From: Dorian Cougias
Sent: Tuesday, December 19, 2017 12:25 PM
To: cyberframework <cyberframework@nist.gov>
Subject: An analysis of the glossary of CSF 1.1, Draft 2

Please find enclosed our analysis of 1.1, Draft 2's glossary.

—

Best,

Dorian J. Cougias
Co-Founder and Compliance Scientist
Unified Compliance Framework

From: Dorian Cougias
Sent: Tuesday, December 19, 2017 4:02 PM
To: cyberframework <cyberframework@nist.gov>
Subject: Re: An analysis of the glossary of CSF 1.1, Draft 2

Sorry, we added one more pretty wild bit. It seems your definition of cybersecurity matches the dictionary definition of information security. Which we are pretty sure you don't want to do lest people think the Cybersecurity framework is merely a restating of information security. Of which there are a zillion documents.

—

Best,

Dorian J. Cougias
Co-Founder and Compliance Scientist
Unified Compliance Framework

[***Final attachment copied below***]

An analysis of the glossary found within NIST Cybersecurity Framework 1.1 draft 2

Some of the significant terms and definitions are missing, others must be "re-termed"

There are three problems with this very short glossary.

1) The glossary is ascribing specific definitions to well-known terms (and it shouldn't do that).
2) The glossary is using terms within definitions that are not defined anywhere.
3) Terms used throughout the document are not referenced in the glossary.
4) Definitions found in the glossary match different terms found in other **dictionaries**.

The problem of ascribing a new definition to an accepted term

The is a difference between "terms of art" and well known and generally accepted terms and their definitions. A term of art is "a word or phrase that has a precise, specialized meaning within a particular field or profession"[i]. As such, terms like Cybersecurity and Cybersecurity event are considered terms of art. They have precise and specific meanings in the field of Cybersecurity.

On the other end of the spectrum are terms that, once evoked, you can expect most of the audience to immediately understand. As such, terms like category and function are well known and have generally accepted meanings. So much so that the meaning for both words is the same in each and every dictionary you search[ii].

Most glossaries enter terms of art – precise words with specialized meanings. They most often do, as they should, forego entering generally accepted terms. What they should **never** do it attempt to abscond a generally accepted term and assign it a new, term of art, definition. Both the Dictionary Society of North America, and the International Society for Historical Lexicography have created rules around when a definition for a generally accepted term *should* be updated and when it *should not* be updated. Neither of them would update their definition for a generally accepted term if a single document's glossary were to redefine that term in its own words. Therefore, **adding a generally accepted term to a glossary with a term of art definition is *never* a good idea**.

Instead, if the authors wish to ascribe a term of art definition to a generally accepted term, they should modify the term within the document to make it *more precise*, which is what a term of art *is*. A *precise* term with a *specialized meaning*.

Such is the case with the NIST Cybersecurity Framework 1.1, draft 2. Here is the list of egregious words that should be changed, as their definitions as stated within the glossary are precise and the terms have generally accepted definitions well beyond what is provided in this document:

Glossary term as stated	**Suggested change**
Category	Cybersecurity outcome category or Cybersecurity Framework category
Framework	Cybersecurity framework
Function	Cybersecurity function
Subcategory	Cybersecurity outcome subcategory or Cybersecurity Framework subcategory

The problem of definitions using terms of art that are not defined

There are several definitions within the NIST Cybersecurity Framework 1.1 draft 2 glossary that use terms of art. Within the definitions of several terms, we find these terms of art used without any definition as to what they mean:

Glossary term(s)	**Term of art found in definition**
Category (and multiple other references)	cybersecurity outcome
Cybersecurity event	cybersecurity change
Framework, Identify (function)	cybersecurity risk
Framework core, Function	cybersecurity activity

Do definitions of these terms exist?

For some, yes. Here are the definitions along with their term IDs as found in ComplianceDictionary.com, the world's largest compliance dictionary with over 250,000 terms.

Term	**Definition**
cybersecurity activity	Security controls that are specific to the realm of Cybersecurity.
cybersecurity risk	A risk to organizational operations, (including mission, functions, image, and reputation), reso and other organizations due to the potential for unauthorized access, use, disclosure, disrupti modification, or destruction of information, Information Tech- nology, and/or Operations Technology.
cybersecurity outcome	No known definition
cybersecurity change	No known definition

Of the terms listed above, cybersecurity outcome is the most referenced, and probably the most-often misunderstood term in the document. One of the very first terms within the updated glossary references "Cybersecurity

outcomes". And yet, *Cybersecurity outcomes* has no formal glossary entry. The closest it comes is stating that the content in the Category and Subcategory columns *are* the Cybersecurity outcomes[iii]." And if you read the document, you'll see that the contents in the Categories and Subcategories are not written as Mandates "do this, don't do that". They are written as *outcomes* – "Physical devices and systems within the organization are inventoried". If the document simply stated the outcomes, we'd all be fine. But it didn't. It later adds that there are *tiers* of implementation involved as well. Four tiers in all, with measurements of each tier's process, integration with the risk management program, and external participation.

