




March 6, 2024

MEMORANDUM FOR THE CYBERSECURITY ADVISORY COMMITTEE MEMBERS

FROM: Jen Easterly
Director 

SUBJECT: **Formal Response to Recommendations Provided on
September 13, 2023**

The Cybersecurity Advisory Committee (CSAC) was established in June 2021 to advise the Cybersecurity and Infrastructure Security Agency (CISA) on the development, refinement and implementation of policies, programs, planning, and training pertaining to CISA's cybersecurity mission. Since that time, the CSAC has worked tirelessly to infuse fresh ideas into CISA's cybersecurity mission, leveraging their members' significant subject-matter expertise.

CISA values the hard work of the CSAC that led to a set of actionable recommendations to improve on CISA's execution of its cybersecurity mission. The expert advice and key insights that the CSAC offers enhances the work of CISA and keeps us well-positioned to help address threats in a rapidly changing cybersecurity landscape.

I have worked closely with my leadership team to determine the feasibility of each recommendation and to ensure that we remain within the parameters of CISA's operating authorities and resources. Our response to each subcommittee follows:

Response to the Building Resilience and Reducing Systemic Risk to Critical Infrastructure Subcommittee

Recommendations 1 – 8

As noted by this subcommittee, a model for operational collaboration is critical. CISA is currently working through the development of a maturity model for measuring and further advancing operational collaboration, which will likely include identification of common attributes of organizations whose operational collaboration with CISA have been most effective. We will engage with our stakeholders to ensure the maturity model provides clear guidance for sector partners as they work to collaborate more with us. CISA also continues to coordinate with the interagency on a new National Security Memorandum (NSM) that will clarify CISA's role as National Coordinator for critical infrastructure security and resilience and describe how CISA will coordinate with Sector Risk Management Agencies (SRMAs) to perform their statutory roles and responsibilities. We agree with the subcommittee that our collaboration with SRMAs must continue to mature, and we are confident that the release of the NSM will lay the groundwork for improved coordination.

CISA concurs with all of the recommendations with the exception of establishing a new Chief Executive Officer (CEO)-led Committee given that the intent of the recommendation is already captured through the structure of Sector Coordinating Councils.

Response to the National Cybersecurity Alert System Subcommittee

Recommendations 9 – 14

CISA strongly agrees with the subcommittee that the establishment of a national cybersecurity alert system (NCAS) is important and that it would provide immense value to the stakeholder community. As noted in the subcommittee's report, the real value lies in the processes, capabilities, discipline, and tradecraft needed to serve as the foundation of an NCAS. CISA is presently working with interagency and private sector partners to revise the National Cyber Incident Response Plan (NCIRP), which will incorporate an updated approach to evaluating and communicating severity for specific cyber incidents. This work is a key prerequisite to establishing a sustainable and credible NCAS, which we intend to evolve as a follow-on activity to the updated NCIRP.

CISA concurs with all of the recommendations provided with the exception of the one relating to developing a legal framework for sharing and acting on cyber threat information. Such a framework already exists, pursuant to the Cybersecurity Information Sharing Act of 2015.

Response to the Transforming the Cyber Workforce Subcommittee

Recommendations 15 – 40

CISA is greatly appreciative of the subcommittee's recognition of all the progress made to date to establish CISA as a People-First agency. We are committed to continuing to improve our culture by empowering our team to use creative, thoughtful, and data-driven ways to improve employee engagement. We are actively engaged in improving our existing programs and creating new ones to ensure employees feel supported as individuals and in their careers. We are currently working to improve and expand our Employee Association Groups, as well as to institute new training pathways to better equip our team for the future. We have also launched programs to improve the data available to us about employee engagement, such as a 360-degree review program where team members provide direct feedback to their managers, and an Exit Interview Pilot to better understand why employees choose to leave. Our leadership team is also engaging in efforts to expand use of development rotations and promote meaningful in-person engagements. As we fully establish and staff the Office of the Chief People Officer, we will develop plans to ensure the recommendations are implemented.

CISA concurs with the recommendations provided with the exception of the one related to using software tools to track employee workload, given privacy concerns, and those related to cohort-based upskilling and linking volunteerism with career development as we do not have the expertise or resources required to do so at this time.

