5566 West Main Street • Suite 207 • Frisco, TX 75033
ENCRYPTICS®

In April of this year, Encryptics responded to NIST's request for comments: Developing a Framework to Improve Critical Infrastructure Cybersecurity. We are pleased to have another opportunity to provide feedback that will help finalize the National Cybersecurity Framework. Below are our responses to the questions posed in the Preliminary Cybersecurity Framework To learn more about our organization, please visit encryptics.com.

- *Does the Preliminary Framework adequately define outcomes that strengthen cybersecurity and support business objectives?* **Th Preliminary Framework does not address incentives that a business may receive should they implement a suggested Tier (see Section 2.4, p. 9). All business sectors lack sufficient incentives to make impactful cybersecurity investments and practices that will mitigate risk. Because critical infrastructure sectors such as defense, energy, and utilities have higher liability du to the type and amount of data they transfer and store and their impact on US citizens should breach occur in these sectors, incentives should be outlined within the Framework.**

  Any rewards-based program designed to help grow businesses would encourage greater investments in cybersecurity. Such incentives could include tax breaks, government refunds, and/or insurance programs. Rewards could include lower costs or refunds for compliance as well as additional benefits for early adopters of the Framework. An incentive program could define metrics in order to track improvements, designate levels of success, and award certifications for each suggested Tier implementation to achieve best cybersecurity practices and risk mitigation within Critical Infrastructure throughout the US.

- *Does the Preliminary Framework enable cost-effective implementation?* **Yes, because the Framework is flexible and because organizations are free to perform their own cost-benefit analysis, decision makers will be able implement the Framework in manner that best suits their organization. Following the steps outlined in section 3.2: Establishing or Improving a Cybersecurity Program (p. 11), only Step 6: Implement Action Plan will require signification cost considerations.**

- *Does the Preliminary Framework appropriately integrate cybersecurity risk into business risk?* **Th Framework states that "a key objective of the Framework is to encourage organizations to consider cybersecurity risk as a priority similar to financial, safety, and operational risk" (p. 1). This suggests that cybersecurity is a significant concern when it comes to national infrastructure, but does not express how organizations may also realize benefit. As a motivator, the Framework could discuss fiscal, legal, brand, and other business implications organizations are faced with when a security breach or data leak occurs.**

- *Does the Preliminary Framework provide the tools for senior executives and boards of directors to understand risks and mitigations at the appropriate level of detail?* **Yes, Appendix A: Framework Core provides appropriate terminology and deconstructs cybersecurity activities in way that senior executives and boards of directors can communicate using a common language relative to cybersecurity risk, in a context that reflects their organization's current disposition and future objectives.**

- *Does the Preliminary Framework provide sufficient guidance and resources to aid businesses of all sizes while maintaining flexibility?* **Appendix A: Framework Core provides sufficient guidance by illustrating common cybersecurity tasks. Also, the concept of security Tiers (p. 9-11) will prove especially useful to smaller organizations as it promotes a crawl, walk, run approach, which will help organizations to achieve their target security objectives over time. However, the Framework could better identify resources associated with completing each task and hyperlink these resources directly in the document to reduce the amount of time readers spend searching external sources. The Framework Core provides Informative References alongside each Subcategory, but these aren't hyperlinked, and in some cases, they don't explicitly mention the topic at hand. For example, o page 18, *NIST SP 800-53 Rev. 4* is listed as an Informative Reference for "PR.DS-2: Data-in-motion is secured." However, *NIST SP 800-5 Rev. 4* does not explicitly mention "data in motion" anywhere in the document. If the Framework clarified the intended purpose of the Informative References and included only clearly pertinent sources, readers would be able to take better advantage of these resources.**

- *Does the Preliminary Framework provide the right level of specificity and guidance for mitigating the impact of cybersecurity measures on privacy and civil liberties?* ***N/A***

- *Does the Preliminary Framework express existing practices in a manner that allows for effective use?* **Yes, the Framework Core provides good examples of existing practices, organized by Function, Category, and Subcategory. These examples provide solid foundation to help readers as they establish or improve their cybersecurity program.**

- *Will the Preliminary Framework, as presented, be inclusive of, and not disruptive to, effective cybersecurity practices in use today, including widely-used voluntary consensus standards that are not yet final?* **Yes, the Framework accommodates widely-used voluntary consensus standards. Additional voluntary consensus standards to consider, along with protecting data-at-rest and data-in-motion (p. 18), are (a) protecting data-in-use and (b) providing pre-internet encryption. We realize the Subcategories are just suggestions and are not comprehensive, however, we believe it important to include the above referenced additions as data protection technologies have evolved to include these additional capabilities, and customers in the market are beginning to identify them as necessity for security requirements.**

- *Will the Preliminary Framework, as presented, enable organizations to incorporate threat information?* **Th Tiers described within the Preliminary Framework in Section 2.4, Framework Implementation Tiers, will be helpful to an organization when conducting a threat assessment and with choosing the level in which they choose to incorporate into their business practices. However, when suggesting that organizations should leverage external guidance, a more specific reference to these external resources would be helpful to organizations as they are attempting to incorporate the cybersecurity Tiers.**

- *Is the Preliminary Framework presented at the right level of specificity?* **Yes, we believe the Framework's five Core Functions identified within the Framework Core, Section 2.1 (p.5) will b helpful to organizations as they develop their cybersecurity practices.**

- *Is the Preliminary Framework sufficiently clear on how the privacy and civil liberties methodology is integrated with the Framework Core?* ***N/A***