May 21, 2024

MEMORANDUM FOR THE CYBERSECURITY ADVISORY COMMITTEE MEMBERS

FROM: Jen Easterly
Director
Cybersecurity and Infrastructure Security Agency (CISA)

SUBJECT: **Formal Response to Recommendations Provided on December 5, 2023**

The Cybersecurity Advisory Committee (CSAC) was established in June 2021 to advise, consult with, report to, and make recommendations to 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 to provide strategic recommendations, leveraging their members' significant subject-matter expertise, for CISA's cybersecurity mission.

CISA values the hard work of the CSAC that led to a previous set of actionable recommendations to improve on CISA's execution of its cybersecurity mission. The continued expert advice and key insights that the CSAC offers will enhance the work of CISA and keep 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 legal parameters of CISA's operating authorities and resources. Our response to each subcommittee is as follows:

Response to the Technical Advisory Subcommittee
Recommendations 1 – 27

We agree that CISA is uniquely positioned to drive consistent messaging and encourage all stakeholders to adopt safer and more secure practices, especially when it comes to memory safe technologies. Through our work with the research and development community, the inter-agency, and the private sector, we will promote memory safe system language (MSSL) and will expand our Secure by Design initiative to address many of the recommendations this subcommittee provided.

While CISA concurs with most of the recommendations provided, we do non-concur with recommendations we believe are non-actionable, such as due to lack of resources or authorities.

Response to the Building Resilience and Reducing System Risk to Critical Infrastructure Subcommittee
Recommendations 28 – 29

CISA appreciates the work of this subcommittee to expand upon the previously provided recommendations. As noted in our previous response, a model for operational collaboration is critical, and the additional information and recommendations provided by this subcommittee will help ensure a framework and maturity model that will allow CISA and its partners to be most successful.

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	ECD
1	**Recommendation**: Work with the R&D ecosystem across government and industry to create and update tools that enable usage of memory safe features of existing languages and hardware.	Concur	Complete
2	**Recommendation**: Add memory safe tools to CISA's existing GitHub to highlight open-source solutions.	Non-Concur	N/A
3	**Recommendation**: Advocate for memory safety in Computer Science, Embedded Systems and Engineering education curricula, for example by maintaining a list of university curricula that include memory safety coursework as well as incentivizing ongoing education of memory safe languages.	Concur	9/30/2024
4	**Recommendation**: Continue to develop and expand the existing CISA "Secure By Design" initiative, publishing memory safe migration roadmaps and supporting materials, including cost/benefit analysis to help inform company transition plans.	Concur	TBD
5	**Recommendation**: Conduct performance studies and comparison between MSSL vs. legacy languages to help answer performance and cost concerns within embedded device communities.	Concur	9/30/2025
6	**Recommendation**: Create a memory safety council that invites both embedded and general computing stakeholders and educators to the table. Should include silicon, RTOS and general computing stakeholders to ensure coverage of both ICS OT and IT ecosystems.	Non-Concur	N/A
7	**Recommendation**: Encourage industry standards groups to take on memory safety standardization efforts.	Concur	TBD
8	**Recommendation**: Advocate for memory safety in education curricula.	Concur	TBD
9	**Recommendation**:Advocate within government for funding to help support the foundations that support key MSSL projects, such as the Rust Foundation.	Non-Concur	N/A
10	**Recommendation**: Work to ensure that independent regulatory agencies like FERC, FCC, FTC, FDA, EPA adopt cyber regulations that enable and do not degrade memory safety efforts throughout the supply chain. This may involve assisting in reviewing existing regulations for items that may run counter to the adoption of MSSLs.	Non-Concur	N/A
11	**Recommendation**: Work with government standards organizations to develop standards that include the use of memory safety technologies and assist in reviewing existing standards to identify any that run counter to memory safety adoption.	Concur	TBD
12	**Recommendation**: Ensure existing FFRDC efforts implement CISA memory safety recommendations and practices and produce or update tools to further enable memory safe adoption.	Non-Concur	N/A
13	**Recommendation**:CISA should make recommendations to DHS and OMB procurement councils to include piloting memory safe product requirements in their cyber security purchasing requirements for providing products and services to all federal agencies.	Concur	TBD
14	**Recommendation**:Collaborate with NIST for the consideration of memory safety updates to the existing requirements in NIST SP 800-53 Security and Privacy Controls for Information Systems and Organizations, SP 800-161 Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations, SP 800-218 Secure Software Development	Concur	9/30/2024

