WILLIAM H. WIDEN
PROFESSOR OF LAW
[redacted]

[redacted]

November 6, 2023

National Institute of Standards and Technology
U.S. Department of Commerce
100 Bureau Drive
Gaithersburg, MD 20899

TRANSMITTED VIA EMAIL: cyberframework@nist.gov

Comments on Cybersecurity Framework 2.0 Draft of August 8, 2023

Please find attached my comments on the above-referenced draft. A version of these comments appears on the Social Science Research Network (SSRN). Any updates to my reflections on this draft will appear at the below link: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4624868 .

I appreciate the chance to comment on this draft which takes the very important step of adding a GOVERN function to the framework.

As you will see, my comments focus on suggestions to further implement the proper inclusion of the GOVERN function into the framework to enhance useability of the framework by boards of directors, senior executives and legal advisors who have little or no cybersecurity background or experience. The key point is to place increased emphasis on the important role of "oversight" as that concept is understood in business and legal circles. This includes an express requirement for those in charge of governance and oversight in an organization to select a management model, align compensation and incentives with cybersecurity goals and address potential internal conflicts of interest which may adversely affect the supply chain.

I would welcome any questions on the attached comments.

Very truly yours,

/s/ WILLIAM H. WIDEN

William H. Widen

UNIVERSITY OF MIAMI SCHOOL OF LAW RESEARCH PAPER

CORPORATE GOVERNANCE, CYBERSECURITY & OVERSIGHT:

A COMMENT ON NIST'S PROPOSED FRAMEWORK 2.0 FOR CYBERSECURITY

WILLIAM H. WIDEN[*]

NIST's public draft of Cybersecurity Framework 2.0 takes the important step of adding a GOVERN function to the framework. This comment recommends that Framework 2.0 start by explicitly identifying the overriding management challenge for cybersecurity—

> ***How does an enterprise effectively govern, manage, and oversee cybersecurity measures when those in governance and senior management positions have little or no cybersecurity expertise?***

The current draft places insufficient emphasis on the corporate law concept of "oversight." This comment makes various textual suggestions that might improve the useability of the framework for its intended audience—which includes boards of directors, executives, and lawyers—by adding "cybersecurity risk oversight" as a keyword to the framework, with appropriate conforming changes that place greater emphasis on the details of the type of oversight required by corporate law. The importance of the oversight role emerges from the essay's consideration of the details of claims made in lawsuits filed against corporate directors for oversight failures (e.g., against Boeing for the 737 Max crashes). Revisions to improve useability by a business and legal audience are needed because other important publications, such as the March 2021 World Economic Forum's Insight Report on Principles for Board Governance of Cyber Risk recommend consideration of a prior version of the NIST framework which did not include a GOVERN function. Increased focus on oversight includes specifically addressing potential internal conflicts of interest in supply chains, aligning compensation with cybersecurity, and limiting the optional nature of the recommendations.

[*] William H. Widen is a Professor at the University of Miami School of Law. He researches laws and regulations relating to autonomous vehicles. He formerly practiced corporate law as a partner at Cravath, Swaine & Moore in NYC.

Contents

1. INTRODUCTION

MANY "frameworks" recommend that companies follow specified corporate governance procedures to promote safety and security in the use of advanced technology.[1] A recent example of appeal to corporate governance appears in the initial public draft of National Institute of Standards and Technology (NIST) Cybersecurity Framework 2.0.[2] [hereinafter the "Draft" or "Framework 2.0"]

The below remarks apply to NIST's request for comments due November 6, 2023,[3] on the Draft posted for public comment on August 8, 2023. The request by NIST for comments presents an opportunity to evaluate the general corporate approach to management oversight of safe technology use, development, and distribution in the context of cybersecurity.

Ideally, NIST would include the recommended changes below in the text of Framework 2.0. However, in the absence of textual changes, these comments can serve as a guide which an enterprise might use to help implement the recommendations of Framework 2.0. Inclusion of changes into the text is preferred because the large and growing number of published frameworks already pose the daunting management challenge of coordinating various recommendations. The multiplicity of resources creates a risk of "information overload."[4]

[1] *See, e.g.*, World Economic Forum, Principles for Board Governance of Cyber Risk, Insight Report (March 2021) (in collaboration with PwC). Cybersecurity efforts include approaches other than corporate governance, such as DARPA's Artificial Intelligence Cyber Challenge (AIxCC), https://aicyberchallenge.com/. Some guidelines apply to parts of an enterprise, such as a chief security officer. *See infra* note 4.

[2] NIST Cybersecurity Framework 2.0. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) NIST CSWP 29 ipd (2023). https://doi.org/10.6028/NIST.CSWP.29.ipd.

[3] Originally due on November 4, 2023.

[4] For example, the Automotive Information Sharing and Analysis Center (Auto-ISAC) has many best practices guides. *See, e.g.*, Auto-ISAC, Automotive Cybersecurity Best Practices, Executive Summary (July 1, 2019), https://automotiveisac.com/best-practices. NHTSA published Cybersecurity Best Practices for the Safety of Modern Vehicles Updated 2022 (Sept. 2022). *See also* Cybersecurity & Infrastructure Security Agency (CISA), Autonomous Ground Vehicle Security Guide: Transportation Systems Sector (listing numerous additional CISA resources for chief security officers and chief information security officers), https://www.cisa.gov/sites/default/files/publications/Autonomous%2520Ground%2520Vehicles%2520Security%2520Guide.pdf.

A. The Central Management Challenge

Framework 2.0 should start by identifying the central and most critical management challenge for cybersecurity:

> **How does an enterprise effectively govern, manage, and oversee cybersecurity measures when those in governance and senior management positions have little or no cybersecurity expertise?**

Recognition of this challenge should guide use of Framework 2.0. Explicit identification of this central management problem at the outset will aid users of Framework 2.0 in their use of other related resources because lack of cybersecurity expertise presents a different kind of challenge which is best addressed by keeping the central problem in focus.

ADD text | Lines 3-9:

> It offers a taxonomy of high-level cybersecurity outcomes that can be used by any organization — regardless of its size, sector, or maturity — to better understand, assess, prioritize, and communicate its cybersecurity efforts. **Use of the Framework will assist those with little or no cybersecurity expertise to govern, manage, and oversee cybersecurity measures within an enterprise**. The Framework does not prescribe how outcomes should be achieved. Rather, **it describes structures and procedures helpful to overcoming a lack of expertise to address knowledge and responsibility gaps within an organization and** it maps to resources that provide additional guidance on practices and controls that could be used to achieve those outcomes.

Cybersecurity management differs from more traditional financial, product and service management challenges faced by board members and senior executives because those persons typically have background expertise in executive leadership, financial management, accounting and the products and services offered by their enterprise.[5] In the complex area of cybersecurity, in most organizations this background expertise is lacking—particularly at senior levels.

Corporate structure and lines of reporting must effectively address this knowledge gap (in addition to providing basic enterprise information through reporting channels) so that senior management can responsibly govern, manage, and oversee cybersecurity efforts.

[5] Though these comments focus on usability of Framework 2.0 by private industry, administrators of different regulatory agencies and branches of government face similar substantive knowledge gaps.

Understanding that corporate structure must address a substantive knowledge gap (and not merely convey information at an appropriate level of detail) should guide use of Framework 2.0.

The below comments aim to address the central management challenge for implementation of effective cybersecurity measures by recommending changes intended to make Framework 2.0 more accessible for use by boards of directors, senior executives and their advisors who are not cybersecurity professionals.

B. Target Audience for Framework 2.0

Per the Draft, the intended audience for Framework 2.0 includes private industry, and specifically mentions "executives." [Lines 78, 124] Elsewhere, the draft describes its target audience as including "executives, boards of directors ... [and] lawyers." [Lines 152-153] The draft aspires to be useful to those "who may not be cybersecurity professionals. [Line 79] Most board members, senior executives and their legal advisors will not have cybersecurity expertise—which creates the central management challenge in the first place.

