February 20, 2024

RESPONSE TO CISA REQUEST FOR INFORMATION ON
"SHIFTING THE BALANCE OF CYBERSECURITY RISK:
PRINCIPLES AND APPROACHES FOR SECURE BY DESIGN SOFTWARE"[1]

The Association for Computing Machinery (ACM), founded in 1947 as a non-profit and non-lobbying organization, is the world's largest and longest-established society of individual professionals involved in virtually every aspect of computing. Our over 50,000 members in the United States and 100,000 worldwide serve in government, industry, academia, and the public sector. Many have pioneered and continue to pursue work on the cutting edge of computing, including artificial intelligence.

USTPC strongly endorses security as a first principle in software development to ensure that customers and their data are appropriately protected. ACM's Code of Ethics and Professional Conduct states that computing professionals should "[d]esign and implement systems that are robustly and usably secure."[2] Further, the ACM Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity of 2017 include a comprehensive guide to knowledge units and topics to train fundamental design principles.[3]

Through its U.S. Technology Policy Committee (USTPC), ACM strives to provide apolitical technical expertise and analysis to Congress, the Executive Branch, and policymakers throughout government to inform technology policy. Consistent with this mission, USTPC is pleased to offer the following general recommendations[4] in response to the Cybersecurity and Infrastructure Security Agency (CISA), Department of Homeland Security (DHS)'s *Request for Information on Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software (RFI)*:[5]

---

[1] See 88 FR 88104 (December 20, 2023) [https://www.federalregister.gov/documents/2023/12/20/2023-27948/request-for-information-on-shifting-the-balance-of-cybersecurity-risk-principles-and-approaches-for].

[2] See https://www.acm.org/code-of-ethics

[3] See https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf

[4] These comments were principally drafted for USTPC by Security Subcommittee member Josiah Dykstra and Subcommittee Chair Carl Landwehr. USTPC Vice Chair Jody Westby also substantially contributed to them.

[5] USTPC notes that the RFI is a revision of the version released in April 2023. It introduces substantial new material that provides explanations and demonstrations of how each of the three guiding principles might be realized in practice in software design, software configuration, and in certain business practices. Overall, the new material is a valuable contribution to the document. Some of the new material repeats what can still be

1) More Explicitly Acknowledge Human Factors in Secure by Design Software Development

Hardware and software exist to facilitate accomplishing users' primary tasks and critical functions, from the delivery of healthcare to private information sharing. Such uses, however, can also adversely affect the privacy of individuals whose private data is being accessed CISA's guidance recommends field tests to "... gain valuable insights into the usability and effectiveness of their security features and controls." While user feedback is a useful byproduct of field tests, USTPC recommends attention to human factors as a first principle throughout the software development lifecycle rather than considering and applying such factors only in field tests late in the development cycle.

By integrating human factors from the outset, developers can anticipate and mitigate privacy risks and potential security vulnerabilities that arise from use of the data or user interactions, thereby designing systems that are not only technically secure but also intuitive and resilient against social engineering attacks and compliant with privacy and security legal requirements. This approach fosters a culture that accommodates the diversity of user behavior, accessibility needs, and data analytic methods, ensuring that security measures are considered from software design to retirement and that they do not become obstacles to productivity or privacy hazards. Ultimately, prioritizing human factors as a first principle in software development bridges the gap between human and technological capabilities, creating a symbiotic relationship in which each enhances the effectiveness of the other. Such symbiosis will lead to more robust and inherently more secure systems.

2) Incorporate Standards for Privacy by Design

USTPC recommends the addition of Privacy by Design as an additional principle throughout the white paper. Privacy by Design was first introduced in 2009 and requires the consideration of privacy in the software development lifecycle. The seven principles of Privacy by Design include end-to-end security.[6] Security by design expands this concept beyond privacy and requires security to be considered throughout the system development lifecycle.

By empowering users with transparency and control, Privacy by Design inherently strengthens the overall security posture. It minimizes exploitable attack surfaces and reduces the likelihood of compliance violations. Ultimately, this approach promotes a digital environment where users and data can coexist harmoniously, ensuring both resilience against threats and respect for individual

found in the Secure by Design and Secure by Default "tactics" sections near the end of the document, but the redundancy is not harmful.

[6] "Privacy by design," Wikipedia (accessed 2-14-24), https://en.wikipedia.org/wiki/Privacy_by_design.

rights. This approach helps guarantee that information protection remains paramount without compromising the fundamental right to privacy.

3) Address the Government's Role in Incentives

At present, the RFI merely urges manufacturers themselves to create "meaningful internal incentives." Governments should assume responsibility for, and affirmatively seek to leverage, the adoption of principles for both Privacy by Design and Security by Design principles.

Government has a further role in the collection of cybersecurity statistics that could foster evidence-based policy and decision making. We note that CISA affirmatively calls "on manufacturers to not just focus on their internal efforts, but to objectively measure and regularly report the results and effectiveness of a product's security efforts and configurations, and to build a feedback loop that creates changes in the SDLC that lead to measurable improvements in customer safety and more secure products." USTPC submits that the government should actively contribute to thought leadership in the science and practice of meaningful software development and privacy and cybersecurity statistics.

USTPC stands ready to further assist CISA. Should questions arise concerning this document, or to arrange a technical briefing with ACM and USTPC's expert members, please contact ACM's Technology Policy Office at acmpo@acm.org or 202-580-6555.