The NIST Cybersecurity Framework 2.0

comments by Kim Schaffer

(pages are from the start of the document, i.e., eight off from the printed pagenation)

■ Page 16 ■

[*Highlights*]

and tolerance (such as outlined in GOVERN), organizations can prioritize cybersecurity activities, 278 enabling them to make informed decisions about cybersecurity expenditures and actions. 279 Organizations may choose to handle risk in different ways — including mitigating, transferring, 280 avoiding, or accepting the risks — depending on the potential impacts. Importantly, 281 organizations can use the Framework both internally and to oversee third parties. 282

🟦 Page 16 🟦

"may choose to handle risk in "one or more ways , not "different ways"

■ Page 16 ■

[*Highlights*]

Creating and Using Framework Profiles to Understand, Assess, Prioritize, 301 and Communicate 302 The Framework's mechanism for describing an organization's current or target cybersecurity 303 posture in terms of the Core's outcomes is called a Framework Profile (Profile). 304 Profiles are used to understand, assess, prioritize, and tailor the sectorand technology-neutral 305 Core outcomes (i.e., Functions, Categories, and Subcategories) based on an organization's 306

🟦 Page 16 🟦

"current or target" is just confusing at this point and is discussed later. Also this should not be a Framework Profile with Framework italicised, but just Profile. Framework profile is not used later and just adds to confusion.

cybersecurity technology-neutral organization's and leading

■ Page 18 ■

[*Highlights*]

Organizations can create and use Profiles to utilize the full capabilities of the Framework (as 329 discussed in Section 1). While organizations can use the Framework without Profiles, they 330 provide the opportunity to develop a prioritized roadmap to achieve the cybersecurity outcomes 331 of the Framework. There are many ways to use Profiles, including to: 332 • Compare current cybersecurity practices to sector-specific standards and regulatory 333 requirements 334 • Document the Informative References (e.g., standards, guidelines, and policies) and the 335 practices (e.g., procedures and safeguards) currently in place and planned in the future 336 • Set cybersecurity goals for the organization, identify gaps between current practices and 337 the goals, and plan how to address the gaps in a cost-effective manner 338

■ Page 18 ■

"achieve the cybersecurity outcomes of the" Profile, which is very different from "outcomes of the Framework."

■ Page 27 ■

[*Highlights*]

The NIST Cybersecurity Framework and the NIST Privacy Framework can be used together to 655 collectively address cybersecurity and privacy risks, as illustrated by Fig. 8. As the right side of 656 the Venn diagram depicts, organizations using the Cybersecurity Framework to manage 657 cybersecurity risks can leverage the Privacy Framework Identify-P, Govern-P, Control-P, and 658 Communicate-P Functions to identify and manage privacy risks unrelated to cybersecurity 659 incidents, such as those described above. The Cybersecurity Framework DETECT, RESPOND, and 660

■ Page 27 ■

This is really confusing as what I think you are trying to say is that adding privacy means that Cyber-related privacy events have to be not only covered by both (extra work for both) but also should remain consistent for both frameworks.