To reach this audience, the draft should use language and concepts best suited to communicate with those in management positions at organizations, including those trained at business and law schools, and others conversant with the literature of corporate governance and management models.

Success of a cybersecurity management program will depend on careful selection of management structures and channels of reporting to facilitate board oversight. During the revision process, NIST should consider making more express references to terms this target audience might use to discuss corporate governance and management among themselves.

C. General Nature of Suggested Revisions

To make the revised Framework more user friendly for persons important to its successful implementation, Framework 2.0 should first stress the importance of the concept of *oversight* as part of enterprise governance; second, clarify the priority and timing of use of the newly added GOVERN function (including specification of a management model), and third elaborate on implementation of oversight in managing cybersecurity.

2. THE GOVERN FUNCTION

A. Addition of the Govern Function

The most significant structural change in Framework 2.0 is the addition of the GOVERN function which touches upon every other function in Framework 2.0. By addition of GOVERN, NIST has correctly made a change critical to effective cybersecurity efforts in organizations of all types. The Draft should, however, build further on this key insight. Using concepts from corporate governance will greatly assist this build-out for all types of enterprises.

The summary of changes at the beginning of the Draft states:

● **Emphasize cybersecurity governance**:

> o *New Function, Govern*, added to cover organizational context; risk management strategy; cybersecurity supply chain risk management; roles, responsibilities, and authorities; policies, processes, and procedures; *and oversight*. **[emphasis supplied by ital. and underline]**
>
> o New guidance offered on integrating the Framework with the NIST Privacy Framework and with enterprise risk management as discussed in NIST IR 8286.
>
> o Focus on people, process, and technology expanded throughout the implementation of the Framework.

While NIST takes the important step of including a new GOVERN function in Framework 2.0 and recognizing the role of oversight, the Framework needs to better highlight the importance of *oversight by the board of directors* (or equivalent) for maximum impact.

The Court of Chancery of Delaware recently noted the enhanced oversight role of directors in cybersecurity in *Firemen's Retirement System of St. Louis on behalf of Marriott International, Inc. v. Sorenson*.[6]

> Delaware courts have not broadened a board's *Caremark* duties to include monitoring risk in the context of business decisions. Oversight violations are typically found where companies—particularly those operating within a highly-regulated industry—violate the law or run afoul of regulatory mandates. *But as the legal and regulatory frameworks governing cybersecurity advance and the risks become manifest, corporate governance must evolve to ad-*

[6] 2021 WL 459377 (Del. Ch. 2022) (not reported in Atl. Rptr.).

> *dress them. The corporate harms presented by non-compliance with cybersecurity safeguards increasingly call upon directors to ensure that companies have appropriate oversight systems in place.* **[emphasis supplied by ital. and underline]**

To avoid liability in a corporate setting, directors must make a good faith effort to put a reasonable compliance and reporting system for cybersecurity risk governance and cybersecurity risk management in place. Effective oversight by any organization (corporate or otherwise) begins with the conscious selection of a management model to implement compliance and reporting.[7]

The target corporate audience will have familiarity with various management models (e.g., top-down, bottom-up) and the legal concept of *oversight* by a board of directors, including the steps needed to avoid a lawsuit by shareholders claiming a failure of oversight. Importantly, these steps to avoid legal liability for a failure of oversight include actions which will enhance cybersecurity as a byproduct of the goal of director liability limitation.

B. Emphasizing the Oversight Role

A common description of corporate governance structure is that the board of directors *governs* the organization, while executives *manage* the organization. The chief executive officer is the conduit and coordinator between the board of directors and the other executives. The Draft reflects this difference between governance and management by recognizing *cybersecurity risk governance* and *cybersecurity risk management* as discrete keywords. [Lines 11-12]

Though governance is often contrasted with management, the primary role of the board of directors is *oversight* of management. **The Draft does not place enough emphasis on the oversight role**. The board of directors has this oversight role as a matter of fiduciary duty imposed by corporate law as interpreted in court decisions and orders.[8]

[7] *See infra* suggested textual changes at Lines 180-184.

[8] Stock exchange rules, and federal and state laws and regulations may expand upon oversight responsibilities or provide additional details for oversight structure. Part of oversight requires establishing compliance structures to meet these obligations. Details of compliance with these requirements, however, is beyond the scope of these comments.

As part of adding the GOVERN function to Framework 2.0, the revision should add the phrase "cybersecurity risk oversight" as a keyword and use that concept when appropriate.

ADD Text | Lines 10-13:

> **Keywords**
>
> cybersecurity; Cybersecurity Framework; cybersecurity risk governance; cybersecurity risk management; **cybersecurity risk oversight;** cybersecurity supply chain risk management; enterprise risk management; Privacy Framework; Profiles **[add bold underline]**

COMMENT | In the existing Draft, the description of the GOVERN function explicitly mentions "*oversight* of cybersecurity strategy" [Line 200; emphasis supplied by italics] but this does not capture the comprehensive oversight needed from a legal perspective to implement the GOVERN function because "cybersecurity strategy" might be interpreted as having a limited scope. Moreover, the Draft does not clearly place this oversight role on the board or one of its committees.

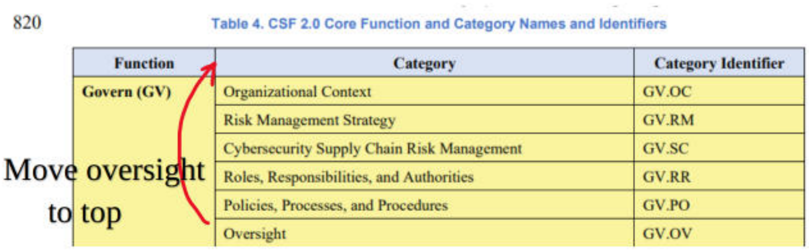
Though the oversight of cybersecurity risks across supply chains also is mentioned as important [Lines 550-551][9] this is only one aspect of the needed oversight corporate law requires. The law requires a good faith effort to create a reasonable compliance and reporting system for cybersecurity risk governance and cybersecurity risk management with comprehensive coverage—not just with a focus on strategy or supply chains.

The inclusion of "Oversight" and its Category Identifier "GV.OV" in Table 4 [Line 820 & ff.] without further elaboration is not sufficient because performing the degree of oversight required by corporate law is not merely a legal requirement in the abstract. Oversight is the primary activity in governance and should appear first.

CHANGE | Appendix C. Framework Core. Table 4. At Line 820 and ff.:

> Place "Oversight" as the lead Category in the Govern (GV) Function.

[9] "The Framework can be used to foster an organization's *oversight* and communications related to cybersecurity risks with stakeholders across supply chains." **[emphasis supplied]**



820

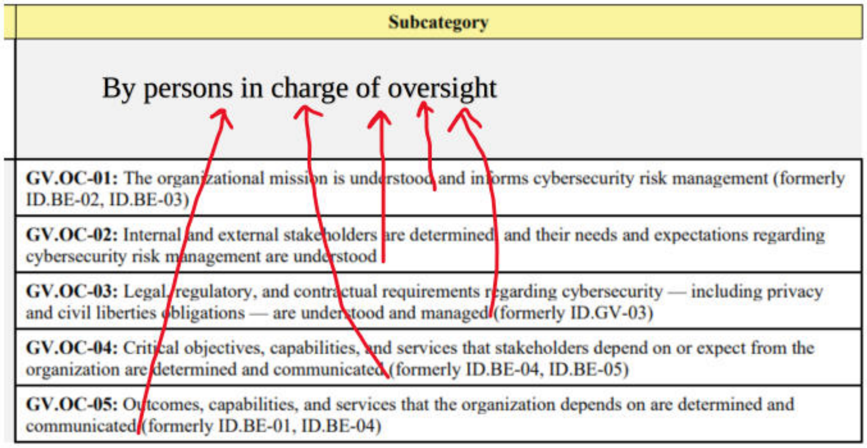
Table 4. CSF 2.0 Core Function and Category Names and Identifiers

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Cybersecurity Supply Chain Risk Management	GV.SC
	Roles, Responsibilities, and Authorities	GV.RR
	Policies, Processes, and Procedures	GV.PO
	Oversight	GV.OV

Move oversight to top

Additionally, the revision process should consider whether "Risk Management Strategy" should instead be referred to as "Risk Management Model" or whether selection of a *general* management model should appear as an additional category.