Response to the Turning the Corner on Cyber Hygiene Subcommittee

Recommendations 41 – 44

CISA's cross-sector Cybersecurity Performance Goals (CPGs) were developed to further a common understanding of the baseline security practices that critical infrastructure owners and operators should follow to protect national and economic security, as well as public health and safety. Further adoption of the CPGs will allow CISA to serve as the definitive and unifying voice for security guidance and fill the gaps identified by the stakeholders this subcommittee engaged with. We have begun developing measures to ensure we are tracking the effectiveness of the CPGs. In fall 2023, we released our first public data on implementation of two CPGs and intend to be able to measure and assess effectiveness of all CPGs within the next two years. In addition to promoting adoption of CPGs, we agree with the subcommittee that more accessible, easy-to-understand products would be valuable. For sectors for which CISA is the SRMA, we will work with our partners to identify information gaps related to sector risk and readiness and develop sector-specific outreach strategies to address them.

CISA concurs with the recommendations provided with the exception of creating a roadmap to action to overcome financial barriers as we lack the expertise and authority required to implement this recommendation.

Response to the Technical Advisory Council Subcommittee

Recommendations 45 – 71

Through the Joint Cyber Defense Collaborative (JCDC) High-Risk Community Protection (HRCP) Initiative, CISA has already begun the important and necessary work noted in this subcommittee's report. Our focus now is on laying a solid foundation for the HRCP Initiative that will allow it to be a valuable – and valued – resource for high-risk communities. We are concentrating initially on civil society since this community is at the nexus of the three criteria used to identify high-risk communities: (1) demonstrated targeting by malicious cyber actors, based on the individual's or organization's work to support humanitarian or democratic causes; (2) low capacity to defend themselves against cyber threats; and (3) low levels of historic government support. In addition to the focus on civil society, CISA is developing a suite of guidance documents that would be applicable to all high-risk communities and individuals. CISA launched the HRCP Initiative in spring 2023, and we have plans to continue to grow the program.

CISA concurs with the recommendations provided.

Response to the Corporate Cyber Responsibility Subcommittee

Recommendations 72 - 108

CISA is greatly appreciative of this subcommittee's work and is committed to building a Corporate Cyber Responsibility (CCR) Initiative. The pillars and recommendations laid out by this report will be extremely helpful in guiding how we build and grow a dedicated program for CCR. While we are currently doing some work in this sphere, through development of training materials applicable to corporate boards and promotion of the CPGs, we acknowledge that there is much more work to be done. We are planning to fully resource the CCR Initiative during Fiscal Year (FY) 2025.

CISA concurs with the majority of the recommendations provided, except for those that exceed either our authorities or expertise, such as the recommendation relating to provision of legal advice to non-federal entities.

Again, I thank the CSAC and its members for their thoughtful recommendations. Please feel free to contact me if you have any questions. We look forward to continued partnership with the CSAC.