So now, if we are to extend this notion of "cybersecurity outcome" to involve the tiers, the mandate to inventory physical devices and systems would look like these potential outcomes (for brevity, we will list two of the four tiers):

Tier 1 Partial

Risk Management Process: Physical devices and systems within the organization are inventoried *on an ad hoc, sometimes reactive basis*.

Integrated Risk Management Program: *There is limited awareness at the organization level that* Physical devices and systems within the organization *should be* inventoried. *There are no defined processes to ensure that* Physical devices and systems within the organization are inventoried.

External Participation: *The organization does not understand its role in the larger ecosystem with respect to its dependencies and dependents when ensuring* Physical devices and systems within the organization are inventoried. *It does not collaborate with or receive information from other entities, nor does it share information when* Physical devices and systems within the organization are inventoried.

Tier 2 Risk Informed

Risk Management Process: Physical devices and systems within the organization are inventoried *using a system approved by management but not established as an organization-wide policy. Prioritization of the need for* Physical devices and systems within the organization *to be* inventoried *is directly informed by organizational risk objectives, the threat environment, or business/mission requirements*.

Integrated Risk Management Program: *There is awareness at the organization level that* Physical devices and systems within the organization *should be* inventoried. *There is no organization-wide approach to ensure that* Physical devices and systems within the organization are inventoried. *How* Physical devices and systems within the organization are inventoried *is shared within the organization on an informal basis. Cyber risk assessment of* Physical devices and systems within the organization *being* inventoried *occurs, but is not typically repeatable or reoccurring*.

External Participation: *The organization understands its role in the larger ecosystem with respect to its dependencies or dependents but not both when ensuring* Physical devices and systems within the organization are inventoried. *It collaborates with and receives some information from other entities, but may not share information when* Physical devices and systems within the organization are inventoried.

This leaves us with a definitional problem

The problem we now have is this. Are cybersecurity outcomes synonymous with the Categories and Subcategories, or are they synonymous with the tiered *implementation* or *level of effectiveness* of the Categories and Subcategories?

Stated another way, does an organization answer yes/no/na to the question "does the organization inventory physical devices"? Or do they answer according to their implementation tier for risk management processes, risk management program, and external participation **for each category and subcategory**? This means that the Cybersecurity outcome for that first question (only focusing on a subset of potential tiered outcomes) becomes this set of questions:

> What level of awareness is there that physical devices should be inventoried? none/limited/full
>
> Are there defined processes to inventory physical devices? processes but not procedures/documented procedures/documented procedures that are risk informed and reviewed/documented procedures that are adapted from lessons learned
>
> etc.

What do others think it means?

Cindy Fornelli, a major influencer for Cybersecurity within LinkedIn, calls out the need for better "Cybersecurity outcomes" in her article Principles for Better Cybersecurity Outcomes[iv]. However, she doesn't define them. The closest she gets is the reference "doing less and hoping that nothing bad happens". Not helpful. Neither doing less nor hoping nothing bad happens was mentioned in the NIST Categories and Subcategories.

David Wennergren, a writer for Federal Week Technology, wrote an article entitled Valuing cybersecurity outcomes instead of oversight[v]. The closest *he* gets is "measurable outcomes that ensure mission results".

Tim Layton, Chief Intelligence officer for SurfWatch Labs wrote an article for Security Week entitled Changing Cybersecurity Outcomes with Intelligence[vi]. The only mention of a Cybersecurity outcome is the title. Everything else is about machine learning and how great it is. Little help there. And there are about 400 articles like this that use the term, but don't even mention the term in the article. Sorry to pick on your Tim.

Wikipedia states in their entry for the NIST CSF[vii] that the NIST CSF "defines a number of subcategories of cybersecurity outcomes and security controls, with 98 subcategories in all". The entry has a further definition for security controls, but no definition for security outcome. And what they point to for security outcomes are the contents in the NST CSF for Category and Subcategory – basically the whole control list. Which leaves *nothing* in the list for Cybersecurity outcomes.

Robert Smith, Systemwide IT Policy Director for the University of California wrote a presentation The NIST Cybersecurity Framework (CSF); Unlocking CSF – An Educational Session[viii]. In it, he states that the outcomes are a cross reference between the Controls and the implementation tier. As an example, "DE.CM-4: Malicious code is detected" is a control and its implementation level could be that it is "formally approved and expressed as a policy." (Tier 2). So according to this model, if the Control is to be able to detect malicious code, the Cybersecurity

outcome for the organization could be that they have a "*formally approved and expressed policy* to detect malicious code."