For a business and legal audience, the elaboration on "Oversight" in Table 5 [At Line 820 and ff.] may miss the mark. Indeed, of the six categories listed under Function | Govern (GV), Oversight is listed last and yet there is a board oversight role for each of the previous five categories under GOVERN. For example, persons responsible for oversight within an enterprise must oversee each of the activities under "Organizational Context".



Subcategory
By persons in charge of oversight
GV.OC-01: The organizational mission is understood and informs cybersecurity risk management (formerly ID.BE-02, ID.BE-03)
GV.OC-02: Internal and external stakeholders are determined and their needs and expectations regarding cybersecurity risk management are understood
GV.OC-03: Legal, regulatory, and contractual requirements regarding cybersecurity — including privacy and civil liberties obligations — are understood and managed (formerly ID.GV-03)
GV.OC-04: Critical objectives, capabilities, and services that stakeholders depend on or expect from the organization are determined and communicated (formerly ID.BE-04, ID.BE-05)
GV.OC-05: Outcomes, capabilities, and services that the organization depends on are determined and communicated (formerly ID.BE-01, ID.BE-04)

One reason to include an oversight component, situate it under governance, require the board (or its equivalent) to perform this role, and elaborate upon oversight is to involve board members directly in cybersecurity risk oversight at a reasonable level of technical detail—which can then be communicated through the CEO to executives and engineers *as a board directive* to address specific questions. This will have the beneficial effect of symbolically conveying the importance of cybersecurity initiatives throughout the organization by starting at the top level of governance. For example, see the chart in Figure 6 following Line 452 which lists “risk governance” above “risk management”.

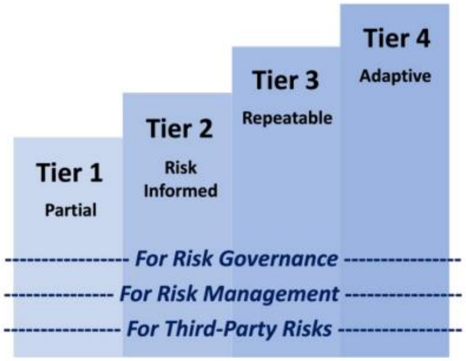


Fig. 5. Cybersecurity Framework Tiers

C. Primacy of the GOVERN Function

The Draft places the GOVERN function in the center of Fig. 2, which visually represents the NIST Cybersecurity Framework.

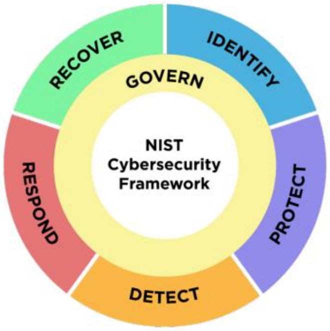


Fig. 2. Framework Functions

The Draft states:

> The GOVERN Function is cross-cutting and **provides outcomes to inform how an organization will achieve and prioritize the outcomes of the other five Functions** in the context of its mission and stakeholder expectations. [Lines 193-195] **(emphasis supplied in bold)**

The emphasized language suggests the primacy of GOVERN because the GOVERN function must be run first if it is to provide “outcomes to inform” implementation of the other five functions. Moreover, the Draft discusses the GOVERN function first and states that “[t]he ordering of the Core is intended to resonate most ***with those charged with operationalizing risk management*** within an organization." [Lines 182-184] **(emphasis supplied in bold)** By its structure, the Draft should expressly prioritize the GOVERN function which it currently does not do.

The Draft is unclear which persons within a typical enterprise would be charged with "operationalizing risk management" for an organization because the term "operationalizing risk management" does not have an accepted reference which identifies persons within an organization. **If the intended reference is to middle management, that misses the mark**. To be effective, the Framework's language and structure should first and foremost resonate with the board of directors and senior executives so that the Framework can guide them in their oversight roles to insure appropriate enterprise structures and lines of reporting.

D. Timing of Exercise of the Govern Function

From a business and legal standpoint, an organization should engage the GOVERN function at a senior oversight level first, at least on a preliminary basis, so that the organization can use the outputs from that function to generate outputs from the other Framework Core Functions.

The Draft creates a concern because it sends mixed messages on the timing appropriate to run the different functions. Though the Draft gives timing guidance in one place, stating that outputs from the GOVERN function are "generally needed for preparing a Target Profile" (which would require running the GOVERN function first) [Line 369], the draft uses contradictory language elsewhere.

The Draft states: "the order of Functions, Categories and Subcategories in the Core is not intended to imply the sequence by which they should be implemented or their relative importance." [Lines 181-184] The Draft claims that "the Functions should be addressed concurrently" [Lines 234-235] and that they "should all happen continuously." [Lines 235-236]

A business and legal audience will likely have difficulty understanding the collective import of these statements. The current Draft's text sometimes seems to place all the described functions on a co-equal level even though its visual representation places the GOVERN function at the center of cybersecurity efforts which many will find confusing.

The Draft should be revised to clearly state that the GOVERN function is the primary function which guides the implementation of the other five functions and that the GOVERN function should be addressed first by selection of a management model and second by oversight of selection of a cybersecurity risk management model.[10] The Draft should add more details to describe the scope of the GOVERN function, including reference to typical governance functions relating to alignment of compensation with cybersecurity goals and to managing conflicts of interest.

CHANGE | Lines 180-184:

> **An organization should implement the GOVERN function first.** ~~Additionally,~~ **With the exception of the initial implementation of the GOVERN function,** the order of Functions **(including iterative uses of GOVERN)**, Categories, and Subcategories in the Core is not intended to imply the sequence by which they should be implemented or their relative importance. The ordering of the Core **by placing the GOVERN function first, and locating it centrally in the graphic depiction of Framework 2.0,** is intended to resonate most with **a board of directors and other senior executives (or their equivalents)** ~~those~~ charged with **oversight of those persons** operationalizing risk management within an organization. **They are structured to facilitate effective communication between those performing cybersecurity risk governance/cybersecurity risk oversight and those involved in active cybersecurity risk management.**

CHANGE | Lines 197-200:

> GOVERN directs **a board of directors (or its equivalent) to develop** an understanding of organizational context **(including the identification of cybersecurity knowledge gaps and gaps in responsibility for cybersecurity risk management with respect to enterprise assets and systems**); ~~the establishment~~ **to establish a management model for cybersecurity risk oversight within which** cybersecurity strategy and cybersecurity supply chain risk management **will occur and to oversee the selection of a cybersecurity risk management model**; **to review** roles, responsibilities, and authorities; **to develop** policies, processes, and procedures; and **to conduct** the oversight of cybersecurity**, including cybersecurity risk** strategy. **Development of policies, processes, and procedures should consider aligning compensation and bonuses with achievement of cybersecurity goals, as well as addressing potential conflicts of**

[10] *See infra* text accompanying note 14.

> **interest which may interfere with effective cybersecurity management. Failure to address compensation incentive structures and conflicts of interest may create responsibility gaps.**

i. Selection of Management Models

An important part of implementing the GOVERN function should be selection by the board of directors of a management model to guide cybersecurity efforts, including a written description for use throughout an organization. Businesspersons refer to management models with labels such as *top-down*, *bottom-up* and *command and control*, etc. The draft does not sufficiently highlight the importance of this selection of a management model as part of the GOVERN function, though in several places it appears correctly to endorse a hybrid approach.

