McCARTER
&ENGLISH
ATTORNEYS AT LAW

December 12, 2013

Mr. Adam Sedgewick
Information Technology Laboratory,
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899-8930

RE: Comments on the NIST Preliminary Cybersecurity Framework

J. Wylie Donald
Partner
T. 302-984-6361
F. 302-220-4608
jdonald@mccarter.com

McCarter & English, LLP
Renaissance Centre
405 N. King Street, 8th Floor
Wilmington, DE 19801-3717
T. 302.984.6300
F. 302.984.6399
www.mccarter.com

Dear Mr. Sedgewick:

I write to provide comments on the NIST Preliminary Cybersecurity Framework as requested in the October 29, 2013 *Federal Register*. By way of background, I am a practicing lawyer with over twenty years of experience and a partner in the Insurance Coverage Group at the law firm of McCarter & English, LLP. A large proportion of my practice has been focused on the representation of policyholders in connection with their commercial insurance coverage, including what is commonly known as cyberliability insurance. I focus my comments on that topic.[1]

The "Notes to Reviewers" segment in the Preliminary Framework asks, among other things:

> Does the Preliminary Framework appropriately integrate cybersecurity risk into business risk?
>
> Does the Preliminary Framework provide the tools for senior executives and boards of directors to understand risks and mitigations at the appropriate level of detail?

It is my view that the Framework currently fails to frame adequately the answers to these two questions because it completely fails to address insurance. A search for that term in the Preliminary Framework yields the null set.

A simple paradigm for addressing risk (the subject of both of the questions) is an assessment of the risk and then a decision to accept, avoid, mitigate or transfer the risk. Insurance is one half of the transfer portion of the paradigm (indemnification is the other half). It is not to be confused with self-insurance, which is the acceptance of a risk, rather than its transfer.

[1] The views expressed here are my own views and should not be considered to be those of McCarter & English, LLP, nor of any clients of the firm.

It also should be recognized that an unavoidable part of every insurance risk transfer is risk acceptance. This comes in the form of deductibles and policy limits; that is, losses below a certain value, as well as those above a certain value, are retained by the insured. But it also includes the very terms and conditions of the insurance contract, which determine whether the materializing risk is covered. Exclusions limiting coverage for risks are the simplest example of this, but one must acknowledge that definitions, reporting obligations, insuring agreements, and a whole host of other terms can also work contractually to limit the actual transfer of risk.

Every cyber risk will be addressed by one of the four paradigm options: accept, avoid, mitigate or transfer. More precisely, various aspects of a risk will be addressed by a combination of the options. The risk of improper access to an organization's computer systems, for example, is mitigated through the use of passwords. The chance that passwords will be compromised may be accepted, or it may be transferred under a cyber insurance policy. The application of the paradigm will occur whether the risk is known or unknown, large or small, simple or complex.

Use of the Framework will result in certain risks shifting from one paradigm option to another. For example, where an organization is unaware of a risk to which it is subject, it is very likely that the organization will have (unknowingly) accepted the risk. However, if the Framework is implemented, then under the "Identify" function of the Framework Core Functions, the risk will be identified, at which point the organization will be able to avoid, mitigate or transfer the risk, if it concludes it is unwilling to accept it.

As another example, an organization that chooses to put its data in the "cloud" avoids the risk of inadequate hardware and software maintenance by its employees. This, of course, leaves open the question of who bears the risk of inadequate hardware and software maintenance by the cloud vendor's employees. The organization will attempt to ensure that that risk remains with the cloud vendor through an indemnification running from the vendor, or through insurance purchased by the vendor, or even both. In fact, if the vendor is unable or unwilling to provide indemnification or insurance, the organization may conclude that the risk is not appropriately transferred to the vendor.

The need for insurance arises in many circumstances. Many who read these comments will be familiar with RSA Security's hacking problem with its SecurID token. Companies using these tokens without a promise of indemnification from RSA if something went wrong, may have wished for adequate insurance coverage if the problem with RSA's tokens brought their business to a standstill. Indeed, where an organization cannot afford to address the occurrence of a particular risk through its own resources, where available, insurance is the universal solution for those risks. But even where the materialization of a risk is not the end of the world for the

organization, transfer by insurance may still be the chosen paradigm option because it is the most cost-effective way to address the risk. Shifting to the commonplace, we know there are many hazards on the highway, yet we do not all drive only the cars with the latest safety technology, or drive less, or not drive at all; instead, we buy insurance.