List of Recommendations and Responses

	Recommendation	Response
1	Recommendation: With respect to recommendations identified in September 2022, implementation of recommendations is underway and should be consistent with outcome of the PPD-21 Rewrite. CISA should not proceed with SIE designations until it collaborates with private sector regarding existing critical infrastructure designations and authorities (i.e., EO 13636 Section 9).	Concur
2	Recommendation: CISA should develop an ongoing process for reviewing attributes and maturity model for achieving operational collaboration. The process should be managed by CISA with sector-led implementations conducted by SRMAs/GCCs and SCCs. This maturity model would create a pathway for both industry and government capabilities to progress in an organized and coordinated fashion that is accountable to scrutiny.	Concur
3	Recommendation: CISA should more clearly define their role as National Coordinator with supporting architecture and an organizational structure. This structure should include defined SRMA roles, responsibilities, and capabilities. At a minimum, CISA should ensure sector-specific points of contacts for ease of integration by non-CISA personnel (SRMAs and Sectors/Subsectors).	Concur
4	Recommendation: CISA, as the lead agency responsible for the White House National Cybersecurity Strategy implementation plan 1.4.1 tasking “Update National Cyber Incident Response Plan” (NCIRP), should develop an owner/operator-centric update to the NCIRP. Rather than considering what government needs to support its decision making and efforts, it should use a first-principles approach to considering how the government can support owners/operators during crisis. The NCIRP update should also align to FEMA’s incident response plan. CISA should include the critical infrastructure asset owners and operators as part of the tasking team.	Concur
5	Recommendation: The National Critical Infrastructure Risk Register exemplifies CISA's commitment to bolstering our national security. To maximize the potential for risk reduction, CISA must refine the governance structure to encompass designated critical infrastructure private sector representatives. CISA should establish dedicated working groups—where public and private experts collaboratively engage in risk analysis—to ensure comprehensive insights that effectively mirror real-world scenarios. Additionally, recognizing the pivotal role of SCCs, CISA should encourage these councils to integrate experts to address intricate risk scenarios in support of a national risk strategy.	Concur
6	Recommendation: To the extent that sectors/subsectors have already developed a risk register, CISA and SRMAs should align their own efforts with industry approaches where possible and appropriate.	Concur
7	Recommendation: CISA's collaboration with SRMAs has proven instrumental but needs improvement. To operationalize the aggregate efforts and effectively diminish risk, CISA’s NRMC should engage in regular collaboration with the critical infrastructure private sector. This engagement should extend to promote systemic interaction with CISA’s JCDC, the SCCs, GCCs, and SRMAs—ensuring all stakeholders with relevant expertise are at the decision-making table and have common operating picture across sectors.	Concur
8	Recommendation: Architecture from both the private and public sector for operational collaboration will form a sustaining approach. CISA should explore ways to establish a standing, private sector CEO-led Committee that would report directly to the President of the United States, with participation from the Office of National Cyber Director, National Security Council, CISA Director and the Homeland Security Advisor, to ensure that resilience—including continuity planning-- is a priority. The function of this Committee would be to support the Continuity of the Economy through exercises with Cabinet-level members.	Non-Concur

9	Recommendation: CISA should assign the task of developing a national cybersecurity alert system to a dedicated team (“CISA national cybersecurity alert system Team” equipped with the authority and resources needed to define, implement, and lead an operational national cybersecurity alert system.	Concur
10	Recommendation: The CISA national cybersecurity alert system Team should initiate its work by identifying and working with stakeholders to define the purpose(s), formats, target groups, and measures of effectiveness for cyber alerts.	Concur
11	Recommendation: The CISA national cybersecurity alert system Team should develop and implement a federated model for the national cybersecurity alert system that leverages authorities, capabilities, and infrastructure across the federal government and its counterparts in the private sector – the Committee offers several courses of action here but strongly recommends one that partners with the FBI organization leading threat response under PPD41 and with sector specific agencies leading sector cyber engagement.	Concur
12	Recommendation: The national cybersecurity alert system should consider a tiered release strategy that provides most timely and granular information to those with largest equity and ability to action the information-in-question on behalf of the broadest population of downstream users. Ring 0 covers warnings that are imminent and specific.	Concur
13	Recommendation: The CISA national cybersecurity alert system Team should build on existing CISA monitoring processes and associated National Cyber Incident Scoring System (NCISS) to add warning, alert, and guidance functions (that yield the so-called national cybersecurity alert system) that ensure this knowledge is leveraged for the benefit of cyber users.	Concur
14	Recommendation: The CISA Director should task the CISA General Counsel (with assistance of the Office of the National Cyber Director chaired cyber lawyers’ council) to examine and recommend a legal framework, incentives, and protections connected to sharing and acting on cyber threat information.	Non-Concur
15	Recommendation: Work with the Office of Personnel Management to obtain access to relevant and appropriate survey and employee data collected from CISA employees. A short technical sprint, in cooperation with OPM and CISA legal counsel, could provide options for OPM to securely share data with CISA about their employees. CISA must be able to access and analyze survey engagement data from its own employees, for the benefit of its workforce.	Concur
16	Recommendation: The OPM survey data will be helpful but may not provide everything needed for CISA to strengthen employee engagement. As such, CISA should develop and manage its own approach to developing a full-scope employee engagement survey.	Concur
17	Recommendation: Gain access to comparative external employee engagement information for benchmark purposes.	Concur
18	Recommendation: CISA’s Chief People Officer and Chief Human Capital Officer should create a working group within the agency, comprised of key leaders and mission support personnel, to continually identify, modify, and validate key metrics CISA uses to measure engagement. Additionally, this group should review and validate the tools used to capture this data.	Concur
19	Recommendation: Drive greater value from CISA’s Employee Association Groups (EAGs) to support employee wellbeing, build community, and enhance culture.	Concur
20	Recommendation: Provide opportunities for employees to propose an EAG-in support of employee wellbeing and building an inclusive culture.	Concur
21	Recommendation: Leverage data from programs that provide quantitative detail around current workloads and employee capacity such as Microsoft Viva to gain insight into employee wellbeing and help address unreasonable workloads.	Non-Concur