Use of a hybrid approach is particularly important to address the primary management challenge because members of the board of directors and senior executives need to receive input from line engineers and middle management to compensate for their own lack of cybersecurity expertise.[11] (In some cases, outside consultants and experts may play an important role by filling knowledge gaps.) Specification of a hybrid approach rather than a pure top-down approach is important because those in some industry sectors suggest that a top-down management model works best for development and management of complex technology.[12]

At Line 492, the draft recommends "foster[ing] bi-directional information flows" and references Fig. 6. Fig. 6 contains a graphic with an arrow figure that points up and down. Line 691 introduces a management concept of "iterative cycle of risk communication at all

[11] *Compare* Katherine C. Kellog, *How to Orchestrate Change from the Bottom Up*, HARV. BUS. REV. (Feb. 13, 2019)(discussing the importance of information flow from lower level workers up to management in an empirical study of hospitals), https://hbr.org/2019/02/how-to-orchestrate-change-from-the-bottom-up *with* Boris Groysberg & Michael Slind, *Leadership Is a Conversation*, HARV. BUS. REV. (June 2012) (discussing the importance of speaking with employees and not simply issuing orders), https://hbr.org/2012/06/leadership-is-a-conversation.

[12] For example, speakers at The Autonomous convention in September 2023 in Vienna, Austria (which I attended as a panelist) emphasized the importance of a top-down management model. At least for cybersecurity, a hybrid approach seems more appropriate to address lack of cybersecurity expertise. The annual Autonomous convention focuses on automated vehicle technology.

organizational levels." The draft seems to recommend use of a hybrid top-down/bottom-up management model when, in lines 494 to 496, it references "top-down dialogue" and "bottom-up reporting" as improving communications across an organization about cybersecurity.

If the draft intends to recommend a hybrid management model (which I think is appropriate), the place to first indicate selection of a management model as one output of the GOVERN function is somewhere in lines 192-200.[13]

The Draft should clarify and strengthen its endorsement of a hybrid management model.

ADD Text | Line 497:

> **Use of a hybrid top-down/bottom-up management model furthers the goal of Framework 2.0 by creating a management structure and lines of reporting which will assist those with little or no cybersecurity expertise to govern, manage, and oversee cybersecurity measures within an enterprise.**

Selection of a management model is separate and distinct from the selection of a cybersecurity risk assessment methodology as mentioned at Line 439, fn. 1. This also should be an output of the GOVERN function. The board should oversee the selection of a risk assessment methodology as well.[14]

The presumption should be that in a responsible organization the board will select a management model and oversee selection of a risk assessment methodology. The Draft should indicate that any determination not to do so must be supported by a compelling reason documented and approved by the board of directors. The observation that the "Framework offers an opportunity to explore or adjust methodologies for measurement and adjustment" is simply too weak. [Lines 438-439]

ADD Text | Lines 438-439:

> Framework offers an opportunity to explore or adjust methodologies for measurement and adjustment. **If the board of directors (or its equivalent) in any organization makes a determination not to expressly adopt a management model for cybersecurity or to oversee the selection of a cybersecurity risk methodology, it should**

[13] *See supra* textual comment on Lines 197-200.

[14] *Id.*

> **support such a determination by documenting compelling reasons supporting this decision.**

E. Relationship of Oversight Failures to Losses

Proper performance of the oversight role is directly related to avoiding adverse outcomes such as a cybersecurity breach. When plaintiffs sue public company directors the claims often allege an oversight failure. When an oversight failure occurs, one might infer that the governance structure in place failed to promote effective oversight and that this failure caused a loss or other adverse events for the company. That is the essence of the legal claim in the complaint.

The FTC used lessons learned from its cases to develop a guide for business.[15] That same approach works to inform enterprises about good practices for corporate oversight in a cybersecurity context reflected in court decisions and orders.

From a legal perspective, when a tragic or adverse event occurs in corporate life, plaintiffs file lawsuits against directors alleging liability for a failure of a duty, such as oversight. If a claim survives a motion to dismiss, that means a judge found that the claim potentially has merit. For this to be true, the failure of oversight must have a plausible causal connection to the tragedy or adverse event. Thus, cybersecurity governance should have an intense interest in avoiding failures of oversight and a description of the GOVERN function should consider the nature of these sorts of alleged failures by recommending corporate structures and lines of communication which would have avoided oversight failures in other tragedies.

F. Nature of an Oversight Failure Claim

In Boeing derivative litigation over the 737 Max crashes, the Delaware chancery court stated that "[s]tockholders have come to this

[15] Federal Trade Commission, Start with Security, A Guide for Business, Lessons Learned from FTC Cases (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

Court claiming Boeing's directors and officers failed them in overseeing mission-critical airplane safety to protect enterprise and stockholder value."[16]

The narrow question before the court decided in this memorandum opinion was whether the Boeing directors faced a substantial likelihood of liability for Boeing's losses. The court concluded that the stockholders had successfully pled two potential sources of board liability: a complete failure to establish a reporting system for airplane safety; and, on "turning a blind eye to a red flag representing airplane safety problems."

The plaintiffs' alleged several key lapses in oversight. First, no board committee had been assigned the specific task of overseeing airplane safety. Second, no committee description of responsibilities included mention of oversight for airplane safety. Third, the strong implication was that the audit committee had too much on its agenda to conduct proper oversight as the primary supervisor of all risk and compliance matters for the company.

This chancery court decision is consistent with a Delaware Supreme Court decision[17] in a case involving claims of oversight failure by the board of Blue Bell Creameries USA, Inc. for a recall of products following a listeria outbreak in 2015 in which three persons died. Stockholders suffered losses because of the resulting operational shutdown, and acceptance of a dilutive private equity investment needed to survive the liquidity crisis that followed the shutdown. The plaintiffs had alleged that Blue Bell "had no [board] committee overseeing food safety, no full board-level process to address food safety issues, and no protocol by which the board was expected to be advised of food safety reports and developments."

The legal responsibility of directors for oversight comes from the *Caremark* case[18] of 1996 in which Chancellor Allen stated: "[A] director's obligation includes a duty to attempt in good faith to assure

[16] In re The Boeing Company Derivative Litigation, Memorandum Opinion, C.A. No. 2019-0907-MTZ, at 1 (Del. Ch. Sept. 7, 2021), https://courts.delaware.gov/Opinions/Download.aspx?id=324120.

[17] Jack L. Marchand II v. John W. Barnhill, et al., C.A. No. 2017-0586-JRS (Del. 2019).

[18] In re Caremark International Inc. Derivative Litigation, 698 A. 2d 959 (Del. Ch. 1996). Older cases decided in the wake of *Caremark* tended to dismiss lawsuits claiming a failure of oversight (e.g., *In re Goldman Sachs Group, Inc. Shareholder Litigation* [2011], *Oklahoma Firefighters Pension & Retirement System v. Corba*t [2017], *City of Birmingham Retirement and Relief System v.*

that a corporate information and reporting system, which the board concludes is adequate, exists."

One lesson from these cases is that a corporate structure to effectively oversee and manage cybersecurity efforts may often require the designation of an executive officer in charge of cybersecurity efforts who reports to the board or a board committee (probably separate and distinct from the audit committee) with primary responsibility for cybersecurity oversight.[19]

The Draft should specifically direct the board to consider creation of an executive officer position in charge of cybersecurity management and the creation of a dedicated board committee to oversee the performance of that officer.

