#	Organization	Commentor	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
1	SUNY-WCC Cybersecurity Program	Brian Cronin	G/T	1	All	1	The name 'Framework' is too generic and should be renamed to 'CyberFramework' since it is dealing with cybersecurity.	change 'Framework' to 'CyberFramework' throughout the document.
2	SUNY-WCC Cybersecurity Program	Brian Cronin	G/T	1	82	1	Should include that cyber attacks change over time and the use of the cyberframework will change also.	Because each organization's risk is unique, along with its use of IT and ICS, and because cyberattacks change over time, the implementation of the CyberFramework will vary accordingly.
3	SUNY-WCC Cybersecurity Program	Brian Cronin	G/T	2	118	1	The cyberframework core terminology should be the same as what all information security professionals are taught in colleges and universities throughout the United States to use to reference the security planning process today. This refers to using the six phases (Identify Assets, Identify Risks, Create Policies, Implement, Monitor, Recover from an incident) of the security process when discussing cyber security issues. This is a fundamental rule that should be carried throughout the entire document including modifying all artwork and illustrations.	The CyberFramework Core consists of six Catagories - Identify Assets, Identify Risks, Create Policies, Implement, Monitor, Recover from an incident -
4	SUNY-WCC Cybersecurity Program	Brian Cronin	G/T	3	210	2.1	The Functions, Categories, Subcategories should be renamed to better indicate their structure in a business environment.	Rename Functions to Categories, Rename Categories to Modules, Rename Subcategories to SubModules and leave Informative References as is.
5	SUNY-WCC Cybersecurity Program	Brian Cronin	G/T	5	216	2.1	Renamed Functions to Categories because businesses and their employees will understand 'Categories' but not 'Functions'. Functions are something that a computer program has.	Categories organize basic cybersecurity activities at their highest level. These Categories include the six phases of the security process: Identify Assets, Identify Risks, Create Policies, Implementation, Monitor and Recover from an incident. The categories aid in communication...
6	SUNY-WCC Cybersecurity Program	Brian Cronin	G/T	6	224-226	2.1	Explain what Modules are so that businesses and employees will understand.	Modules are the subdivisions of a Category into groups of cybersecurity outcomes, closely tied to cyber security needs and particular activities. Examples of Modules include: Asset Management, Access Controls and Detection Processes.

7	SUNY-WCC Cybersecurity Program	Brian Cronin	G/T	6	227-231	2.1	Explain what SubModules are so that businesses and employees will understand.	SubModules further subdivide a Module into higher-level outcomes, but are not intended to be a comprehensive set of practices to support a module. Examples of SubModules include: Cataloging physical devices and systems within the organization, Databases are protected and notifications from the detection system are investigated.
8	SUNY-WCC Cybersecurity Program	Brian Cronin	G/T	6	232-237	2.1	To longwinded, Explain what the Informative References section is, so that businesses and employees will easily understand it.	Informative References are links to specific sections of standards, guidelines and common practices that illustrate a method to accomplish the activities associated within each SubModule.
9	SUNY-WCC Cybersecurity Program	Brian Cronin	G/T	6	242	2.1	Change to core categories	The six CyberFramework Core Categories defind below apply to both IT and ICS.
10	SUNY-WCC Cybersecurity Program	Brian Cronin	G/T	6	243-244	2.1	Explain 'Identify Risks'	Identify Risks – Develop the institutional understanding to manage cybersecurity risks to organizational systems, assets, data and capabilities.
11	SUNY-WCC Cybersecurity Program	Brian Cronin	G/T	6	245-251	2.1	Explain 'Identify Risks'	The Identify Category includes the following SubCategories of outcomes: Asset Management, Business Environment, Governance, Risk Assessment and Risk Management Strategy. Understanding the business context, the resources that support the critical IT infrastructure and the related current cybersecurity threats, helps to enable an organization to focus its efforts and resources towards positive results.
12	SUNY-WCC Cybersecurity Program	Brian Cronin	G/T	6	252-254	2.1	Explain 'Create Policies'	Create Policies – Develop policies using appropriate safeguards to ensure the delivery of critical infrastructure services.