22	Recommendation: Implement an employee-driven recognition program that allows employees to recognize each other's exemplary performance, provide a measure of success for achievement, and take an active role in promoting CISA's culture.	Concur
23	Recommendation: Establish a working group that benchmarks CISA's approach to employee support against the private sector's approach on a regular basis.	Concur
24	Recommendation: Formalize and educate employees on organizational growth paths and career progressions to provide more structure and clarity around development.	Concur
25	Recommendation: Build a cohort-based continuous learning opportunity to upskill employees in key areas of strategic interest while also driving culture through connection.	Non-Concur
26	Recommendation: Establish internal events (like Capture the Flag competitions) that provide the broader organization with the chance to deepen their cyber skillsets through access to CISA's cyber range or other cyber-specific training tools.	Concur
27	Recommendation: Create people manager specific training pathways to equip them with the tools needed to support employee wellbeing and reinforce the importance of their role in proactively identifying and addressing employee burnout.	Concur
28	Recommendation: Leverage the NICE Framework Career Navigation Pathways to align job roles and responsibilities more closely to widely accepted industry framework and make it easier for external talent to join CISA as part of their career progression.	Concur
29	Recommendation: Create more opportunities for team members to share feedback on their managers to gain insight into leadership effectiveness and empower employees to feel more ownership of CISA's culture.	Concur
30	Recommendation: Conduct Exit Interviews vs. exit surveys to better understand the motivations of people separating from CISA.	Concur
31	Recommendation: As part of CISA's ongoing efforts to amplify their cultural principles and values, CISA should gather a small working group of key senior stakeholders to identify opportunities for remote and hybrid employees to actively engage with the culture. This will help to drive a sense of cultural ownership and support adoption of the culture.	Concur
32	Recommendation: Develop a remote/hybrid on-boarding program that provides structure for new employees and a checklist of essential actions, trainings and learning modules that they need to complete.	Concur
33	Recommendation: Host a weekly welcome meeting for new joiners led by senior leadership to reinforce the cultural messages received during onboarding and make them feel like part of the team.	Concur
34	Recommendation: Intentionally bring teams together on a regular basis for the kind of collaboration and culture building that is best done in person such as larger meetings, project-specific work and team development days.	Concur
35	Recommendation: Implement an internal talent marketplace to facilitate internal mobility, help increase transparency and democratize opportunities for career development. A platform like this allows employees to own their own careers while upskilling CISA's workforce.	Concur
36	Recommendation: Identify career development opportunities that support volunteerism efforts, giving employees the chance to blend their passion and profession while supporting communities that lack the ability or knowledge to effectively secure themselves— including those that are target-rich, cyber-poor such as hospitals, K-12 school districts, or nongovernment organizations (NGOs).	Non-Concur
37	Recommendation: Develop multi-year strategic development rotations for talent to gain interdisciplinary experience.	Concur

