DRAFT - Framework Glossary

Term	Draft Definition
Category	The logical subdivision of a function; one or more categories comprise a function. Examples of draft categories include “Know the enterprise assets and systems”, “Implement controls: Access Control”, “Implement controls: Risk monitoring & detection”, “Perform incident response”, and “Perform system recovery”.
Critical Infrastructure	Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.
Cyber Environment (infrastructure)	Includes electronic information and communications systems and services and the information contained in these systems and services. Information and communications systems and services are composed of all hardware and software that process, store, and communicate information, or any combination of all of these elements. Processing includes the creation, access, modification, and destruction of information. Storage includes paper, magnetic, electronic, and all other media types. Communications include sharing and distribution of information. For example: computer systems; control systems (e.g., supervisory control and data acquisition–SCADA); networks, such as the Internet; and cyber services (e.g., managed security services) are part of cyber infrastructure. SOURCE: NISTIR 7628
Cybersecurity	The ability to protect or defend the use of cyberspace from cyber attacks. SOURCE: CNSSI-4009
Detect	The Framework function that involves activities that identify (through ongoing monitoring or other means of observation) the presence of undesirable cyber risk events, and the processes to assess the potential impact of those events.
Framework	A voluntary structure to reduce cyber risks that relies on private sector input and existing standards, guidelines, and practices. Also known as the “Cybersecurity Framework”.
Framework Implementation Level (FIL)	The extent and degree to which an organization has implemented the functions, categories, and subcategories of the Framework.
Function	One of the main components of the cybersecurity risk management approach used for the Framework. The five functions are Know, Prevent, Detect, Respond, and Recover.
Informative References	References to existing cybersecurity-related standards, guidelines, and practices.
Know	The Framework function that involves an organization gaining the institutional understanding to identify what systems need to be protected, assess priority in light of organizational mission, develop an understanding of risk, and manage processes to achieve cost effective risk management goals.
Prevent	The Framework function that involves the categories of management, technical, and operational activities that enable an organization to decide on the appropriate outcome-based actions to ensure adequate protection against threats to business systems that support critical infrastructure components.
Recover	The Framework function that involves categories of management, technical, and operational activities that restore services that have previously been impaired through an undesirable cybersecurity risk event.
Respond	The Framework function that involves specific risk management decisions and activities enacted based upon previously implemented planning (from the Prevent function) in reaction to an adverse event.

Term	Draft Definition
Risk	The level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring. SOURCE: NIST IR 7298r2
Risk Management	The process of managing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the nation resulting from the operation or use of an information system, and includes: (1) the conduct of a risk assessment; (2) the implementation of a risk mitigation strategy; (3) employment of techniques and procedures for the continuous monitoring of the security state of the information system; and (4) documenting the overall risk management program. SOURCE: CNSSI-4009
Risk Mitigation	Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process. SOURCE: CNSSI-4009; NIST SP 800-30; NIST SP 800-39
Sector Coordinating Council	A private sector coordinating council composed of representatives of owners and operators within a particular sector of critical infrastructure established by the National Infrastructure Protection Plan or any successor. SOURCE: Executive Order 13636
Structure	The components that comprise the Framework and how they fit together; the functions, categories, subcategories, informative references, etc.
Subcategory	The logical subdivision of a category; one or more subcategories comprise a category. Examples of draft subcategories include “Inventory hardware assets”, “Restrict and protect remote access”, “Implement and test fire/physical intrusion detection devices / systems”, “Perform incident handling activities as described in the incident handling plan”, and “Provide alternate work site to recover work activities”.