Organizational Information	Response
Organization Name	Siemens Industry Inc. Digital Factory / Process Industries and Drives Divisions
Organization Sector	Industrial Controls Systems
Organization Size	
Organization Website	http://www.usa.siemens.com/entry/en/
Organization Background	The Siemens Industry Inc. divisions Digital Factory (DF) and Process Industries and Drives (PD) are responding as suppliers of Industrial Control Systems.
Point of Contact Information	**Response**
POC Name	Rajiv Sivaraman
POC E-mail	rajiv.siva@siemens.com
POC Phone	+1 678 231 8082

Views on the Framework for Improving Critical Infrastructure Cybersecurity

Siemens Industry Inc.
Digital Factory / Process Industries and Drives Divisions

#	Question Text	Response Text	References
1	Describe your organization and its interest in the Framework.	Within Siemens Industry Inc., the Digital Factory (DF) division and the Process Industries and Drives (PD) division are suppliers of industrial control components and systems that are used to control and automate machines, processes, and systems within the physical world. The Framework addresses operators of industrial infrastructures. Siemens systems help these operators to implement the activities described in the Framework.	
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 Siemens Industry Inc. divisions DF and PD are responding as suppliers of Industrial Control Systems.	
5	What portions of the Framework are most useful?	The entire document provides useful information to an audience of wide experience levels in the area of cybersecurity. The Framework Core, which provides in a tabular format the Functions, Categories, Subcategories, and Informative References, is especially useful. This table allows security experts to communicate with senior management using a common, easy-to-understand framework that provides the opportunity for dialogue on the status of various categories.	
6	What portions of the Framework are least useful?	All portions of the framework are useful. The framework was designed to appeal to a wide audience of readers with varying levels of cyber security experience. The importance of individual sections of the framework is related to the cyber security experience of the reader.	
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)?	Siemens as a supplier of industrial control systems follows the international standard ISA99/IEC62443 which is one of the standards that supports the framework.	

Views on the Framework for Improving Critical Infrastructure Cybersecurity Siemens Industry Inc. Digital Factory / Process Industries and Drives Divisions			
#	**Question Text**	**Response Text**	**References**
10	Should the Framework be updated? Why or why not?	Yes. The framework should continue to evolve as existing standards are updated, and new standards are released.	
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.	Changes to the Framework should be determined using a series of workshops in a manner similar to the methods used for initial development.	
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?	Continued mapping of the categories and subcategories of the Framework to the current versions of internationally-accepted security-related standards (e.g. ISA99/IEC62443) should be part of the focus of any Framework update.	
20	What should be the private sector's involvement in the future governance of the Framework?	The private sector should be involved in providing input directly to the Framework (via NIST sponsored workshops) and to the international standards bodies that support the implementation of the cybersecurity activities that the Framework describes.	