David Leigh, in his blog Defcon Cyber, What's in YOUR Profile? [ix] suggests that the tiers are separate from the Cybersecurity outcomes, they exist to "provide an outcome effectiveness value". Like Tim's article, there are about a hundred or so other articles like this that have the same loose tie in between the categories and each organization's audited implementation.

What does NIST say in ancillary documents?

In their Cybersecurity Framework FAQs Framework Components[x] NIST states that cybersecurity outcomes are "based on business needs that an organization has selected from the Framework Categories and Subcategories". So this *looks, at face value*, like it contradicts Wikipedia by stating that the outcomes *are* the Categories and Subcategories. Or as Wikipedia lists them, the Controls. But that's at face value. You could also read into this that the Cybersecurity outcomes are the actual *tiered implementations* because if you add a business need to the definition, maybe the business need would only be for simple documentation (and not adaptive risk-based documentation), no sharing, but lots of monitoring. In other words, adaption for each and every Category and Subcategory from tier 1 to 4.

So far what have we learned?

So far, the closest we've gotten to a workable definition is the one we built from Robert Smith's presentation, coupled with David Wennergren's statement that a Cybersecurity outcome should be measureable, and what NIST added in an ancillary document that an outcome should be tied to a business need. So far, the vote from the two writers and the NIST document is to conjoin Categories and Subcategories with their outcome effectiveness values.

So we are left with a *strict* interpretation, choice A: A Cybersecurity outcome is one of the outcomes listed in either the Categories or Subcategories section of Table 2 in the NIST Cybersecurity Framework.

Or an *inferred* interpretation, choice B: A Cybersecurity outcome is the business need defined, tiered implementation of the outcomes listed in either the Categories or Subcategories section of Table 2 in the NIST Cybersecurity Framework.

The online survey

Because even our own lexicographer team at Unified Compliance couldn't figure it out, we turned to using a survey to ask our constituents. 1/4th of the respondents (so far) believe that a Cybersecurity outcome should be defined along the lines of choice A listed above. 2/4th of the respondents believe that a Cybersecurity outcome should be defined along the lines of choice B listed above. And the final 1/4th provided their own interpretation.

The final problem – this glossary is somewhat insufficient

While the glossary has defined certain cybersecurity terms, it has left out definitions of terms it uses within the Framework Core, that are not defined in any other Authority Document (or at least not in the over 1,000 Authority Documents mapped into the Unified Compliance Framework). The significance of this, is that out of the **couple hundred thousand**

Citations found within the UCF, NIST's Cybersecurity Framework *alone* is using these terms – and they have not defined them in their glossary.

Here is a partial list of these terms that have *never been defined anywhere*. Once the Unified Compliance team have mapped the document and tagged the nouns and verbs, we will release to NIST a fuller mapping and terminology report.

- organizational communication and data flow
- industry ecosystem
- sector specific risk analysis
- unnecessary assets
- specialized systems
- baseline of normal operations and procedures
- cybersecurity data

Definitions found in the glossary match different terms found in other **dictionaries**

There is a hard and fast rule in the world of lexicography – you can't usurp an existing definition and ascribe it to a new lemma (term). Examining the dictionary entry for *cybersecurity,* the primary term in this document, we find that the document's definition is:

> The process of protecting information by preventing, detecting, and responding to attacks.

And that is completely encompassed in the definition for **information security**, as defined by several **dictionaries**.

> The process by which an organization protects the creation, collection, storage, use, transmission, and disposal of information from unauthorized access, use, disclosure, disruption, modification, or destruction.

Others have defined cybersecurity in a way that distinguishes it from normal information security. One such definition could be the following:

> The process of protecting information by preventing, detecting, and responding to attacks that take place through computer networks against computers, information technology, and virtual reality.

Whatever wording NIST ultimately chooses, the definition should result in something much more specific than the definition of information security. Unless we are all to conclude that cybersecurity is merely a rewording of information security.

For more information on Cybersecurity and other compliance terms, search ComplianceDictionary.com

---

[i] https://en.oxforddictionaries.com/definition/term_of_art
[ii] Instead of entering the very long Google string, search what is a category, or what is a function
[iii] "Categories are the subdivisions of a Function into groups of cybersecurity outcomes closely tied to programmatic needs and particular activities." Line 302 and 303 of version 1.1 Draft 2.

[iv] https://www.linkedin.com/pulse/principles-better-cybersecurity-outcomes-cindy-fornelli/
[v] https://fcw.com/articles/2015/06/15/comment-wennergren.aspx
[vi] http://www.securityweek.com/changing-cybersecurity-outcomes-intelligence
[vii] https://en.wikipedia.org/wiki/NIST_Cybersecurity_Framework
[viii] http://www.ucop.edu/ethics-compliance-audit-services/_files/webinars/5-5-16-nist-cyber-security/nist-cyber-security.pdf
[ix] https://rofori.wordpress.com/tag/nist-cybersecurity-framework/
[x] https://www.nist.gov/cyberframework/cybersecurity-framework-faqs-framework-components