60-Day Federal Register Commenting Period
NPPD SUMMARY OF COMMENTS and RESPONSES

1670-NEW (IT Sector SMB Survey)		
#	***Comment***	***Response***
Comments from a Project Manager/Idaho Small Business Development Center/Boise State University		
1	Speaking personally, the Small Business Development Centers (SBDC) can be valuable on the workgroup; either speaking on behalf of businesses or providing businesses with which the workgroup can talk.	Thank you for your response! Although SBDCs currently serve the Small and Midsize Businesses (SMB) Working Group as subject matter experts (SMEs), the Working Group has not specifically used the SBDCs to speak on behalf of businesses. Rather, the Working Group has leveraged the Small Business Administration (SBA) as a tool for communicating with SMBs in the development of the survey. Given the current structure of the questionnaire, the working group will not move forward with this recommendation, but will take your suggestion into consideration for possible future survey studies.
2	I would recommend getting engagement from the Procurement Technical Assistance Centers (PTAC) and Manufacturing Extension Partnerships (MEP) as they are both anticipating an increase of concern with cybersecurity from their clients and should have the opportunity to fully engage in steps such as this.	Currently, SBDCs serve the Small and Midsize Businesses (SMB) Working Group as subject matter experts (SME's). Specifically, the Small Business Administration (SBA) played a vital role in the development of the survey. Given the current structure of the questionnaire, the working group will not move forward with this recommendation. However, we will take your suggestion into consideration for possible future survey studies.
3	Please ensure the survey is delivered *in layman's terms*. Even being the project manager for SBDC Cybersecurity (though not being a cyber expert), this survey is not a walk	In developing the survey, it was specified that the survey is broken into two parts based on the necessary knowledge required to complete the survey. Questions 1-11 are intended for the Chief Executive Officer (CEO)

1670-NEW (IT Sector SMB Survey)		
#	***Comment***	***Response***
	in the park. Remember many SBE will not have a dedicated IT person who understands the tech language.	of a SMB, and as such were written in a way that can be easily understood. For example, question 4 provides descriptive language for the CEO to evaluate each critical asset as related to their organization. Questions 12 – 22 are intended for technical experts of SMB's that are implementing the NIST Framework. Therefore, existing implementation of the framework should imply an adequate level of IT Knowledge within the organization to answer the questions being asked.
4	Time is money. Are all these survey questions necessary? Do you expect to pull data from all of them? The shorter it is, the more completed responses you'll receive.	The motivation for the survey, as outlined in the submission package, is to obtain very specific type of information from SMBs, including: a) An understanding of current cybersecurity practices across the IT SMB sector; b) An assessment of familiarity with the NIST Framework and other cybersecurity standards; and c) A cost-benefit analysis of NIST Framework adoption and implementation. This analysis and supporting survey were requested by the IT SCC community as part of an on-going DHS initiative to provide IT SMBs with more effective practices to mitigate the current cyber threats that could jeopardize company assets. Therefore, it requires both sufficient technical depth and level of detail for the survey to deliver meaningful results that could support development of effective recommendations. The questionnaire was developed by the IT SCC, with the content and length of the survey having been vetted with the IT SCC community prior to FRN publication.