	Framework (SSDF) and similar guidelines.		
15	**Recommendation**: CISA should recommend to DHS S&T to fund pilot projects to help industry create memory safe tools and products to increase the availability of memory safe products on the market.	Concur	6/30/2024
16	**Recommendation**: CISA should request the inclusion of memory tagging technologies into the roadmap of all major silicon vendors powering cloud, pc, mobile, and IoT devices leveraged in national infrastructure.	Concur	9/30/2024
17	**Recommendation**: Request compiler and IDE vendors, both open-source and commercial, to default to secure options such as Span, InitiAll, and Castguard for C/C++ compilers and common libraries (C/C++ Standards).	Concur	TBD
18	**Recommendation**: Collaborate and fund workforce projects with academia and open-source communities for migrating to MSSL, and related tools necessary to implement memory safety features of legacy languages in C and C++ libraries.	Non-Concur	N/A
19	**Recommendation**: Encourage accreditation bodies to include memory safety concepts in Computer Science and Systems Engineering degree program guidelines.	Concur	9/30/2024
20	**Recommendation**: Help identify and fund or study outstanding issues slowing adoption in MSSL.	Concur	TBD
21	**Recommendation**: CISA, in coordination with others, should publicly signal to decision makers that memory safety is important, and decision makers should pay attention, through actions such as those identified in this report.	Concur	Complete
22	**Recommendation**: Encourage the development of white papers, research reports, and supporting documentation to assist decision makers in having the information necessary to justify investing in memory safety and provide a public repository for this documentation.	Concur	TBD
23	**Recommendation**: Educate executives in existing critical infrastructure sector coordinating councils on the need for MSSL, including in the supply chain.	Concur	9/30/2024
24	**Recommendation**: Update the existing CISA SBOM and HBOM guidance to require disclosure of details (all, some, or none as an example) if each component was developed with MSSL or technologies to better inform consumers of product capabilities.	Concur	12/31/2024
25	**Recommendation**: CISA should recommend that incentives like legal safe harbors for following best security practices that can help encourage industry to move toward memory safety, be included in legal and regulatory decisions that may adopt best security practices. CISA should advise legal and regulatory agencies to be sure that these practices are standards agnostic, future focused, and do not create perverse incentives, such as abandoning software projects to avoid potential liability.	Non-Concur	N/A
26	**Recommendation**: As part of the Secure By Design initiative create or support a public tracker that lists what important software is available in a MSSL to create public awareness and peer pressure.	Concur	9/30/2025
27	**Recommendation**: Include the academic community and connect them with industry and government through efforts such as sponsoring workshops on memory safety with the top academic conferences.	Concur	9/30/2025

28	**Recommendation**: CISA should create a framework that: • Makes explicit and emphasizes the need to incentivize collaboration with increased transparency on the roles and responsibilities, capabilities, and authorities of the private and public sector partners involved. • Is broad and flexible enough to include all 16 critical infrastructure sectors/subsectors. The sectors are organized differently and have unique priorities and diverse needs. A standard should take those differences into consideration. • Aligns with similar standards used by the USG to coordinate responses to physical threats (i.e., FEMA's National Preparedness System and National Response Framework). • Is based on a cybersecurity response to a disruption no matter the cause (e.g., the cybersecurity repercussions of a natural disaster, etc.). • Encompasses steady state and incident response collaboration. • Recognizes the differences between the ways different USG agencies collaborate with the private sector and clarifies the roles in those relationships. • Outlines a mechanism for governance. • Describes what successful collaboration looks like at the strategic, risk mitigation, and operational levels. Include the public policy efforts that levels.	Concur	9/30/2025
29	**Recommendation**: CISA should create a maturity model that: • Measures Cybersecurity Collaboration at risk, strategic, operational and public policy levels. • Defines the planning horizons associated with each level of collaboration (e.g., risk is immediate/crises response, strategic is planning for likely incidents, operational is continual partnership, etc.). • Includes steady state and incident response collaboration. • Defines maturity as a repeatable process. • Includes guidance on successful governance structures.	Concur	9/30/2025