38	Recommendation: Support the expansion and usage of a tour-of-duty program that enables talent swapping 1) between CISA and the private sector and 2) within government agencies. As part of this, CISA must gain insight into current program usage, areas of opportunity for improvement, and barriers to usage.	Concur
39	Recommendation: Establish a working group of senior CISA leaders to evaluate emerging technologies and incorporate it into their plans to reskill, upskill, and cross-skill the CISA workforce.	Concur
40	Recommendation: Review the current approach to employee development to ensure that employees have access to a variety of relevant and effective trainings that are both experiential, hands-on training and more traditional academic training.	Concur
41	Recommendation: CISA serves as the unifying voice for security guidance.	Concur
42	Recommendation: Define sector specific communications that are themed around “Understanding. My Risk & Readiness”.	Concur
43	Recommendation: Create a roadmap to action to overcome financial barriers.	Non-Concur
44	Recommendation: Establish key security metrics.	Concur
45	Recommendation: Engage with a diverse set of NGOs that provide support to high-risk civil society organizations. To gain a better understanding of how they support civil society, ask about: (A) What the organization does and how it operates, how it works with civil society organizations, what it offers proactively and why, what it offers reactively, the resources it’s able to dedicate to this effort, constraints such as budget, resources, relationships, insight. (B) How CISA and industry partners can help support them by sharing information, connecting organizations for mutual support while promoting their efforts.	Concur
46	Recommendation: Engage with U.S. nationals who have been targeted by nation-state actors using sophisticated spyware to learn from their experiences.	Concur
47	Recommendation: Engage with academic researchers that study the security of individuals from high-risk communities to facilitate their interactions with and research on the needs of said high-risk communities. Response: Concur. This is on-going work for CISA, and therefore we believe the recommendation may be marked as completed. Through the JCDC HRCF Planning Effort in FY23, CISA has engaged with security researchers at academic institutions (e.g., Citizen Lab) as well as universities with cyber volunteer clinics (e.g. Berkeley Center for Long-term Cybersecurity) to better understand the needs of high-risk communities, advocate for industry action, and build capacity at cyber volunteer clinics to support high-risk communities. CISA through the HRCF initiative would like to continue to build on this work in coming years and will only constrained by lack of resourcing.	Concur
48	Recommendation: Work with the State Department’s Internet Freedom program to assist them helping high-risk communities overseas.	Concur
49	Recommendation: Define the scope of the communities and threats that CISA will focus on initially.	Concur
50	Recommendation: Initially prioritize entities that can multiply CISA’s efforts through “train the trainer” and act as trusted partners and gateways to the smaller entities.	Concur
51	Recommendation: Prioritize the protection of life and minimize physical harms.	Concur
52	Recommendation: Prioritize harms that can stop or undermine the effectiveness of organizations and communities’ work in the public sphere.	Concur

53	Recommendation: Prioritize preventive defense guidance to high-risk communities.	Concur
54	Recommendation: Push out tools and how-to materials to enable low resourced organizations and individuals to evade spyware used by oppressive governments and violent organizations targeting their demographics.	Concur
55	Recommendation: Create a high-risk reporting form online that requests certain information and shows people what to watch for and report for assistance in determining if they're being targeted and how aggressive the entity is going about targeting them.	Concur
56	Recommendation: Identify, promote, and fund tools to help communities and organizations self-assess their cyber maturity and risk levels. For example, look to the Ford Foundation's Cybersecurity Assessment Tool as a starting point.	Concur
57	Recommendation: Identify, promote, and fund 'One and Done' ways to increase protections, such as advanced protection features on phones, with explicit step-by-step instructions.	Concur
58	Recommendation: CISA should build on the success and visibility of the Shields Up guidance and (A) Expand it into a "Wizard-like" resource that will forward organizations of sufficient risk level to further technical security recommendations. (B) Gather information necessary to identify mitigation gaps, and encourage the development of further mitigations. (C) Create a series of best practices and resources that civil society can use when the preventive side of this has failed, or when the civil society organization got engaged post-compromise.	Concur
59	Recommendation: Field questions from HRC entities as they determine their risk level. CISA would fill a critical lack here, as there is a current significant gap in technical resources for such determination.	Concur
60	Recommendation: Connect an HRC entity with a list of security vendors, open-source projects, and other resources that may be needed at that entity's risk level. This is a natural effect of CISA's positioning in between these communities.	Concur
61	Recommendation: Connect government entities with HRC entities for the former to better understand the latter's needs and stature. As a government entity, CISA may carry enough internal weight to effectively support such conversations.	Concur
62	Recommendation: Connect academics to HRC entities to facilitate academic studies in HRC risk management and defense. CISA's relationship with HRC entities can significantly improve the reach and applicability of academic studies on the topic and augment our understanding of risk among these communities.	Concur
63	Recommendation: Provide threat modeling information to the HRC community to help them fully understand their threat and what is a worthwhile tradeoff for the loss of functionality for additional tech protections.	Concur
64	Recommendation: Develop a way to provide information to HRC at an organizational level, as well as high-risk individuals directly.	Concur
65	Recommendation: Work with partners and industry to alert HRC of detected targeting, such as what Google Gmail does when they detect a foreign adversary attempting to compromise your email account. This alert would warn the end user to move to the next level of protection, provide actionable recommendations for self-help such as revoking other linked device permissions and then signing out and back in to get a new login token.	Concur
66	Recommendation: Provide a mechanism for people to suggest tools and guidance for CISA to review and include in their recommendations.	Concur
67	Recommendation: Develop a life cycle to keep in touch with providers and high-risk groups to evolve these recommendations based on real world experiences.	Concur