ADD Text | Line 200:

> **Consideration of roles under the GOVERN function includes consideration of allocation of workload among board committees and other groups within a management structure, with specific written designation of cybersecurity roles and responsibilities to groups within the management structure including possible use of an officer dedicated to cybersecurity management.**

Day to day active cybersecurity risk management ideally should be conducted by a dedicated officer and that officer should report to the board or a board committee designated as responsible for cybersecurity risk management. This oversight role should only be placed with the audit committee after careful consideration by the entire board of directors to make sure that within the context of the organization this responsibility does not overburden the audit committee.[20]

Good [2017]) but the case law is trending to expect more from directors. *See supra* text accompanying note 6.

[19] *Cf.* M.L. Cummings, *Identifying AI Hazards and Responsibility Gaps*, Computer ethics across disciplines: applying Deborah Johnson's philosophy to algorithmic accountability and AI (Noorman, M. E. & Verdiccio M., eds.) (Forthcoming in Springer Nature).

[20] For a description of the heavy workload of a typical audit committee, see Maria Castañón Moats, Stephen G. Parker, Tracey-Lee Brown, *Audit committee effectiveness: practical tips for the chair*, Harv. L. Sch. Forum on Corp. Gov. (Dec. 21, 2022), https://corpgov.law.harvard.edu/2022/12/21/audit-committee-effectiveness-practical-tips-for-the-chair/.

Both knowledge and responsibility gaps might be managed to an extent by having a central person in charge of cybersecurity.[21] As a point of comparison, Executive Order 13800 reinforces the Federal Information Security Modernization Act[22] by holding agency heads accountable for managing cybersecurity risks to their enterprises. It requires each agency to assess its cybersecurity risks and submit a plan to OMB detailing actions to implement the NIST Cybersecurity Framework.

4. USAGE OF CONVENTIONAL JOB TITLES & FUNCTIONS TO DESCRIBE ROLES IN AN ORGANIZATION

A concern about effective communication with the intended corporate audience arises because the current draft sometimes uses terms to describe a role, structure, or function in an organization with an uncertain meaning or reference for the intended corporate audience. Consider the following examples.

On the one hand, Line 270 uses the phrase 'technology *leaders*' to refer to persons *outside* the organization.

In other places, the term '*leader*' is used to refer to persons *within* the organization, and the draft introduces other terms. For example, the draft refers to "executive leadership" [Line 400], "leaders within the organization" [Line 402], "implementers" [Line 404], "mission-level planners" [Line 406], unspecified "leaders" [Lines 532, 689, 695], and "[e]nterprise leaders [Lines 686, 716].

These various references to "leaders" are in addition to terms used in related NIST documents—for example, in which "senior leaders" are described contextually:

> "The term enterprise level refers to the top level of the hierarchy where *senior leaders* have unique risk governance responsibilities."[23]

The concern arises because legal advisors to board members and senior executives (as well as the board members and executives

[21] Dr. Cummings stresses the importance of a central person responsible for safety and security of AI. *See supra* note 19. Knowledge and responsibility gaps are discussed *infra* at KNOWLEDGE & RESPONSIBILITY GAPS.

[22] *See* Federal Information Security Modernization Act of 2014, https://www.cio.gov/policies-and-priorities/FISMA/.

[23] Stephen Quinn, et al., NISTIR 8286B, Prioritizing Cybersecurity Risk for Enterprise Risk Management, NIST at p. v (Feb. 2022), https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8286B.pdf.

themselves) will struggle with the intended reference and scope of these different terms.

Clarification of the roles played by persons with different titles and job descriptions could be achieved by using specific reference to conventional positions and titles familiar in business and legal circles such as board members, chief executive officer, senior executives, and executives.

A. Generic Job Titles & Functions

NIST could take the clarifying step of adjusting its use of terms in the revision process by keeping before it a generic archetype of corporate governance and management structure terms and concepts used to describe positions and functions within an organization such as the following.

A board of directors typically includes both *inside* directors and *outside* directors. *Senior executives* typically report directly to the chief executive officer. The chief executive officer is the conduit between senior management and the board. Other executives appear in hierarchies of varying complexity, variable by organization, which culminate in a reporting obligation to a senior executive.

A board of directors has a chairman of the board. The chairman of the board may be the CEO or an independent outside director. Rarely, the chairman will be an insider director other than the CEO.

Inside directors include the chief executive officer (the CEO or, sometimes, the "president") and other senior executives responsible for important functions who report directly to the CEO, such as the chief financial officer (the CFO or, sometimes, the "treasurer"), and can include the general counsel and the chief records custodian (sometimes, the "secretary"). Often a single person holds several titles and performs several functions. Outside directors do not hold an executive office or other employment position within the organization though they may be significant shareholders.

Corporations sometimes intentionally blur the distinctions in position within the organization and function to avoid SEC reporting obligations with respect to certain persons and their compensation levels. One example is hiring an individual to run a significant aspect of the corporation pursuant to a management or consulting contract. However, even when a corporation blurs titles and job descriptions for reporting purposes, management and their legal advisors who will use Framework 2.0 understand the scope of responsibilities intended by references using conventional and generic terms.

B. Confusion About Roles and Management Titles

Confusion about the individuals in an organization appropriate to address different aspects of cybersecurity appears in numerous places.

At a general level, the Draft places "senior executives" at the top of the organizational chart in Fig. 6 above Line 498. Yet, in more traditional corporate governance terminology, the board of directors would appear at the top of an organizational chart. While senior executives would be involved in management activities, they would not be the persons setting mission objectives, enterprise risk appetites and priorities. Importantly, the board would oversee the "cybersecurity program" if that is an intended reference cybersecurity risk governance. Both the reference to "senior executives" and to "cybersecurity program" in Fig. 6 is ambiguous and potentially confusing given terminology used elsewhere in the Draft. Fig. 6 should be revised to correct the ambiguity.

But the confusion appears more broadly. For example, at Lines 686-688 the GOVERN function includes integrating governance with risk strategy by "enterprise leaders." Is the intended reference to the board, senior executives, or others? Integration of governance with risk strategy is properly a board function as part of oversight.

At Lines 689-690 the Draft indicates that "leaders" make informed decisions about the direction of the enterprise. It should be clear that these "leaders" are board members (perhaps members of a cybersecurity committee) who make decisions under the GOVERN function. The direction of the enterprise is properly a board function undertaken as part of an oversight role and not a matter left to middle managers.

At Lines 708-709, the Draft indicates that enterprise risk management (ERM) roles can be performed by an enterprise risk steering committee, senior executives, and officers. But this looks like it does not include board members. Is this intentional? Oversight of general risk management is a board role typically located in an audit committee. The important concern would seem to be making sure that the expectations of the board (or its enterprise risk management committee) articulated as part of the GOVERN function appear in cybersecurity risk management materials constituting an action plan.

ADD Text | Lines 708-710:

> Ensuring that expectations from those in ERM roles **at governance and oversight levels** (e.g., a board level enterprise risk steering committee~~, senior executives, and officers~~) are included in the analysis and prioritization **used by management (e.g. senior executives and officers)** to create an action plan (step 4)

5. Knowledge & Responsibility Gaps

A board without reasonable technical experience or, at least, information supplemented by educational efforts, cannot effectively oversee cybersecurity efforts. The recent Clorox crisis is instructive.[24] Clorox's 2023 Proxy Statement did not disclose any plans for a board technology committee and none of the twelve seated and nominated directors had meaningful technology experience.[25]

The SEC had proposed a rule that would have required a registrant to disclose the cybersecurity experience of members of the board of directors. In response to industry objections, however, the SEC did not include this reporting requirement in the final rules which became effective September 5, 2023. This decision to omit disclosure of cybersecurity expertise will prove an unfortunate one if its omission takes focus away from a necessary review of knowledge and competence gaps at an organization by the board of directors.

