May 31, 2023

Ms. Vanessa Countryman
Secretary
U.S. Securities and Exchange Commission
100 F Street N.E.
Washington, D.C. 20549

Re: Cybersecurity Risk Management Rule for Broker-Dealers, Clearing Agencies, Major Security-Based Swap Participants, the Municipal Securities Rulemaking Board, National Securities Associations, National Securities Exchanges, Security-Based Swap Data Repositories, Security-Based Swap Dealers, and Transfer Agents, [Release No. 34-97142; File No. S7-06-23] https://www.sec.gov/rules/proposed/2023/34-97142.pdf

Dear Ms. Countryman:

I respectfully submit this comment letter in response to the Securities and Exchange Commission's (the "Commission") proposed rules.

> "If one has a hammer one tends to look for nails…" Silvan S. Tomkins, Princeton University from the conference paper collection Computer Simulation of Personality: Frontier of Psychological Theory, in Chapter 1, Page 8, presented June 1962.
>
> "I suppose it is tempting, if the only tool you have is a hammer, to treat everything as if it were a nail." Abraham H. Maslow, The Psychology of Science, page 15, 1966

5 Bullet Summary:

- The proposed rules are based on a false premise -- that the system in which cybersecurity risk lives is like the system in which bookkeeping/ICFR risk lives.
- Bookkeeping checks and frameworks that do not reflect the full system in which cybersecurity risk lives ➔ wasted money and time ➔ burnout and stress for cyber pros ➔ setup cyber pros for failure ➔ breaches.
- The proposed rules violate math and methods that have been proven and practical for decades in managing risk in other disciplines. Cyber already lags other disciplines by decades, the proposed rules would reinforce this lag.
- I understand that proposed rules naturally take a rules-based approach. Yet, if a rules-based approach is used, it would 1) encourage tick-box compliance (especially via attorneys and auditors seeking to minimize their liability) over protecting against national security threats to financial markets and 2) be counter to proven methods of protecting people from danger in other areas of government oversight.

Summary

The proposed cyber security rules are like a “hammer” looking for a “nail.”

- **The proposed rules apply the “hammer” – bookkeeping checks of internal control over financial reporting (ICFR) – wrongly to the “nail” of cyber security and warfare**
    - The system in which cybersecurity lives is vastly different from the system in which bookkeeping and ICFR risk lives.
    - Thus, it is a structural flaw (in the technical sense) to conflate these two vastly different systems.
    - **It is a category error and structural flaw because ICFR risk lives in a linear stable system. The high-end threats are expense account cheats, accelerating sales and paying bribes. Bad actors have employee badges.**
    - **In sharp contrast, cyber security and warfare risk live in a system that is complex, dynamic, adaptive even chaotic (in the technical sense of the term), and highly adversarial. The high-end threats are far more severe.**
- The risk assessment-heavy approach in the proposed rule reinforces this error because its emphasis is focused on common external threats using bookkeeping methods, rather than balanced with 1) the entire system (including broader threats) and 2) the structural flaws of how the internal cybersecurity system works.
    - This bookkeeping approach contravenes everything known about risk management in disciplines ranging from medicine to military to sports to aviation to process safety.
    - In ICFR/bookkeeping, this is a reasonable assumption because the system is relatively linear and stable.
    - **In cyber security and warfare, this assumption is clearly false.**
- **Citing the Verizon Data Breach Report is an example of this error** – the math and methods used to create this report are contrary to methods used in the federal government for decades and Bell Labs (from which I have 6 patents)
- Citing the NIST Framework for Improving Critical Infrastructure Cybersecurity is helpful. Yet it also **makes clear that the NIST “frameworks” for cybersecurity fall short of the frameworks that NIST has for other disciplines and frameworks elsewhere in federal government**.
    - A key test for a framework is that anything that can change the outcome of a system is part of the system – and thus a framework.
    - This particular NIST framework cites work to which I contributed but excluded other parts of the system.
    - Thus, by typical tests of frameworks it is not a framework.
    - Would you:
        - Go into a building where steel girder systems design was excluded?
        - Have surgery from a doctor who did not understand your body as a complete system?
- **The proposed rules make no reference to President Biden’s Executive Order from May 12, 2021,** regarding cybersecurity and authentic Zero Trust (please see reference section at the end)
- The proposed bookkeeping paperwork-based approach…
    - Cannot create an award-winning restaurant or sports team
    - By creating wasteful busy-work, it **sets up cyber pros for failure -- burnout, stress, and cognitive overload – causing breaches**.

