Submitted by: _____
Date: _____

#	Organization	Commentor	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
1	Intelligence and National Security Alliance (INSA) Cyber Council		G	6	245		Cyber intelligence must drive any effective cybersecurity enterprise. To meet the emerging challenges of the cyber domain, critical infrastructure organizations need to operate within the context of a well thought out and dynamic defense, informed by intelligence at the strategic, operational and tactical levels, which addresses actual threats and prepares for potential threats. Reactive defense postures are no longer sufficient for an adequate risk management strategy. Cybersecurity planning and operation must be intelligence-driven. Intelligence driven cybersecurity: • Transforms the cybersecurity posture from reactive to proactive. • Permits a shift from perimeter defense to maneuver operations. • Enables an adaptive cybersecurity posture based on a continuous assessment of the threat/risk environment and its implications for an organization's enterprise security activity. Risk assessment is an important part of intelligence-driven cybersecurity, but the function of "risk assessment" does not subsume cyber intelligence.	We propose adding "Cyber Intelligence" as a new category under the IDENITFY function. The categories subdivide the Functions into groups of cybersecurity outcomes, which are closely tied to programmatic needs and particular activities. Although the implications of cyber intelligence permeate most of the framework functions, we believe that designating a category for cyber intelligence will provide adequate guidance to critical infrastructure protectors and clarify the need for a proactive, intelligence-driven cybersecurity posture. Recommended insertions in bold and underscored below. The Identify Function includes the following categories of outcomes: Asset Management, Business Environment, Governance, **Cyber Intelligence,** Risk Assessment, and Risk Management Strategy. The activities in the Identify Function are foundational for effective implementation of the Framework. Understanding the business context, resources that support critical functions and the related cybersecurity risks enable an organization to focus its efforts and resources. **Establishing and employing a Cyber Intelligence capability promotes an intelligence-driven enterprise that transforms the cybersecurity posture from reactive to proactive.** Defining a risk management strategy enables risk decisions consistent with the business needs or the organization.
1 (cont)	Intelligence and National Security Alliance (INSA) Cyber Council						(Comment #1 continued.) Cyber intelligence informs investment and policy decisions and shapes the operational and technical defensive posture of an organization.	

#	Organization	Commentor	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
2	Intelligence and National Security Alliance (INSA) Cyber Council		G	6	245		Executive Order 13587, *Structural Reforms to Improve the Security of Classified Networks* and the *Responsible Sharing and safeguarding of Classified Information*, signed in October 2011, and the *National Insider Threat Programs*, signed in November 2012, mandate and provide guidance for insider threat programs in federal agencies that handle classified information. Since the release of this guidance, the federal government has paid significant attention to its insider threat mitigation programs. However, no mandates, standards, or benchmarks exist for the insider threat programs in the private sector. Therefore, it is difficult for companies to assess where they stand relative to their peers and to make decisions about their insider threat mitigation strategies. Proposed changes to the *National Industry Security Program Operating Manual* (NISPOM) mandate insider threat programs for private sector organizations subject to NISPOM. However, the remainder of the private sector organizations that support the nation's critical structure have no such mandate. Without such a mandate, US companies are unprepared to tackle the pressing risk of insider threat.	We propose adding "**Insider Threat**" as a new category under the IDENTIFY function. Insider Threat risk mitigation is integrated into an enterprise risk management process. A formal insider threat program integrates and analyzes technical and nontechnical indicators to provide a holistic, continuous insider threat risk assessment on an individual basis. Manual or automated processes identify psychosocial events - anomalous, suspicious, or concerning non technical behaviors. Technology is used to detect suspicious online activity, and to focus on monitoring specific people who have been identified as high risk individuals.
3	Intelligence and National Security Alliance (INSA) Cyber Council		T	15 & 16	466	Appendix A		Delete ID.RA- 2 and ID.RA-3

#	Organization	Commentor	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
4	Intelligence and National Security Alliance (INSA) Cyber Council		T	15	466	Appendix A	Same rationale as for comment #1.	Please insert the Cyber Intelligence Category within the "Identify" Function and the seven cyber intelligence subcategories. Recommend that Cyber intelligence immediately follow the Governance Category and precede the Risk Assessment Category. Descriptions of the recommended Category and Subcategories in the format of the Appendix A Table is provided in the Cyber Intelligence Category tab of the worksheet for clarity. **Cyber Intelligence (IN):** The organization continuously collects, processes, analyzes, and disseminates actionable information about the vulnerability of valued assets in relation to the risk posed by the evolving array of internal and external threats, and uses that information at the strategic, operational , and tactical levels to guide its efforts to Identify, Protect, Detect, Respond, and Recover.
5	Intelligence and National Security Alliance (INSA) Cyber Council		T	15	466	Appendix A	Same rationale as for comment #2.	Please insert the Insider Threat Category within the "Identify" Function . Recommend that Insider Threat immediately follow the Cyber Intelligence and precede the Risk Assessment Category. **Insider Threat:** The organization continuously collects, processes, analyzes, technical and nontechnical indicators to provide a holistic, continuous, insider threat risk assessment on an individual basis and uses that information at the strategic, operational , and tactical levels to guide its efforts to Identify, Protect, Detect, Respond, and Recover.

#	Organization	Commentor	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
6	Intelligence and National Security Alliance (INSA) Cyber Council		T	15	466	Appendix A	Same rationale as for comment #1.	**ID.IN-1**: Information is systematically collected from both internal and external sources and integrated with vulnerability information. The scope of threat-related information goes "beyond the network" and includes known and potential adversaries or threat actors and their capabilities, intentions and activities in the cyber realm. Collection includes automated feeds, periodic regular queries, targeted research around topical events, etc.
7	Intelligence and National Security Alliance (INSA) Cyber Council		T	15	466	Appendix A	Same rationale as for comment #1.	**ID.IN-2:** Specialized and designated personnel systematically analyze threat-related information (internal and external) to identify current threats, forecast potential threats, protect assets, and assess impact.
8	Intelligence and National Security Alliance (INSA) Cyber Council		T	15	466	Appendix A	Same rationale as for comment #1.	**ID.IN-3:** Analyzed threat information is translated into "products" that address the information needs and interests of the organization's key decision makers IT, and security and is disseminated to those stakeholders in a timely way.
9	Intelligence and National Security Alliance (INSA) Cyber Council		T	15	466	Appendix A	Same rationale as for comment #1.	**ID.IN-4:** An appropriate range of tools is available for collecting and processing internal and external threat-related information that can be used to develop actionable intelligence about attacks, attackers and motivations.
10	Intelligence and National Security Alliance (INSA) Cyber Council		T	15	466	Appendix A	Same rationale as for comment #1.	**ID.IN-5:** Properly trained and qualified cyber intelligence staff are in-place to analyze information and create actionable intelligence products.
11	Intelligence and National Security Alliance (INSA) Cyber Council		T	15	466	Appendix A	Same rationale as for comment #1.	**ID.IN-6:** Procedures are in place for disseminating actionable intelligence products, and for feedback to analysts about the usefulness of those products, and the evolving information needs and interests of the organization's decision makers.

Submitted by: _____
Date: _____

#	Organization	Commentor	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
12	Intelligence and National Security Alliance (INSA) Cyber Council		T	15	466	Appendix A	Same rationale as for comment #1.	**ID.IN-7:** Procedures are in place for cyber intelligence to inform and be used at all levels within the organization to make policy, investment, technical, risk assessment, and security decisions.