The Draft should provide that, as part of the GOVERN function, the board (or its equivalent) should expressly oversee the identification of cybersecurity gaps which should include an express reference to *knowledge gaps* within an organization as well as *responsibility gaps* for cybersecurity in the governance and management structure. Risks created by both types of gaps should be identified and addressed as part of the output of the GOVERN function.

ADD Text | Lines 108-110:

> ○ Determine where an organization may have cybersecurity gaps, including with respect to existing or emerging

[24] Noah Barsky, *Clorox Crisis Shows Cyber Risk's Harsh Business Downsid*e, Forbes.com (Oct. 6, 2023, 12:00pm EDT), https://www.forbes.com/sites/noahbarsky/2023/10/06/clorox-crisis-shows-cyber-risks-harsh-business-downside/?sh=7a5b84f3632b.

[25] *Id.*

> threats or technologies, and assess progress toward addressing those gaps. **A cybersecurity gap may exist based on a lack of knowledge or expertise within an organization or with respect to a failure to assign responsibility within an organization to manage a cybersecurity risk with respect to an enterprise asset or system. Failure to establish appropriate channels of communication between different departments or groups within an organization may create the equivalent of a knowledge gap (e.g., if the department in charge of cybersecurity differs from the department in charge of safety without a structure in which security is placed under safety or both security and safety report to a single officer).**

ADD Text | Lines 197-200:

> GOVERN directs **a board of directors (or its equivalent) to develop** an understanding of organizational context **(including the identification of cybersecurity knowledge gaps and gaps in responsibility for cybersecurity risk management with respect to enterprise assets and systems**); ~~the establishment~~ **to establish a management model for cybersecurity risk oversight within which** cybersecurity strategy and cybersecurity supply chain risk management **will occur and to oversee the selection of a cybersecurity risk management model**; **to review** roles, responsibilities, and authorities; **to develop** policies, processes, and procedures; and **to conduct** the oversight of cybersecurity**, including cybersecurity risk** strategy. **Development of policies, processes, and procedures should consider aligning compensation and bonuses with achievement of cybersecurity goals, as well as addressing potential conflicts of interest which may interfere with effective cybersecurity management. Failure to address compensation incentive structures and conflicts of interest may create responsibility gaps.**

A. Oversight: Special Challenges for Identification of Knowledge Gaps

Effective identification of knowledge gaps within an organization presents special challenges. Only 65% of executives rate their boards as having at least fair cybersecurity, data security and data privacy expertise. In contrast, 90% of directors think their boards understand cybersecurity and data privacy at least somewhat well.[26] Half of executives surveyed say "their boards *understand neither* the impact of digital technologies nor the climate strategy."[27] This suggests a lack of self-awareness by board members about the limits of their knowledge of cybersecurity issues.

In a May 2023 survey, 7% of CEOs had a concern that their board members did not understand the concerns of key stakeholders such as employees, customers, and regulators. In contrast, 56% of all C-suite executives believed their board members did not understand these key concerns. This suggests a lack of insight by CEOs about the limitations of the knowledge of their board members. The highest percentage of doubters existed among the chief legal officers and IT executives, at 69% for each group.[28]

Data which suggest that CEOs have an inaccurate perception of their board members' awareness of important issues for the organization, coupled with data which suggest that a large majority of chief legal officers and IT executives believe board members lack this understanding raise warning flags for effective cybersecurity risk management because legal and IT matters have significant bearing on managing this risk. Understanding the concerns of employees, customers and regulators is important for developing an effective cybersecurity risk management program. Framework 2.0 should thus emphasize the need for a probing self-examination to identify knowledge gaps so that they might be eliminated.

I would contrast the problem of cybersecurity risk management with addressing environmental, social and governance (ESG) issues, a topic which has been another recent focus for corporate boards. With ESG, there is a reasonable expectation that board members un-

[26] Governance Insights Center, *Board effectiveness: A survey of the C-suite*, THE CONFERENCE BOARD (May 2023), https://www.conference-board.org/pdf-download.cfm?masterProductID=46419.

[27] Maria Castañón Moats & Paul Washington, Report | There's a Wide Gap Between Boards and Management. How to Close It., The Conference Board (May 17, 2023)[emphasis supplied], https://www.conference-board.org/publications/barrons-wide-gap-between-boards-management.

[28] Merel Spierings, *Report | One Board, Many Stakeholders: Understanding Priorities*, THE CONFERENCE BOARD (June 15, 2023), https://www.conference-board.org/publications/board-effectiveness-many-stakeholders.

derstand what is being said—but some may not appreciate the significance of these issues or agree that the corporation should spend significant time or resources addressing them.[29]

In contrast, with cybersecurity risk management, at a certain level of abstraction, there is a reasonable expectation that board members understand its importance and the need for attention and resources. However, the concern remains that board members do not have sufficient technical understanding to make informed judgements about strategy. In many organizations, the existing board members are simply the wrong team to perform the needed oversight function without some technical education and information which would allow proper performance of the oversight role.

An organization might address a cybersecurity knowledge gap at the board level in several ways. One approach might add specialist directors to the board (though there are likely not enough specialists to populate all the boardrooms who might benefit from specialist directors). Another might replace some existing board members with new members who have more technical expertise. A review might propose new director nominees at the time of director elections to address gaps. A third approach might be for the organization to make efforts to ensure that existing board members have fluency with technical matters relevant to cybersecurity risk management by internal technical briefings for board members or by requiring board members to attend external events and education programs related to cybersecurity. Lastly, an organization might engage outside experts to fill knowledge gaps.

B. Addressing Responsibility Gaps | Examples

As one example of responsibility gaps and how they might be covered, consider the different classes of information which an organization must safeguard. In broad terms, an organization should protect the privacy of information about its customers/clients, the privacy of information about its employees, and the privacy and integrity of the corporate records of the organization. The corporate records of the organization will include documents maintained in

[29] Some have suggested that, for ESG issues, the answer lies with education programs for board members. Merel Spierings, Report | Moving Board Education—Not Expert Directors—to the Front Burner, The Conference Board (June 6, 2023), https://www.conference-board.org/publications/moving-board-education-to-front.

electronic form (such as contracts, corporate minutes, personnel files) as well as financial records (such as bank statements, payroll, billing, collections, and accounts payable).

In a large organization, primary responsibility for cybersecurity of personnel information might be assigned to the manager of the human resources department, cybersecurity of customer/client information might be assigned to the department manager who administers the product or service for which maintenance of customer/client records is needed, and cybersecurity of corporate records might be divided between a corporate secretary and a treasurer or chief financial officer. But, in the example, if payroll information is maintained as a treasury function (and not by human resources), cybersecurity for payroll might fall to the treasurer or chief financial officer and not fall under the jurisdiction of human resources.

The Draft should provide that the board of directors (or its equivalent) oversees the identification of all types of records and assets within the organization which require special protection and the assignment of responsibility for maintaining the confidentiality and integrity of those records. Creation of a chief cybersecurity officer would aid an organization in identifying responsibility gaps by situating management responsibility in a single officer.

Beyond concerns over gaps in coverage, responsibility gaps may result from a failure to align compensation and bonuses with cybersecurity goals. An AICPA report in 2022 noted that 44% of companies listed competing corporate priorities as preventing effective risk management.[30] An AICPA report in 2023 noted that risk management activities are not an explicit component in determining management performance compensation in 34% of companies, and only a minimal component in another 29% of companies.[31]

The Draft opens the door for cybersecurity management failures when it expressly sanctions competing goals as limitations on cybersecurity efforts. For example, the Draft states at Lines 612 and ff.

> This often entails some degree of trade-off with other requirements, comparing multiple products or services and

[30] AICPA, *The State of Risk Oversight: An Overview of Enterprise Risk Management Practices 13th Edition* at 26 (June 2022), https://www.aicpa-cima.com/professional-insights/download/2022-the-state-of-risk-oversight-13th-edition.