- Reflect on the breaches in the federal government and elsewhere. If proven and practical systems and root cause analysis (e.g., Mr. Ishikawa's famous "Fishbone Diagram") were used, it would reveal how **most all breaches are self-inflicted.**
- W. Edwards Deming (who worked in what is now the Ford Office Building) noted that over 95% of problems were from "common causes," a.k.a., "structural flaws" – flaws designed into a system that set people up for failure. To this with a bit of humor, see:
  - Video of Deming himself leading his famous "Red Bead" exercise.
  - Charlie Chaplin, Modern Times, factory scene on YouTube (about 80 million views) or Lucy and Ethel in the Chocolate Factory.

In revising the proposed rules, it would be helpful to focus on the objective – protecting people and financial markets from danger.

- In cyber security and warfare, the opportunity is to encourage the use of Critical Thinking, Systems Thinking, Design Thinking and authentic Zero Trust strategies to make companies more secure. This then contributes to national and global security – as has been done successfully for decades in other areas of federal government.
- Following the logic of these proposed rules, would the SEC overrule the FAA and force public company airlines to use bookkeeping checks for managing aviation risk?
- **If the proposed rules are not revised, then they would become the root cause of breaches and a threat to national security** – simply because they are completely inappropriate given decades of proven and practical methods elsewhere in federal government.
- **The SEC could look to other agencies (federal and state) with oversight roles for protecting people from danger**.

After an explanation of this summary, resources are provided on how the proposed rules could be revised by taking advantage of how Critical Thinking, Systems Thinking, Design Thinking and authentic Zero Trust strategies are already used in the U.S. Government and beyond.

Explanation: Managing risk is all about understanding the system

Successfully managing risk requires 1) thoroughly understanding "how it works" – the nature of the system, 2) discovering the real problem, 3) asking, "What if?" 4) to solve the real problem. This is fundamental to systems thinking and applies from cooking to driving a car through a storm to ice skating to kinetic warfare to new products management to forestry.

The confidentiality, integrity and accuracy of the information reported to the SEC's EDGAR system is entirely different from cyber security and warfare.

- Financial reporting is about **reasonable assurance** of the accuracy of the financial **consequences** of tangible transactions (e.g., payment for raw materials) that happened in the **past** in a **linear, stable system** -- general ledger. A high-end threat is detecting fraud or a bribe paid. Debates about accounting treatments happen within the confines of rules and professional guidance. Errors and omissions are addressed with routine methods. Thus, confidence in error ranges and predictability are relatively high.

- Cyber security and warfare are about managing **risk in unfolding situations** in a **complex dynamic, adaptive, chaotic system** in an unpredictable, **emerging future**. Cybersecurity is more **highly adversarial**. High-end threats include disabling a power grid, contaminating water supplies, halting logistics, or turning off infusion pumps in hospitals. While scenarios can be imagined using creative, film-script style methods and wargaming, a company faces an emerging future as do President Biden and world leaders facing Putin's aggressive war. Law enforcement revelations about hacking gangs like LAPSUS$ reinforce the nature of the system and the future.

In short, because of these differences in the nature of the system, it would be a **structural flaw** (technical term for a flaw design into the structure of a system) and the "wrong tool for the job" to apply linear stable system bookkeeping checks a complex dynamic and highly adversarial system.

Consequences of the proposed rules – a category error

The proposed rules use the term "controls" broadly. While "control" can be applied in many senses, simplifying here into just two.

- Those in the bookkeeping tradition previously termed "checks" that are "to do" lists with origins in ancient Egyptian grain accounting. They are best for linear, repetitive tasks. They are the nature of the "policies and procedures" disclosures listed in the proposed rules.
- Those in the mechanical/automated tradition, with origins in ancient animal traps now found in steam engines, air conditioning, consumer electronics, avionics and more. These are designed with specific ranges, tolerances and service lifetimes – look at the back of your laptop power supply.

Reliability and use are strikingly different, especially in the complex dynamic system of cybersecurity. For example, please see the CISA page for the SolarWinds compromise https://www.cisa.gov/uscert/remediating-apt-compromised-networks. To better understand the mechanical/automated approach in the context of systems for cybersecurity, please see https://csrc.nist.gov/publications/detail/sp/800-160/vol-1/final

More, the bookkeeping/ICFR approach defocuses, is wasteful and distracts from actions to strengthen security and reduce business losses.