13	SUNY-WCC Cybersecurity Program	Brian Cronin	G/T	7	255-258	2.1	Add ‘Implementation’ section and explain	Implementation – implement policies and safeguards that protect the assets. The Implementation Category includes the following Modules of outcomes: Access Control, Awareness and Training, Data Security, Protective Technology and Information Protection Processes / Procedures. The Protective activities are performed consistent with the organization’s risk strategy defined in the Identify Risk Category.
14	SUNY-WCC Cybersecurity Program	Brian Cronin	G/T	7	259	2.1	Change 'Detect' heading to 'Monitor' because the cyberframework core should be the same as the six phases in the security process that all information security professionals reference today.	Change 'Detect' to Monitor'
15	SUNY-WCC Cybersecurity Program	Brian Cronin	G/T	7	261-272	2.1	Move the 'Respond' paragraph into the 'Monitor' Category because this is how it is handled within the six phases in the security process that all information security professionals reference today.	Develop and implement the appropriate activities prioritized through the organization’s effective planning and risk management process to identify the occurrence and detection of a cybersecurity event. The Monitor elements include the following modules: Anomalies and Events, Response Planning, Analysis, Mitigation, Improvements, Security Continuous Monitoring and Detection Processes.

16	SUNY-WCC Cybersecurity Program	Brian Cronin	G/T	7	273-280	2.1	Change 'Recover' to 'Recover from an incident' because this is how it is handled within the 'six phases in the security process' that all information security professional reference today.	Recover from an incident – Develop and implement the appropriate policies and procedures, prioritized through the organization's risk management process, to restore the capabilities or critical infrastructure services that were impaired through a cybersecurity event. The Recover from an incident category includes the following Modules: Recovery Planning, Improvements and Communications. The activities performed in the Recover from an incident category are performed consistent with the business context and risk strategy defined in the Identify Risks Category. The activities in the Recover from an incident Category support timely recovery to normal operations to reduce the impact from a cybersecurity event.
17	SUNY-WCC Cybersecurity Program	Brian Cronin	G/T	7	292-298	2.2	Reworked the last paragraph of the Framework Profile to be current with the Categories, Modules and SubModules sections.	The Profile is the alignment of the Categories, Modules, SubModules, industry standards and a best practice which takes into account the business requirements, risk tolerance and the financial resources of the organization. Identifying the gaps between the organizations current profile and its goals, allows the creation of a prioritized roadmap that the organization will implement to reduce its cybersecurity risks.
18	SUNY-WCC Cybersecurity Program	Brian Cronin	G/T	38	600-601		change 'these enabling' technologies to 'insecure' technologies because these technologies are inherently insecure.	growth. However, the functioning of the critical infrastructure has become dependent on insecure technologies, spurring governments around the globe to view cybersecurity increasingly

								Organizations. As many organizations and corporations operate globally or rely on the interconnections of the global digital infrastructure, many of the requirements are affecting or may affect how organizations operate and conduct business. Diverse and unique business requirements and constraints can impede interoperability, produce duplication, harm cybersecurity and hinder innovation, thus significantly reducing the availability and use of innovative technologies to critical infrastructures in all industries. This ultimately hampers the ability of critical businesses and organizations to operate globally and to effectively manage new technology and the evolving risks of such technologies. The CyberFramework is designed to create international standards that can be scaled to any size organization or business to help manage and eliminate cybersecurity risks.
19	SUNY-WCC Cybersecurity Program	Brian Cronin		38	604-612	c.6	Changes to the International Aspects, Impacts, and Alignment seciton to focus more on how the CyberFramework can help the corporation and business.	
20	SUNY-WCC Cybersecurity Program	Brian Cronin	G/T	3	170-171	1.2	‘optimize target states’ does not mean anything and the sentence need to be more concise and geared towards business needs.	Enable organizations to review and prioritize decisions regarding cybersecurity. The CyberFramework utilizes risk assessment to help organizations select goals for cybersecurity activities.
21	SUNY-WCC Cybersecurity Program	Brian Cronin	G/T	3	182-183	1.2	The original sentence is fragmented and needs to be more concise and geared towards business needs.	Because of these differences, the CyberFramework is designed as a risk-based guide, with a goal of providing flexible implementations for all business models.