ACM US Public Policy Council

Association for Computing Machinery (ACM)
US Public Policy Council of ACM (USACM)

1828 L Street NW, Suite 800
Washington, DC 20036
Main Phone: 212-626-0541
acmpo@acm.org

Cybersecurity Legislation

Similar to members of Congress, we are very interested in ensuring a more secure cyberspace. We recognize and appreciate the work put into the cybersecurity legislation currently under consideration. We do not want that effort to go to waste. We share Congressional concerns that our current Federal cybersecurity policies are not adequate to address the threats against our cyber infrastructure. Speaking on behalf of the computing discipline that is on the front lines of this battle, we urge that whatever new laws emerge from Congress takes into account the following general recommendations:

USACM supports appropriate protections for personally identifiable information (PII) within any information sharing process. Sharing of threat and incident information can greatly benefit organizational stakeholders. However, doing so should not come at the expense of vastly increased privacy risk to individuals. Irrelevant PII should be removed from information prior to sharing. PII that is not removed must be safeguarded with effective technical as well as administrative controls, and must not be used for unrelated purposes. These practices are consistent with our long-standing privacy recommendations, which themselves are consistent with internationally recognized Fair Information Practice Principles that the U.S. pioneered.

USACM supports recognizing the legitimacy of all types of risk management response in any risk-based approach. The desire to mitigate all identified risks is an understandable one, but usually does not produce the most effective results. Depending on the circumstances, including the severity of the risk and the cost of mitigation, it may make more sense to simply accept the risk or to transfer it through such mechanisms as insurance. We caution against any approach that unnecessarily restricts risk management options.

USACM opposes broad certification requirements for cybersecurity professionals. Previous cybersecurity proposals have included provisions for a complex, untested, and mandatory certification regime for public and private cybersecurity practitioners. We believe it is premature to require a massive new certification program without careful review of the feasibility and side effects of any such program, and thus we would support a formal study along these lines.

USACM supports including systems analysis and design in cybersecurity education. Training in narrow techniques for specific networks and/or systems has its place in cybersecurity education, but it is only one facet of such education. It is not enough to focus on the symptoms of cybersecurity problems. A broader education that includes systems analysis and design is critical to prepare cybersecurity professionals for designing, implementing, and protecting the systems upon which we rely. In particular, the Scholarship for Service program has been an important educational tool in preparing the future workforce, and we encourage continued support for it.

USACM supports targeted cybersecurity standards. Given the different challenges in different sectors of cybersecurity practice, any effort to establish effective standards will need to take those variations into account. Encouraging the establishment of standards commensurate with risk is the right way to approach such an effort, but the effort should be explicit about recognizing the differences across systems. Targeted sets of standards will be more effective than a single set of standards intended to cover all systems.

USACM supports continued Federal encouragement of research and development. We welcome additional encouragement for Federal support of cybersecurity research. We caution, though, against specifying research problems. The field is still too young to be able to map out research trajectories in such a granular fashion. More general recommendations, such as "research to develop metrics and decision tools to support better understanding of cyber risk, security tradeoffs, and consequences of cyber incidents" would be more beneficial and provide sufficient guidance to knowledgeable funding agencies.

We appreciate the concern you and your colleagues have about our cybersecurity risks and think carefully crafted legislation will be helpful in improving the nation's cybersecurity. Please contact our Public Policy Office at 212-626-0541 if we can be of further assistance in this difficult task.

About ACM and USACM
With over 100,000 members, the Association for Computing Machinery (ACM) is the world's oldest and largest educational and scientific computing society. The ACM U.S. Public Policy Council (USACM) serves as the focal point for ACM's interaction with U.S. government organizations, the computing community, and the U.S. public in all matters of U.S. public policy related to information technology.