NIST Cybersecurity RFI

Kevin J. Slonka, Sc.D.
Information Technology Architect
[redacted]
Sourceree (https://www.sourceree.com)

1. Please update the use of the term “cybersecurity” across the federal government to be two words: cyber security. The term “cyber” stands alone, as demonstrated by your many documents where you use it as a modifying noun: cyber supply chain, cyber software engineer, etc. You never create compound words in any other case (cybersupply chain, cybersoftware engineer, etc.) so why do you do it in the case of cyber security? It is grammatically incorrect and should be fixed.
2. Regarding the generality of the framework it is safe to say that there are too many frameworks and too little direction. CSF, 800-171, 800-53, RMF, HIPAA (800-66), CMMC, ISO, HITRUST, PCI, etc. Unless you’re an organization that is required by law to adhere to one of them, it’s too confusing. As an MSP, we have to deal with many of them at the same time because of the wide range of clients we support and it’s ridiculous. But if you’re a random business that isn’t legally obligated to adhere to a specific framework, which do you choose to use on your own? NIST would like to say that companies should choose CSF, but why would they? From a business owner perspective, why wouldn’t you want your business to be just as secure as companies that deal with the government? In that case, you’d choose 800-171 or CMMC. From my (a cyber professional) perspective, CSF is missing some key elements that I believe every business should implement. CMMC contains these elements (even more so in its 1.0 version). So what should NIST do: keep the CSF incomplete or add those elements, effectively making CSF exactly the same as CMMC? In such a case, why should CSF even exist? Just tell people to use CMMC. Returning to the point of this section, there are too many frameworks.
3. Regarding the direction given in the framework, there is none. Unless you are an experienced assessor/auditor, when a framework tells you “Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process” you throw your hands up and quit. NIST’s answer is that companies are expected to understand that CSF is simply a framework and when it tells you to use a supply chain risk assessment process you are supposed to know to look for other NIST documents, finding 800-161, and use that to guide you. First, most organizations would never make that connection. Second, 800-161 is 282 pages of yet another ridiculously difficult to understand framework that the average business owner (nor his IT staff) would never be able to implement. Even CMMC has this problem, but they began fixing it by offering “plain English” directions on how a company would actually assess/implement each security control. Should CSF stick around this would be beneficial, especially from a supply chain perspective with NISTIR 8276 being made into a more formal, easy to use, document.