These ideas appear to lurk behind the Framework. In section 1.2 the Preliminary Framework states: "Risk management is the process of identifying, assessing, and responding to risk. . . . [O]rganizations determine the acceptable level of risk for [information technology] and [industrial control systems] assets and systems, expressed as their risk tolerance." One of the results of this process is to "enable organizations to optimize cybersecurity expenditures."

Because insurance is so central to how an organization responds to risk, it should be expressly included in any framework focused on addressing a class of risks, including a cyber risk framework. At least four of the Framework Core Functions ("Identify", "Detect", "Respond" and "Recover") could capture some aspect of the role of insurance. For example, in the Framework's Appendix A, under the Identify Core Function, the Asset Management category is set forth as a focus:

> The personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.

While "system" is a broad enough term to capture insurance, and insurance is undoubtedly a part of an organization's "risk strategy," based on the subcategories describing Asset Management insurance is not intended to be included. Similarly, a Risk Management Strategy category is included in the Identify Core Function, but again insurance is omitted from each of the identified subcategories. This same routine could be used to examine other elements the Framework sets out under other functions; in many cases it could be shown that insurance has a role but is omitted.

This failure expressly to include considerations about insurance in the Framework is not merely a theoretical problem. My colleague, Jennifer Black Strutt, and I have focused directly on the interplay of insurance and government notifications of cyber threats (which might fall under the Detect function subcategory of "Event detection information is communicated to appropriate parties."). I state below some thinking we published in the Edison Electric Institute's publication, *Electric Perspectives*. A complete copy of the article is attached.

On February 12, 2013, the Obama Administration issued Executive Order 13636 – Improving Critical Infrastructure Cybersecurity, which establishes a voluntary set of

security standards for critical infrastructure industries. One of the primary objectives of the Order is the dissemination to critical infrastructure entities of notification that they may be the targets of cyber threats. However, it is unclear what information will be provided to an entity pursuant to the Order. Dr. Andy Ozment, the White House Director for Cybersecurity, provided comments at the 2013 Armed Forces Communications & Electronics Association's 4th Annual Cybersecurity Symposium that offered little guidance. Dr. Ozment indicated that, although the government recognizes the need to broadly share information, "information sharing is complicated for the government."

While sharing information can prevent the realization of certain threats, sharing the same information too broadly may provide the sources of the cyber threats (hackers, cyberactivists, criminals, corporate spies and foreign intelligence services) the opportunity to modify their behavior. Thus, indiscriminate dissemination of information may make it even harder to prevent a cyber attack.

Indiscriminate dissemination can be controlled with security clearances (an application by the government of the mitigation option of the paradigm). However, as Dr. Ozment advised, the government "can't give a clearance to everybody who needs to understand cybersecurity and operate to defend their critical infrastructure." Thus, even though there is a demonstrated need for the information, it may not be forthcoming. Instead of the details necessary to prepare for and prevent a crippling cyber attack, a critical infrastructure entity might find itself the recipient of a vague and incomplete notification that lacks the specificity necessary to take concrete actions to turn away the attack. Alternatively, the organization may meet the security requirements to receive detailed classified reports, but those details may be restricted from dissemination outside the organization. Failure to abide by those restrictions could result in severe penalties or even imprisonment.

What happens if the security threat becomes an actual attack? Prudent organizations will have procured insurance and will have implemented steps to address the cyber threat. Thus, in many cases, the organization will be able to defeat the attack with few or no ill effects. But, as a matter of statistics, some organizations will find all their defenses unavailing. In those cases, the organization's insurance policy may be able to take the sting out of the attack. But if the organization failed to give its insurer timely notice, the organization may find itself the recipient of a denial of coverage.