[31] AICPA, *The State of Risk Oversight: An Overview of Enterprise Risk Management Practices 14th Edition* at 30 (June 2023), https://www.aicpa-cima.com/resources/download/2023-state-of-risk-oversight-report-14th-edition.

> considering other needs such as cost, functionality, and supplier and supply chain risks.

Legal advisors should counsel board members to not let profit seeking, cost savings, etc. subordinate regulatory compliance, safety, security, and disclosure. The Draft should reflect this corporate law idea.

ADD Text | at Line 614:

> This often entails some degree of trade-off with other requirements, comparing multiple products or services and considering other needs such as cost, functionality, and supplier and supply chain risks. **Management oversight should make clear, however, that considerations of trade-offs should not let profit seeking and cost savings subordinate regulatory compliance, safety, security and disclosure.**

Indeed, in many cases, it would be negligent to not take an action when a cost-benefit or "Hand test" analysis[32] showed that an enterprise was the least cost avoider to address a cybersecurity risk.

ADD Text | at Line 464:

> Progression to higher Tiers is encouraged when risks or mandates are greater or when a cost-benefit analysis indicates a feasible and cost-effective reduction of cybersecurity risks. **As part of governance, an organization should have oversight structures and lines of reporting in place to identify situations in which the organization is reasonably expected to be the least cost-avoider to address a cybersecurity risk.**

Of equal concern is the potential for conflicts of interest to create responsibility gaps—as addressed by textual comments in CYBERSECURITY SUPPLY CHAIN RISK MANAGEMENT below. As one example, a parts supplier might engage an officer at an OEM as a technical consultant. This could create an incentive for the officer to se-

[32] A Hand test analysis attempts to quantify the probability of a loss and its magnitude and compare that to the cost of a preventive measure. If the cost of the preventive measure is less than the discounted value of the loss, then it is negligent to not take the preventive measure. See United States v. Carroll Towing Co., 159 F.2d 169 (2d Cir. 1947) (Learned Hand, J.) (describing the calculus of legal negligence).

lect products from the parts supplier without full vetting of the suitability and, perhaps, better security characteristics of a competing product.

6. Cybersecurity Supply Chain Risk Management (C-SCRM)

A. Addressing Conflicts of Interest

Draft Framework 2.0 conceptualizes C-SCRM as focused on considerations about third parties.

> The primary objective of C-SCRM is to extend appropriate first-party cybersecurity risk management considerations to third parties, supply chains, and products and services an organization acquires, based on supplier criticality and risk assessment. Lines 567-570.

Referenced resources similarly focus on *third party risks*. A preferred conceptualization would begin the supply chain risk analysis *within the organization and its employees* with a primary focus on the risks posed by *conflicts of interest*.

Draft Framework 2.0 takes a step in the direction of beginning a C-SCRM analysis within the organization when it comes to internally developed software.

> Organizations that develop software solely for their own use may benefit from adopting other C-SCRM practices, in effect treating their software development units as part of their supply chain. [In box ending at Line 606]

The following suggested drafting changes attempt to extend this approach to all C-SCRM analysis so an organization might address internal conflicts of interest as part of the output of the GOVERN function.

ADD Text | Lines 553-557:

> This ecosystem is composed of public- and private-sector entities **as well as employees and departments in an organization** (e.g., acquirers, suppliers, developers, system integrators, external system service providers, and other technology-related service providers, as well as **internal product/project managers, technical specification writers, and purchasing departments**) that interact to research, develop, design, manufacture, acquire, deliver, integrate, operate, maintain, dispose of, and otherwise utilize or manage technology products and services

ADD Text | Lines 557-558:

> These interactions are shaped and influenced by technologies, laws, policies, procedures, and practices**, and negatively impacted by potential conflicts of interest**.

ADD Text | Lines 562-564:

> See SP 800-161r1 (Revision 1), *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*, for in-depth information on C-SCRM **for risks primarily external to an organization. For C-SCRM of risks internal to an organization, an organization should consider application of generally accepted methods for addressing conflicts of interest, appropriate background checks on personnel, and related matters, in the context of minimizing cybersecurity risks. An organization should address these concerns by internal controls established as part of the GOVERN function**.

COMMENT | Supply chain risk management (SCRM) is indeed critical for any organization. However, the referenced resource at Lines 562-564 (though extensive at more than 300 pages) does not focus on supply chain risks which exist within the organization itself. Rather, it focuses on the external physical characteristics of products and services, including how they may be compromised by malicious actors. At Lines 570-572 the Draft focuses on these external concerns but could be expanded to include compromised acquisition practices within the enterprise.

ADD Text | Line 572

> Examples of risks include products and services that may potentially contain or become a vector for malicious functionality, are counterfeit, or are vulnerable due to poor manufacturing and development practices within the supply chain **(and which internal enterprise practices fail to exclude based on conflicts-of-interest or other deficient acquisition policies and practices).**

ADD Text | Table 6. IDENTIFY (ID): Help determine the current cybersecurity risk to the organization [at p. 34] * * *

> **Risk Assessment (ID.RA):** The organization understands the cybersecurity risk to the organization, assets, and individuals **(including potential conflicts of interest).**

In case of a potential conflict of interest only outside directors should be involved in oversight of the potentially compromised matter. Then a special committee of outside directors will make the related decision or recommendation.

B. Consistent Inclusion of Both Products and Services Suppliers

The Draft often refers to both providers of *products* and suppliers of *services* when a cybersecurity measure or consideration is appropriate for both. Consistent references to both products and services would more directly link the comment to a possible concern about a related supply chain risk and might be preferred for that reason so that both products and services receive appropriate attention. Consistent reference to both products and services will help address persistent legal confusion over what constitutes a good and what constitutes a service—a question with particular relevance to software.[33]

As an EXAMPLE of comprehensive reference to products and services | Lines 665-666: When reviewing cybersecurity programs for privacy risks, an organization can consider taking actions such as the following: . . . Lines 675-676:
Inform ***providers of cybersecurity-related products and services*** about the organization's applicable privacy policies **[emphasis supplied in bold and italics]**

The Draft often refers to both suppliers of *products* and suppliers of *services* when a cybersecurity measure or consideration is appropriate for both. [Lines 594, 601, 604, 605, 611, 614] In other places it refers only to a product [Line 618] or service [Lines 536-537] when a reference to both is likely more appropriate. The following drafting suggestions advance clarity by adding a more inclusive reference.

[33] *See, e.g.*, Quinteros v. InnoGames, 2022 WL 898560 (W.D. Wash. March 28, 2022), Rodgers v. Christie, 795 F. Appx. 878, 880 (3d Cir. 2020). Because a business and legal audience will be familiar with these categorization issues, the Draft can remove any doubt about the intended scope of a reference in Guideline 2.0.

ADD Text | Lines 536-537:

> ● Express its cybersecurity risk management requirements to an external service provider (e.g., a service provider with which it is exchanging data) **or a supplier (e.g., a manufacturer from which it is obtaining microprocessors)** through a Target Profile

ADD Text | Lines 545-547:

> ● Share high-level information on cybersecurity practices with prospective customers, **suppliers,** business partners, and others who may need to understand the organization's cybersecurity posture before engaging with the organization

ADD Text | Line 548:

> ● Define shared responsibility models with cloud service providers **and allocation of system engineering responsibilities with product suppliers**

In Table 6. IDENTIFY (ID): Help determine the current cybersecurity risk to the organization:

ADD Text |

> ID.AM-04: Inventories of **products and** services provided by suppliers ae maintained

ADD Text |

> ID.AM-08: Systems, hardware, software, **products** and services are managed throughout their life cycle (formerly PR.DS-03, PR.IP-02, PR.MA-01, PR.MA-02)

In Table 8. DETECT (DE): Find and analyze possible cybersecurity attacks and compromises.