Consider a restaurant. It could have the most hygienic kitchen. It could have the finest ingredients – far beyond certification standards for organic. It could have the happiest staff. Yet will those actions cause a "5-star" rating across the categories of presentation, experience and taste of food?

Consider further:

- Does the method used for checking the cash box at a sporting event make a team win?
- Does the method used for checking a pilot's hotel bill make a safe flight?
- Does the method used for checking the cash box at a circus ensure animal welfare?

Moreover, consider the structural flaw of applying bookkeeping/ICFR-based methods of managing risk to cyber security and warfare.

- By that same logic would the SEC demand that bookkeeping-based methods be applied to other business disciplines – new product management, marketing, logistics or IT systems response time on "Black Friday." Those disciplines have decades of proven and practical math and methods.
- By that same logic would the SEC demand that bookkeeping-based methods be used for all aspects of a business – including industrial operations and transportation? Would it override the guidance of the CSB or NTSB for public companies and replace that guidance with bookkeeping-based methods? Or overrule the FAA?

Creating causes of action or solving the real problem?

More, the proposed rules would reinforce an error in the application (not what the Act states) of Section 404 of the Sarbanes-Oxley Act. Too often, bookkeeping/ICFR-based methods used for the linear, stable system of financial reporting are applied by external auditors to the complex dynamic system of cyber security and warfare. Too often, the root cause of an incident is bad math and method used by the cybersecurity team – often based on bookkeeping/ICFR or insurance claims methods. The proposed rules would legitimize those common errors.

The bookkeeping paperwork nature of the proposed rules gives rise to problems:

Paperwork is not always bad. Aviation, medical procedures, auto repair and more have detailed documentation. But those are for linear tasks that are done exactly the same way by any person. Flight safety or military success in complex dynamic systems comes from thinking and practice – flight simulators or years of experience in tumor removal. The crash of Air France Flight 447 is a tragic reminder.

The focus on paperwork – policies, procedures and assessments -- over solving the real problem…

- Defocuses from understanding the nature of the system and solving the real problem
- Causes companies to reach for the SEC's bookkeeping/ICFR tools rather than the right tools
- Causes companies to double-down on what they perceive will protect from enforcement actions and private causes of action, rather than what improves security for customers, employees and the United States
- Sets up cybersecurity professionals for failure due to stress and burnout associated with wasteful tasks
- Wastes budget especially for smaller companies with smaller cybersecurity teams

Consider one aspect of the proposed rules – risk assessments – more closely. The error of focusing on risk assessments instead of focusing on understanding the nature of the system and "how it works."

- Reflect on winter snowstorms that clogged freeways and electric vehicles that lost power on those freeways becoming roadblocks. Car owners failed to understand the limitations of the system that was their electric vehicle.

- **Bookkeeping/ICFR-based (even insurance-based) risk assessments are inappropriate for the nature of the system in which cyber risk lives.** Instead, they could be modeled after military or COVID logistics or NTSB or CSB investigation methods of systems and root cause analysis.
- When a systems-based approach to cyber is calculated, many typical controls (of the bookkeeping check type) are found to be wasteful, inappropriately placed in the system, inefficient or ineffective. The math is clear.

The proposed rules cite a NIST risk management framework, without realizing that the Framework (which is not a framework as it is not comprehensive) states "However, the variety of ways in which the Framework can be used by an organization means that phrases like 'compliance with the Framework' can be confusing."

The cumulative effect of this path would be to create vulnerabilities that become incidents that become breaches.

In sum, the **errors and flaws in the proposed rules would put the SEC at the root cause of breaches**. This is the opposite of the objectives of the Biden Administration.

Regarding cybersecurity expertise on boards of directors, the real question is, "What expertise?"

- If it is more bookkeeping/ICFR-based expertise, then that would reinforce the structural flaw of using ICFR-based methods for cyber security and warfare. It would also reinforce the problem of having cybersecurity overseen by audit committees.
- All board members should be encouraged to bring their personal and professional backgrounds in critical thinking, systems thinking and design thinking to best oversee and guide management and empower CISOS in improving, including: 1) fixing the root cause of waste, vulnerabilities and breaches and 2) implementing authentic Zero Trust strategies. Many disciplines include design thinking, and systems and root cause analysis – cooking, information technology resilience, architecture, biology and assembly line design. Board members should be encouraged to bring their "whole self" experience in systems and root cause analysis and design expertise to cybersecurity discussions – not feel excluded.
- The "expert" needs to bring strength in critical thinking, systems thinking and design thinking – <u>especially in a cybersecurity context</u> – **to draw out the strengths of other board members and guide the asking of smart questions of management to empower management, CIOs and CISOs and thus to improve company and financial markets security.**

References for proposed rule revisions

Proven and practical alternatives are available to the SEC.