Over fifty different carriers offer cyber coverages as either stand-alone policies or as enhancements to other standard policies. A simple definition of cyber insurance is an insurance contract that covers financial losses arising from computer or network-based incidents. Limits in some cases can exceed $100 million although many policies are much smaller. Coverage is "claims-made," meaning the policyholder must report a covered claim to the insurer within the policy period or an extended

reporting period (if applicable). The requirement that a policyholder provide timely, written notice of the claim is usually a condition precedent to coverage.

Policies also may ask the policyholder to provide notice of circumstances likely to give rise to a claim – i.e., a "notice of circumstances." Often, a notice of circumstances is optional, but, on occasion insurers have argued (and courts have found) that a notice of circumstances is required for coverage.

Under a "notice of circumstances" requirement, an organization faced with a cyber threat, for example, may be expected to provide written notice that describes the circumstances of the threat and the consequences that may result, identifies the potential claimants, and explains how the organization learned of such circumstances. Court decisions have penalized insureds that fail to provide sufficient detail concerning the potential claim. Once this information has been provided to the insurer, a claim that later arises from those circumstances will be covered under that policy. This may be of significant benefit to the organization because future exclusions or other limitations of coverage such as higher deductibles or lower limits will not apply to that claim.

If an organization receives a warning from the government about an expected cyber threat, the organization must determine whether and how to provide notice to its insurer. If the government provides specific information about the threat, the organization - theoretically - is able to provide the level of detail required for a notice of circumstances. However, in practice, the organization may be restricted from doing so. It is very possible, even likely, that the government's detailed information will be classified, and the transmission of such information to anyone who does not have a security clearance may result in fines and imprisonment. Obviously, if the organization possesses this information, but does not provide the insurer with a notice of circumstances as the policy requires, the organization risks having its subsequent claim denied.

Even if the notice of circumstances is not mandatory under the policy, the organization's failure to provide written notice of circumstances may subject the organization to a future denial of a subsequent claim. For instance, if the claim arises after the policy has been renewed, the insurer may deny the claim based on the "known loss" doctrine – i.e., the insurer will argue that any subsequent loss was not by chance, which is a fundamental requirement of insurance.

The organization may be in a difficult spot even if the governmental notice is not classified. As Dr. Ozment suggested, unclassified information from the government may be vague. As a result, the organization may not possess the level of detail required to comply with the policy's requirement for a notice of circumstances. Indeed, it is likely that a vague report from the government will not enable the organization to describe the circumstances of the potential threat, the likely consequences, or the expected plaintiffs. As a result, the notice of circumstances

may not be sufficient to trigger coverage under the policy when the claim ultimately comes in.

Additionally, the organization should expect that the insurer will consider the cyber threat disclosed in the notice of circumstances during renewal of the policy. Specifically, the insurer may add new exclusions, lower the limit, raise the deductible or increase the premium based upon the possible threat. If the incomplete notice of circumstances is insufficient to trigger coverage for a subsequent claim, but causes the insurer to provide more limited future coverage at a higher price, the organization is harmed without any benefit.

In sum, the organization may be in an impossible situation, regardless of whether the government's report is classified or unclassified and whether the policy's request for a notice of circumstances is optional or required for coverage.

This focused discussion demonstrates the interplay of an organization's response to a cyber threat with its insurance. With this background, we can return now to the questions posed at the beginning,

> Q. Does the Preliminary Framework appropriately integrate cybersecurity risk into business risk?
>
> A. No, because insurance is a central element of how businesses address risk and the Preliminary Framework does not include it.
>
> Q. Does the Preliminary Framework provide the tools for senior executives and boards of directors to understand risks and mitigations at the appropriate level of detail?
>
> A. No, because the Preliminary Framework provides no basis for executives to understand how one of their primary risk management tools, insurance, fits into a comprehensive program to address cyber risk.

Addressing, as the Framework does, cyber issues without including insurance increases the chances that the responses developed will have unforeseen and negative impacts on an organization's total risk management program. Accordingly, it is my belief that the final Cybersecurity Framework should expressly include insurance as an activity addressed by some or all of the Core Functions.

Thank you for your consideration.

Sincerely,

J. Wylie Donald *
* Admitted in NJ, MD, NY, DC, FL, PA and MA

JWD/blh

Enclosure