68	Recommendation: Continue to enable, require and push for increased security-by-default features turned on for products and devices out of the box especially for end consumers and small or low resourced user base.	Concur
69	Recommendation: Push product vendors to consider creating slimmed down small org and non-technical user versions of their products and solutions for the end consumer, non-profit and low resourced organizations to move them off of enterprise solutions.	Concur
70	Recommendation: Create a way to recognize companies which participate in HRC protection programs.	Concur
71	Recommendation: Promote collaboration amongst these companies to share threat intelligence.	Concur
72	Recommendation: Produce a report on the board director education gap. As soon as practicable, CISA should initiate a collaboration with relevant stakeholders to produce a data-driven report that enumerates the cyber literacy gap in the boardroom.	Concur
73	Recommendation: Establish expected levels of cybersecurity knowledge for board directors. CISA, in coordination with other stakeholders, should create and promote an expectation of the baseline level of knowledge about cybersecurity all directors should have and should create recommendations for a standardized cybersecurity curriculum for directors to be incorporated into training offerings.	Concur
74	Recommendation: CISA, in coordination with other stakeholders, should determine levels of cybersecurity proficiency for directors above the baseline level of knowledge referenced above.	Concur
75	Recommendation: Expand and enhance training. As soon as practicable, CISA should work with relevant stakeholders to expand and tailor existing educational offerings for directors to ensure all directors have the recommended baseline level and to help more directors attain higher levels of cybersecurity proficiency.	Concur
76	Recommendation: Deliver training at scale. CISA, in coordination with other stakeholders, should encourage and help lead the creation of a centralized cyber education platform, including creating content into which all stakeholders can integrate. This will provide stakeholders with a continuous method for enhancing their cyber literacy.	Concur
77	Recommendation: Promote director certification and accreditation. CISA should encourage the broader adoption of cybersecurity certifications and accreditations like what is offered today by NACD, ISC2 and other stakeholders. NACD's certification includes cybersecurity content aligned with business resilience exposures.	Concur
78	Recommendation: CISA should use its influence and voice to encourage companies to look for this certification in selecting directors and to weigh the attainment of this certification in their director selections.	Concur
79	Recommendation: Educate about business imperative. CISA should work with partners to develop quantitative and qualitative analyses demonstrating the relationship between inadequate cybersecurity programs and business and operational risk and by actively and broadly discussing and promoting this concept among all stakeholders.	Concur
80	Recommendation: Expand and enhance training for other stakeholders.	Concur
81	Recommendation: CISA should work with other relevant federal agencies and stakeholders to generate Principles for Cyber-resilient Investing, the purpose of which shall be to bring cyber resilience to the forefront of investor decision-making. These principles could be modeled after the Principles for Responsible Investment developed in 2006 by an organization affiliated with the United Nations, the purpose of which was to promote the incorporation of environmental, social, and corporate governance factors (ESG) into investment decision-making.	Non-Concur
82	Recommendation: Identify data deficiencies. CISA should work with other stakeholders to identify areas where data is deficient and to seek new data sources for these.	Concur

