From: Vytautas Butrimas
To: cyberframework
Subject: Comments to NIST Cybersecurity Framework (CSF) 2.0
Date: Sunday, August 27, 2023 3:45:54 AM

Have read the NIST Cybersecurity Framework (CSF) 2.0 released for public comment on August 8, 2023 and present these comments and suggestions:

In a sense the "if it ain't broke, don't fix it" rule has not been followed. Right from the beginning the authors note that the title of the earlier version has been changed from the original "Framework for Improving Critical Infrastructure Cybersecurity" to a "Cybersecurity Framework". The rationale is that the new title reflects the author's intention for the framework to be used 'by all organizations". This in my opinion weakens the document by introducing an unhelpful ambiguity in determining what needs to be protected. In short it could not be understood that everything needs to be protected, which is not realistic considering that resources to implement the advice in the Framework will be limited. Having the focus on critical infrastructure makes good sense in a national policy document where protecting economic activity, national security and well-being of society should be main objectives. By the way the document later contradicts itself on line 99 where it states "The voluntary Framework is not a one-size-fits-all approach to managing cybersecurity risks. An important and wise recognition of reality but why start off by saying the document applies to all organizations?

Since the title of the document refers to "cybersecurity" in general then it is important to determine what it is the authors are seeking to protect. Again as at the beginning the authors are seeking a broad application of the Framework as seen on line 139-139 where it is stated that it "applies to all information and communications technology (ICT), including information technology (IT), the Internet of Things (IoT), and operational technology (OT) used by an organization". It extends the umbrella even further to "to all types of technology environments, including cloud, mobile, and artificial intelligence systems". The latter is a very topical subject and has also found a place here.

This broad application in my opinion is a sign of a poor understanding of the various environments where technology is being used. There are many caveats to consider when applying the same security practices to data centric and process control environments. Having a framework that covers both is a mistake. Better to have a framework for each environment. One for where data is the focus of protection and one for where the focus is on protecting the technologies used to monitor and control processes governed by the laws of physics and chemistry. To put it more clearly in an illustration: one for the electric utility's billing department and one for power generation and distribution operation.

I am sorry to say again that we have another IT cybersecurity biased document which now, in

addition, the authors think will cover every environment. For example let us look at the statements about the "intended audience

The primary audience as stated on line 150 is for "those responsible for developing and leading a cybersecurity program". It appears that the main burden for implementation is placed on the CISO. This may be fine for the office IT environment where the CISO should have the training, but it is doubtful whether this knowledge can be successfully applied when addressing the issues peculiar to process centric control environments.

The authors also say on line 156 that the Framework is also for "policymakers (such as associations, professional organizations, and regulators)". This is fine but why not also include that it would be useful to automation engineers and senior plant engineers? They know how things run (the physical process) and could be of great help (especially with explaining the caveats) in assisting the CISO in implementing the Framework.

The next disappointment is the lack of attention to describing the threats. To conduct risk management, in addition to knowing what assets need protection it is vital to know what can threaten those identified assets. Figure 3 which illustrates "Cybersecurity Framework Profiles" does include a graphic depicting "Threat Environment", but this is not developed in the text with an appropriate description. A lost opportunity to inform the reader about the kinds of threats and their associated skill sets that would inform work on developing security profiles. For example, much material is available, which is not found here, from the documented cases of advanced persistent threat (APT) attacks on critical infrastructure. The one who is responsible for cybersecurity for an organization would for example benefit from knowing about the use of cyber means to disrupt nuclear enrichment facility operations (Stuxnet), petrochemical plant (Triton), electric power (Industroyer/Black energy), pipeline operations (Colonial) and compromise of network management software (Solar Winds/Orion). The above examples are useful cases for learning about cyber cyber-attack methods and about what was targeted and should inform the work in developing a security profile.

For the most part this document which pretends to apply to all organizations is focused on just cyber threats to data, privacy and those that can come through the supply chain. Much language is devoted to addressing privacy and supply chain threats. Figures 7 and 8 feature "privacy" in the center of the graphics. Again the bias towards protecting data is stressed as is stated on lines 640-642 where it states that "Cybersecurity risk management is essential for addressing privacy risks related to the loss of confidentiality, integrity, and availability of individuals' data. For example, data breaches could lead to identity theft".

Grossly missing is any understanding of the link between cybersecurity and control. Especially the technologies that are also cyber vulnerable and control physical processes that can lead to fatalities, damage to property and environment. The one threat that does get worthy attention is the cyber threat that can come through the supply chain. This is discussed

in its own dedicated section 3.5. One of the few times where clear actionable advice is provided for how this threat can be addressed in contracts and procurements from vendors.

In summary while this is a valiant attempt by a government agency to get everybody organized around a framework for cybersecurity it is too shallow in its understanding of what needs to be protected and from what threats. This can be remedied if more effort is put in adding a section on the cyber threat environment. One that includes documented and successful efforts by advanced persistent threat actors to take away the view and control of a physical process found in critical infrastructure. The places where we get our electricity, water and heat from. Turning the focus away from critical infrastructure protection to cover all systems and putting responsibility on the back of the CISO without appreciating the contribution of the engineers that know how things run are just a few serious flaws in this draft document. The authors should go back to using the original title. While this may not be possible at this late date then at least they should reach out to those who know how critical infrastructure runs for help in adding more process control relevant language to this document.

Thank you for the opportunity to comment and wish the work on completing the draft the best of success.

Vytautas Butrimas
Industrial Cybersecurity Consultant
Co-Moderator SCADASEC List
Member of ISA 99 Workgroups 13 (Education) and 14 (Substation security profiles)
Vilnius, Lithuania