1670-NEW (IT Sector SMB Survey)		
#	***Comment***	***Response***
5	Emphasize confidentiality and be as clear as possible!!! If poorly executed, this survey itself could look like a cyber threat.	Currently, none of the survey questions inquire about the system architecture or specific defensive capabilities in place. While the requested information allows assessment of the overall cybersecurity practices and maturity level, the questions do not reveal vulnerabilities or specifics of the security posture. The questionnaire was developed by the IT SCC, with the content and length of the survey having been vetted with the IT SCC community prior to FRN publication. As stated in the supporting documentation, The IT SCC will administer the survey and anonymize the data, which will then be sent to DHS for analysis. The private sector will collect Point of Contact (POC) information through the survey instrument, but will not include that information on the anonymized dataset they submit to DHS. DHS will use anonymized data to conduct their analysis. The IT SCC will administer the survey via Survey Monkey and process raw inputs. DHS will only receive anonymized micro-dataset to come up with the summary statistics and aggregated summary results. DHS will aid with the statistical analysis as needed, but will not be working with the individual responses to the questionnaire. Only aggregate results will be utilized for the development of tailored cybersecurity practice recommendations.
Comments from the National Institute of Standards and Technology (NIST) Information Technology Lab (ITL) Applied Cybersecurity Division (ACD)		
In addition to the below responses, NPPD held meetings with NIST to ensure that their questions and concerns were addressed. Based on the meetings, NIST recommended adding an additional question to the survey and		

1670-NEW (IT Sector SMB Survey)		
#	***Comment***	***Response***
provided suggested wording for the question. NPPD added the additional question and accepted a majority of the suggested wording.		
1	Overall length: It could take longer than 30 minutes to fill out this questionnaire. Even one question: "what is the value of your top assets?" could potentially be a large undertaking.	The questionnaire was tested on the IT SCC membership. Time to fill out the questionnaire is separate from the time that the respondents may need to take to conduct internal analysis depending on the level of organizational maturity and internal process efficiencies or inefficiencies.
2	Terminology: the questionnaire uses the terms "implementing" and “adopting” the Framework. NIST specifically avoided using those terms as it implied there was a "right way" to implement/adopt. Therefore, NIST opted for "using" the Framework. NIST suggests the questionnaire remain consistent.	Decision to adopt vs awareness of the framework are two distinct concepts that the survey is intended to capture. The objective is to understand what challenges or barriers (technical, economical, etc.) prevent the SMBs that are aware of the NIST CSF from decision in favor of its implementation. Usage of the term “implement” is also consistent with the Executive Order 13800, Section 1c(ii)B.
3	There are questions regarding CSF spending. What is the end goal of these questions? To say how much is being spent per use? Each use of the Framework is unique and risk based, therefore each organization's spending is unique. Any aggregation or averaging of these data points could be taken out of context. Additionally, the results could be vastly skewed by one or 2 organizations responses depending on the aggregating methodology. The fact an organization chooses to use the Framework is a simple statement that they think it's a cost-effective	Yes, the organizations choosing to use the CSF does show that they think it could be an effective use of their resources. Yes, point estimates and averages can be misleading. This is in part why IT SCC decided in favor of conducting a survey to gather sufficient data to estimate the distribution of the associated investment and potential benefits. Part of the objective is to empirically validate whether the CSF is cost-effective. Currently no empirical data has been provided to verify that assertion. If only 2 organizations respond, the interpretation will be limited only to the two respondents with the appropriate disclaimer as to the exact number of respondents. This survey is voluntary, and therefore, due to inherent self-selection bias, the results of the

1670-NEW (IT Sector SMB Survey)		
#	***Comment***	***Response***
	use of their resources. To address the third bullet [comment], questions 12 e, f, and g could be replaced with the following: • "Does your organization see ROI in your use of the Framework?" (Yes/No/Maybe) • "How does your organization measure cybersecurity ROI?" (Free text) • "How did your use of the Framework affect your people, processes, and technology?" (Free text)	survey should only be interpreted within the context of the number and characteristics of those who responded. As stated in the PRA package documentation, by design no statistical representativeness will be claimed with respect to the survey results, irrespective of the number of respondents. A disclosure will be included to clarify that it is a voluntary survey, where statistical inference of the survey results on the rest of the population (beyond the actual survey respondents) is not appropriate, and therefore the results will not be generalized for the population. In case if 2 responses dominate the sample, analysis of the company characteristics is important to understand whether those data points truly come from a different data-generating process (i.e. outliers). The specific objective is to collect measurable quantitative data that can support empirical analysis of the CSF cost-effectiveness.