetary, or government indemnification against breach).	
20	What should be the private sector's involvement in the future governance of the Framework?	In order to gather buy-in, the private sector should be heavily consulted via rfi's such as this one, and by forums in major cities in the major regional areas.	

#	Question Text	Response Text	References
21	Should NIST consider transitioning some or even all of the Framework's coordination to another organization?	NIST, under the Department of Commerce, is the appropriate place for this Framework and the coordination.	
22	If so, what might be transitioned (e.g., all, Core, Profile, Implementation Tiers, Informative References, methodologies)?	See 21.	
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?	See 21.	
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?	See 21.	
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?	See 21.	