The references below are to critical thinking, systems thinking and design thinking as used elsewhere in U.S. Government. Some references are in the context of cybersecurity and some are for other complex dynamic systems where these approaches have been successful.

The point is that these thinking types apply to complex dynamic systems that are the environment of cyber security and warfare. Bookkeeping or ICFR methods are simply not appropriate for the nature of the system in which cybersecurity lives.

With these approaches to "thinking," the SEC can revise the proposed rules to be less likely to cause vulnerabilities and breaches in regulated companies.

By adopting proven and practical approaches appropriate to complex dynamic and highly adversarial systems, then the proposed rules would achieve the intended objective of reducing danger to people and financial markets.

Zero Trust Strategies

- President Biden's Executive Order including Zero Trust https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
- NSTAC Report https://www.cisa.gov/sites/default/files/publications/Final%20Draft%20NSTAC%20Report%20to%20the%20President%20on%20Zero%20Trust%20and%20Trusted%20Identity%20Management.pdf

Critical Thinking

- https://files.eric.ed.gov/fulltext/EJ1143316.pdf
- https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4216424/
- https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4235550/
- https://www.dol.gov/sites/dolgov/files/odep/topics/youth/softskills/problem.pdf
- https://leb.fbi.gov/articles/perspective/perspective-need-for-critical-thinking-in-police-training
- https://emilms.fema.gov/is_0453/groups/46.html
- https://www.dhs.gov/publication/media-literacy-and-critical-thinking-online
- https://humancapital.learning.hhs.gov/e-blast/eblast201904.asp
- https://appel.nasa.gov/course-catalog/critical-thinking-and-problem-solving-appel-ctps/
- https://psnet.ahrq.gov/issue/developing-critical-thinking-skills-delivering-optimal-care

Systems Thinking

- https://csrc.nist.gov/publications/detail/sp/800-160/vol-1/final
- www.ntsb.gov
- www.csb.gov
- https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3940421/
- https://www.dhs.gov/publication/st-operations-and-requirements-analysis-overview-fact-sheet
- https://www.dhs.gov/science-and-technology/ora
- https://apps.dtic.mil/sti/citations/AD1045468
- https://www.airforcemedicine.af.mil/News/Display/Article/1089321/afms-uses-systems-thinking-to-keep-everyone-on-the-same-team/
- https://archive.epa.gov/ged/tutorial/web/html/index.html
- https://www.fs.usda.gov/treesearch/pubs/60063

Design Thinking – please notice use in military

- Department of Defense Joint Special Operations University https://www.youtube.com/channel/UCL7hOd0ihWzmJlga_Y4wCJg
- https://www.dyess.af.mil/News/Features/Article/2552100/afgsc-design-thinking-course-leads-to-dyess-afbs-first-sbir-phase-3/
- https://www.dhs.gov/sites/default/files/publications/OCIO%20Strategic%20Plan.Dec2018.pdf
- https://www.secnav.navy.mil/agility/assets/documents/WCD%20Fac%20course%20version%2020200830.pdf
- https://juniorofficer.army.mil/turn-your-meetings-into-intrapreneur-workshops/
- https://www.nist.gov/blogs/manufacturing-innovation-blog/five-hottest-innovation-tools-0
- https://www.cdc.gov/pcd/issues/2018/18_0128.htm
- https://www.acf.hhs.gov/ofa/report/creating-solutions-together-design-thinking-office-family-assistance-and-3-grantees
- https://www.ed.gov/sites/default/files/documents/stem/cybersecurity-slides.pdf
- https://niccs.cisa.gov/training/search/skillsoft/prototyping-design-thinking
- https://assets.section508.gov/files/Copy%20of%20Universal_Design_%20White%20Paper_vFinal_0.pdf

Summary of the above

- www.thinkdesingcyber.com
- www.tdcleadershub.com

Very respectfully submitted,
Brian Barnier
OCEG Fellow (OCEG is the organization that created the concept of Governance, Risk and Compliance)
ISACA V. Lee Conyers Award recipient
ISACA Joseph J. Wasserman Award recipient