ADD Text |

> DE.CM-06: External **product and** service provider activities**, products** and services are monitored to find potentially adverse events

C. Supply Chain Risk Associated with Reliance on Provider Certifications | Need for System Engineering

Supply chain risks for an organization are not limited to concerns about acquisition of products and services from compromised providers or through internal acquisition policies and practices subject to conflicts-of-interest. Organizations should be cognizant of risks associated with unobjectionable marketing efforts and certifications from reputable providers to ensure that use of a product or service does not create a knowledge gap or a responsibility gap.

For example, in the case of automated vehicle technology, a supplier of a semiconductor chip may advertise its product as meeting certain requirements such as satisfaction of ASIL-D and compliance with FCC requirements—neither of which have significance for cybersecurity measures.[34] Moreover, a provider may advertise specification of its product as a cost saving measure.[35]

There is, of course, nothing improper about marketing efforts such as these. However, an organization must take special care when evaluating products to ensure that it does not misunderstand the import of these statements, or the risks associated with cost-saving measures. An infamous cost-saving measure gone bad relates to the Ford decision to remove a protective bladder from the gas tank of the Pinto to meet a target set by senior management.[36]

An organization has financial incentives to minimize its own investment in system engineering and to rely on providers to do the safety and security analysis. The mere fact that a component has achieved a safety rating such as ASIL-D or compliance with a government requirement (such as that promulgated by the FCC) does not mean that the component may be incorporated into a product without cybersecurity risk because the component must function securely as part of a larger system in the product within which it is incorporated.

Moreover, the product itself may permit various configurations by an OEM—some of which may present cybersecurity challenges.

[34] An example of such a product from a reputable supplier is Nvidia's upcoming Thor system on a chip (SOC) which will be available in 2025.

[35] *Id.*

[36] *See, e.g.*, Stuart Strother, *When Making Money is More Important Than Saving Lives: Revisiting the Ford Pinto Case*, 5 J. INT. & INTERDISCIPLINARY BUS. RESEARCH 166 (2018), https://scholars.fhsu.edu/cgi/viewcontent.cgi?article=1104&context=jiibr.

For example, Nvidia's Thor chip may be configured to run system critical navigation, as well as infotainment. In the commercial aviation field, public discourse considers whether passenger access to infotainment presents a risk of compromising system critical navigation.[37]

7. LIMITATIONS OF A VOLUNTARY FRAMEWORK APPROACH

Framework 2.0 is a foundational resource that is adopted voluntarily and potentially through governmental policies and mandates. We know that voluntary compliance with governmental cybersecurity recommendations does not work well.

Recently the Securities Exchange Commission (SEC) confirmed this unfortunate limitation of voluntary compliance with recommendations in its release adopting cybersecurity disclosure requirements effective September 5, 2023, noting "[o]verall, we remain persuaded that, as detailed in the Proposing Release: under-disclosure regarding cybersecurity persists despite the Commission's prior guidance ..."[38]

Within the project to create a voluntary Cybersecurity Framework 2.0, NIST nevertheless has the option to deliver its message with more force. The Draft's voluntary language takes the notion that its recommendations are optional too far. For example, at Lines 665 and ff. the Draft appears to suggest that compliance with applicable privacy statutes and regulations are mere considerations:

> When reviewing cybersecurity programs for privacy risks, an organization can consider taking actions such as the following: * * *
>
> ● Comply with applicable privacy statutes and regulations

Those charged with oversight as part of governance have a fiduciary duty to put in place corporate structures and lines of reporting for the express purpose of complying with laws and regulations. It is not an optional "consideration."

[37] *See, e.g.*, Air Line Pilots Assoc. Intl., *Aircraft Cybersecurity: The Pilot's Perspective*, ALPHA WHITE PAPER (June 2017) (noting potential risks with "E-enabled" aircraft), https://www.alpa.org/-/media/ALPA/Files/pdfs/news-events/white-papers/white-paper-cybersecurity.pdf?la=en.

[38] SEC Release, Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure at 13.

At Line 98 [page 2] the Draft is referred to as a "voluntary" Framework. It is voluntary, except when it is not voluntary because of a mandate by another law. And the status of policies is what exactly?—the sort of policies such as those floated by the SEC which were ignored and thus required the issuance of new regulations on cyber disclosure? The policies reflected in NIST's Framework 2.0? If policies are, in fact voluntary too, then this should be noted—but in the case of cybersecurity that itself presents a risk which is one reason to make the language of the framework much more imperative.

The presumption should be that failure to engage with Framework 2.0 at the level of corporate oversight is negligent and, indeed, a failure to fulfill a fiduciary duty. The burden should be on the board of directors (i.e., those responsible for oversight in an enterprise) to give a good reason for taking another approach or omitting a step.

ADD/DELETE Text | Line 103

> This collection of cybersecurity outcomes creates a taxonomy and structure that ~~can be~~ **should be** used **absent a compelling reason documented by those charged with oversight of an enterprise** to understand, assess, prioritize, and communicate about cybersecurity risks.

The use of too much hedging language can create the same compliance problem which led the SEC to adopt cybersecurity reporting obligations because it overemphasizes "flexibility".[39] [Lines 422-424]. The kind of flexibility that an organization should have is found at Line 434 where "[o]rganizations are encouraged to innovate and customize how they incorporate measurement into their application of the Framework." The presumption or default expectation should be that organizations use the NIST framework and that they use it in institution appropriate ways—not whether they use it.

8. USING CONTRACTS TO POLICE AN ORGANIZATION'S CYBERSECURITY REQUIREMENTS

The Draft contemplates that an organization may use contracts to further its cybersecurity management goals. [Lines 607-608] While a contracting approach can supplement cybersecurity in important

[39] *See supra* note 38.

ways, such an approach presents risks related to imbalances in market power which may limit its effectiveness.

For example, in the automotive industry, critical components of an automated driving system (ADS) such as advanced microprocessors may be available only from a single or small number of suppliers. These suppliers may understandably have concerns over creating civil liability for breach of an obligation to report information to an OEM. Indeed, they may have the market power to reject any suggestions for adding contractual reporting covenants to a supply contract.

Bilateral negotiation of reporting obligations (even if agreed) may prove less efficient than relying on reporting obligations which might arise by membership in industry groups—such as Auto-ISAC. Thus, the Draft should urge suppliers of goods and services to become members of industry groups with mutual reporting obligations to the users of its goods and services to avoid difficult and costly custom reporting obligations in individual contracts. This would not, of course, prevent the negotiation of custom contract terms in appropriate cases.

ADD Text | Lines 607-610

> An organization can use Framework Profiles to delineate cybersecurity standards and practices to incorporate into contracts with suppliers <u>**of goods and services**</u> and provide a common language to communicate those requirements to suppliers. Profiles can also be used by suppliers <u>**of goods and services**</u> to express their cybersecurity posture and related standards and practices. <u>**Suppliers of goods and services ought to consider membership in industry groups with mutual reporting obligations to foster communication whether or not contract terms impose reporting obligations.**</u>

9. CONCLUSIONS

In the current Draft, NIST has taken the important step of adding a GOVERN function to Cybersecurity Framework 2.0. In various places, the Draft engages with the import of adding a GOVERN function, including recognition that this involves an oversight function. The Draft needs to complete this engagement.

To make Framework 2.0 most effective, the next step is to revise the Draft to make it easily useable by businesspersons and their legal advisors. This requires more specific reference to specific tasks that come within a typical governance and oversight function such as selection of a management model, aligning compensation with cybersecurity goals, managing conflicts of interest within the enterprise which might compromise the cybersecurity mission, and addressing problems of contracting efficiency.

This project holds the promise allowing persons without cybersecurity expertise to effectively govern, manage and oversee the critically important task of implementing cybersecurity.

William H. Widen
Professor of Law
University of Miami School of Law
[redacted]