NIST Framework Response

This response includes the personal comments of Dr. Eric Burger, speaking as an individual and not on behalf of Georgetown University, the Security and Software Engineering Research Center at Georgetown, USACM, IEEE-USA, or any other organization.

Narrative Comments

Target Organization Size as well a Sector

We would like to consider the question asked on line 17, whether the *Preliminary Framework* provides **sufficient** guidance for businesses **of all sizes**. We think that most small business, even in designated critical infrastructure sectors, will not have the resources to apply the *Preliminary Framework*. This is so, even with a mere eight pages for the framework description and 40 pages for the framework proper. The vast majority of American businesses will not be able to digest the *Preliminary Framework* on their own. A simple, one-page summary of the *Preliminary Framework*, with pointers for where to get assistance, would go a long way to broaden the appeal, adoption, and execution of th *Preliminary Framework* model. Otherwise, the *Preliminary Framework* will be limited to only large enterprises that can afford dedicated staff or mid-size enterprises that will have to pay cash for outside assistance to understand, evaluate, and most likely execute the *Preliminary Framework*'s suggestions.

Along these lines, the *Preliminary Framework* focuses mostly on how the framework will apply to a given organization. However, and as tangentally acknowledged around lines 303 and 322, such a framework can, and should, apply across entire sectors. Perhaps adding, "provides guidance to an organization **and sector**" on line 84 would help advertise the broader scope of the framework early on for the reader.

Framework Core Components

The framework core component functions (line 119) do not line up with Presidential Policy Directive 8 on National Preparedness.[1]

Preliminary Framework	PPD-8 (*National Preparedness*)
Identify	**Prevention**
Protect	Protection
Detect	**Mitigation**
Respond	Response
Recover	Recovery

[1] See http://www.dhs.gov/presidential-policy-directive-8-national-preparedness

The above table compares the terms used in the two documents. It may be valuable and avoid problems in the future if the framework referenced PPD-8 and briefly explained why NIST is using *almost* the same flow. The last thing the community needs is people asking why the government suggests one framework for everything related to critical infrastructure (PPD-8) and something different for Cybersecurity (*Preliminary Framework*).

Insider Threat

The framework needs to describe the insider threat. While politically motivated cyber attacks are sexy and cool, the insider threat represents a large risk. The first we hear of the insider threat is through an oblique reference at line 255ff. The framework should be more explicit. Moreover, this will give context and justification for the HR-related core functions described later.

Threat and Tier 2

Tiers 1, 3, and 4 explicitly reference the threat landscape facing the organization. The risk management process for tier 2 may or may not be threat-based, and the framework should say so (line 348).

Nits

Footnote 2 (line 80) points to the generic DHS critical infrastructure page. http://www.dhs.gov/critical-infrastructure-sectors points to the listing of sectors and associated critical functions and value chains.

Line 295 is rather presumptuous. Perhaps a better wording would be, “organizations can implement to reduce Cybersecurity risk.”

Core Comments

Protect

PR.IP-11 is the first hint we have that not all threats come from outside the organization. Given the insider threat has historically been one of (if not) the greatest threat to an organization, not mentioning it by name and only tangentially referring to it reduces the impact of the subcategory. A person reading the *Preliminary Framework* that is unaware of the issues of insider threat might not understand that this subcategory may be the **single most important threat to address**.

Describing how the human resources function fits in to access control may be of use in this section. The point being that access control is first about people and only later about technology. If the framework focuses on technology, we will have technology for technology’s sake and not have a meaningful security posture.

PR.DS-7: This should also mention removing or disabling unused applications or services.

Nit: What is DLS? Can we have a translation in the glossary?

Detect

Perhaps this is intended in DE.AE-1, but it is not clear: the baseline needs to include more than just information technology systems. It needs to include a baseline that can integrate anomalies and events reported from non-cybersecurity sources. Such sources, such as IT Help Desk, police, human resources, etc. may even deliver the reports electronically, enabling automated action and sharing.

Most of the Detect function appears to be in checklist language. However, the sub-categories, as written are not actionable. What does it mean that “malicious code is detected” (DE.CM-4) or “unauthorized mobile code is detected” (DE.CM-5)? It is an aspiration to detect trouble, but is not the point of the framework to get the organization into a posture where it is *possible* to *detect* the anomaly? Clearly, an organization fails if there is malicious code in its network and it does not detect it. However, what does it mean for the framework if there is no malicious code to detect? How would an organization measure itself against these sub-categories?

Penetration testing would not be sufficient, as that, by definition, uses known attacks.

At the least, these sub-categories need to be reworded to discuss monitoring and what action to take when detected.

Respond

Following the previous comment, what does it mean that a “response plan is implemented during or after an event”? It is great that we want organizations to have a plan and then execute the plan, but is there any meaning for an organization to say it really would like to execute on a plan it spent time, money, and other resources to create? Is this part of a checklist: analyze, detect, respond, act? Does this need saying? If we do need to say it and provide such a basic checklist, our critical infrastructure sectors have much larger problems!

In fact, the whole Respond Function area reads like a checklist. Is this what we want the *Proposed Framework* to be? See, e.g., RS.PL-1, RS.AN-1, RS.AN-3, etc.

Saying at the Respond function that notifications are investigated (RS.AN-1) is a bit late in the process. How is this different from the Detect function?

Stating “forensics are performed” (RS.AN-3) is a function without a goal. What does this checklist item mean? One thing that is missing is a framework item that organizations may need to retain forensic data. However, this is also a sector-, threat-, and organization-specific item. Some sectors may need to retain forensic data for years, while others may need to retain it for minutes. The framework needs to inform organizations that they may need to have a process and a policy for retaining and protecting incident artifacts.

RS.MI-2: What does it mean for “incidents are eradicated”? Can an incident be eradicated? Does this mean we change history and make the incident go away as if it did not happen? **Vulnerabilities** can be eradicated. An **incident** can be remediated. Perhaps we have an ontology problem: just what is an incident in this context?