83	Recommendation: Measure director engagement. CISA, in collaboration with relevant U.S. agencies, should develop a list of research and data that is necessary to assess directors' level of education and engagement on matters of cybersecurity oversight.	Concur
84	Recommendation: CISA, in partnership with relevant agencies and stakeholders, should promulgate guidance on how to measure director engagement and director effectiveness in executing their responsibilities.	Concur
85	Recommendation: Measure the effectiveness of communications. CISA should determine what data and metrics are needed in this area, and then develop guidance on best practices in communications between management and boards, including what level of technical detail and preferred formats and modes for transmission of such information. Response: Concur. CISA agrees that this is important work, however, there are currently resource limitations on CISA's ability to implement this recommendation.	Concur
86	Recommendation: CISA should develop a subset of this guidance as it pertains to directors of non-public companies.	Concur
87	Recommendation: Measure the effectiveness of board oversight.	Non-Concur
88	Recommendation: Measure enterprise cyber risk.	Concur
89	Recommendation: CISA, in partnership with the White House and SEC, should consider whether corporations should be required to adopt CPGs as the cybersecurity risk management framework against which they must report. This requirement could apply to all publicly traded companies or could apply only to those that are not already required by a U.S.-based regulatory agency to implement a NIST-based set of cybersecurity controls.	Concur
90	Recommendation: CISA, in partnership with public and private sector stakeholders, should hold a series of workshops demonstrating how companies effectively implement the CPGs or other cybersecurity risk management frameworks.	Concur
91	Recommendation: Manage risk transfer. CISA should study the criteria used by underwriters in setting cybersecurity insurance policies and establish practices for managing risk via the risk transfer markets to understand the role of risk transfer more accurately in influencing corporate and director behavior and to inform the promulgation of guidance recommended elsewhere in this report.	Non-Concur
92	Recommendation: Utilize third party assessments. CISA should promulgate guidance that includes best practices and recommendations for how companies can successfully incorporate such capabilities into their cyber risk assessments.	Concur
93	Recommendation: Stay neutral on cyber risk ratings by credit rating agencies. CISA should not encourage credit rating companies to establish ratings of companies' cyber risk.	Concur
94	Recommendation: Help directors build better understanding of business impact. CISA should create materials that explain the loss and liability to companies for certain types of cybersecurity events.	Concur
95	Recommendation: CISA should create methods for directly linking certain actions and non-actions, as well as investments and failure to invest, to potential cyber risk and then, in turn, communicate that risk in dollar amounts.	Concur
96	Recommendation: CISA should conduct and publish research on this question and in doing so, should ask the industry to collaborate and provide data.	Concur
97	Recommendation: Generate more relevant and accurate data. CISA should create such a data set and continually update it, with assistance from the Information Sharing and Analysis Centers (ISACs) and the insurance industry.	Concur

98	Recommendation: Create Performance Goals for Cyber-Responsible Boards. CISA, in collaboration with relevant stakeholders, should create Performance Goals that contain a set of principles and accompanying best practices for cyber-responsible boards to help directors focus their efforts and attention and help their firms improve cybersecurity outcomes.	Concur
99	Recommendation: Create common controls, measurements, and reporting. Consistent with the recommendations included in Pillar II/(Measure enterprise cyber risk), CISA should work with the White House and the SEC to consider whether the CPGs should serve as the prevailing baseline of controls against which determinations of material weaknesses (MWs) and significant deficiencies (SDs) are made for the purposes of SEC reporting, whether for all companies or only for those that are not already required by a U.S.-based regulatory agency to implement a NIST-based set of cybersecurity controls.	Non-Concur
100	Recommendation: Amend CPGs to include flow-down to suppliers and encouragement of secure-by-design. CISA should adapt the CPGs to include, under “Vendor/Supplier Cybersecurity Requirements,” questions to suppliers and potential suppliers regarding their board governance practices (to determine how much oversight their boards provide and how engaged they are on cybersecurity matters) as well as questions about their implementation of a widely accepted cybersecurity risk management framework.	Concur
101	Recommendation: CISA should adapt the CPGs to include guidance to software and hardware manufacturers to follow the secure-by-design and secure-by-default principles and approaches created by CISA.	Concur
102	Recommendation: Promote greater use of checklists by auditors. CISA should encourage the inclusion of these broadly and through the CPGs to elicit more board engagement and accountability.	Non-Concur
103	Recommendation: Greater clarity on due diligence and liability. In addition to efforts to support the adoption of the CPGs as the common set of controls for publicly traded companies, CISA should create guidance for directors on what constitutes due diligence when it comes to cybersecurity.	Non-Concur
104	Recommendation: CISA should help define for boards and management the legal frameworks to help them navigate personal and organizational liability issues.	Non-Concur
105	Recommendation: CISA should simultaneously work with relevant federal agencies and stakeholders to determine what barriers exist to shareholders’ pursuing class action lawsuits against companies for weak cybersecurity programs that result in harm to them or their customers.	Non-Concur
106	Recommendation: Assign a high-level leader and staff. As soon as practicable, CISA should designate an official under its Cybersecurity Division (CSD) to lead a line of effort around increasing national corporate cyber responsibility.	Concur
107	Recommendation: Create an awareness campaign.	Concur
108	Recommendation: CISA should create an awareness campaign to encourage a nationwide culture of corporate cyber responsibility. Through this campaign, CISA should solicit feedback from relevant stakeholders and promote the resources it and its partners have created to foster and enable stronger board engagement.	Concur