usacm ACM US Public Policy Council

COMPUTING RESEARCH ASSOCIATION CRA

March 22, 2010

The Honorable John Rockefeller	The Honorable Kay Bailey Hutchison
Chairman	Ranking Member
Senate Commerce Committee	Senate Commerce Committee
508 Dirksen Senate Office Building	508 Dirksen Senate Office Building
Washington, D.C. 20510	Washington, D.C. 20510

The Honorable Olympia Snowe
United States Senate
154 Russell Senate Office Building
Washington, D.C. 20510

Dear Senators Rockefeller, Hutchison, and Snowe

We wish to express our deep concerns regarding several key provisions in the most recent manager's amendment to S. 773 released last week. While we agree with the overall goal of the bill – a more secure cyberspace – the current draft continues to rely on ideas that will undermine this goal. We specifically are concerned about three provisions: 1) required certification of cybersecurity professionals, 2) a continued emphasis on training vs. education, and 3) a real-time "dashboard" of security vulnerabilities for federal agencies.

In January, USACM and CRA sent you a detailed letter with our recommendations for improving the December draft the committee circulated, which is attached to this letter. We appreciate the changes that you made that were responsive to our recommendations; however, our core concerns were not addressed by this latest draft. We wish to work with the committee to address these issues.

Specifically, we continued to be deeply troubled by the certification provisions in the bill. The legislation would require a complex, untested, and mandatory certification regime for public and private employers almost immediately after a National Academies study is conducted to determine – and it has not yet been determined - whether such a program would even be feasible. It is premature to mandate the creation of a massive new certification program without the benefit of a careful, deliberate Academies study that examines both the feasibility and side effects of any such program.

We are also concerned about how the bill emphasizes training in narrow techniques rather than an education in holistic systems design. The language on "secure coding" reflects this narrow emphasis. Systems thinking is a critical aspect of designing more secure systems, otherwise attention gets focused on merely the *symptoms* of poor cybersecurity and not the underlying problems.

In addition, we see that there has been no change to the real-time cybersecurity dashboard description. If such a system is feasible, the systems that use it would risk too much exposure to outside threats to warrant its deployment. The need for better risk and threat assessment is well understood, but the dashboard as proposed in the legislation would cause many more problems than it would solve.

We do share the committee's concerns that our current federal cybersecurity policies are not adequate to address nature of the threats against our cyber infrastructure. However, speaking on behalf of the computing discipline that is on the front lines of this battle, we find that some of the key provisions of the legislation are unworkable. They will not serve the computing field and will not address the hard challenges that our country and the world faces in making cyber infrastructure more secure. Some portions of the proposed legislation will make the situation more difficult to correct. We provided several recommendations in our January letter that address our concerns while supporting your goals, and we urge you to adopt them.

Thank you for considering our view. We look forward to a continued dialog with you. If you have any questions, please feel free to contact us directly, or through Cameron Wilson, Director of Public Policy for ACM, at 202-659-9711, cameron.wilson@acm.org.

Sincerely,

Eugene H. Spafford, Ph.D., D.Sc.
Chair
U.S. Public Policy Council of the
Association for Computing Machinery

Stuart S. Shapiro, Ph.D.
Chair
Committee on Security and Privacy
USACM

Eric Grimson, Ph.D.
Chair
Computing Research Association Board of Directors

Attachment: January 20, 2010 letter from USACM and CRA

ABOUT ACM AND USACM

ACM, the Association for Computing Machinery is the world's oldest and largest educational and scientific computing society, uniting computing educators, researchers and professionals to inspire dialogue, share resources and address the field's challenges.

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. USACM responds to requests for information and technical expertise from U.S. government agencies and departments, seeks to influence relevant U.S. government policies on behalf of the computing community and the public, and provides information to ACM on relevant U.S. government activities.

ABOUT CRA

The Computing Research Association is an association of more than 200 North American academic departments of computer science, computer engineering, and related fields; laboratories and centers in industry, government, and academia engaging in basic computing research; and affiliated professional societies. CRA's mission is to strengthen research and advanced education in the computing fields, expand opportunities for women and minorities, and improve public and policy maker understanding of the criticality of computing research in our society.

usacm ACM US Public Policy Council

COMPUTING RESEARCH ASSOCIATION CRA

January 20, 2010

The Honorable John Rockefeller
Chairman
Senate Commerce Committee
508 Dirksen Senate Office Building
Washington, D.C. 20510

The Honorable Kay Bailey Hutchison
Ranking Member
Senate Commerce Committee
508 Dirksen Senate Office Building
Washington, D.C. 20510

The Honorable Olympia Snowe
United States Senate
154 Russell Senate Office Building
Washington, D.C. 20510

Dear Senators Rockefeller, Hutchison, and Snowe

Thank you for the opportunity to submit comments on the proposed changes to your bill, S. 773, the Cybersecurity Act of 2009 (draft of 12/22/09).

The Association for Computing Machinery (ACM)—a leading society for computing professionals—and its U.S. public policy committee (USACM) are leaders in educating the public and policymakers about technology policy issues. We share your concern about the state of cybersecurity in today's computing infrastructure. Several of our members rank among the most senior experts in the nation in issues of cybersecurity, policy, and privacy. Securing cyberspace is a grand challenge for the computing field and we thank you for the attention you have brought to this issue through hearings and legislation.

Joining us in this response is the Computing Research Association (CRA), an association of more than 200 North American (principally U.S.) academic departments of computer science, computer engineering, and related fields; major laboratories and centers in industry, government, and academia engaging in computing research; and the leading professional societies in computing.

We agree with the overarching goal of S. 773—that of a more secure cyber infrastructure—and find many positive aspects of the legislation supporting that goal. As cybersecurity is a relatively new specialization in a rapidly evolving field, there are too few experienced practitioners and insufficient foundational research results to meet current needs. However, we have concerns about some of the provisions of the legislation, and we have suggestions how they may be made more robust.

In particular, we are deeply troubled by the legislation's provisions that establish requirements for the certification of cybersecurity professionals. We understand the committee's intent is to help mature the field of computer security, and make the field one to which professionals may aspire and to increase public trust in safety critical systems. These are laudable goals; however, what amounts to mandatory licensing of both public and private cybersecurity professionals will actually undercut, not advance, these goals.

Below are more detailed comments on this these issues as they arise in an examination of the December 22, 2009 draft of the committee amendment to S. 773.

Certification (Section 101)

ACM has taken a position that is formally opposed to the licensing of software engineers; for many of the same reasons, USACM was opposed to the certification requirement present in earlier drafts of S. 773. We are gratified to see that the most recent draft of S. 773 includes language directing the National Academies to study certification needs and maturity. However, the legislation then calls on the President to establish a certification regime shortly after delivery of that report. This is certainly premature, as the study may well indicate that the field is still too inchoate to warrant such a formal (and large scale) certification regime, or that certification will have a net negative effect on the industry. Any such legislative action should only occur *after* the delivery of that study, so we *strongly* urge you to drop that portion of the bill.

Additionally, we note that the scope of the proposed study is too narrow. The study should also examine what effects—positive and negative—certification might have, what the economic issues surrounding certification might be, international implications, whether sufficient controls exist to ensure that private-sector-developed certifications remain credible and cost-effective, and other issues that should be considered before taking any Federal actions.

A certification would appear to many as an authoritative claim that the certified individual could effectively secure a network of systems from all threats and guarantee its reliability, dependability, and usability. However, it is our professional opinion that the body of knowledge in computer science/engineering and in cybersecurity is simply not at a point where those claims can be made with any authority. If professionals are certified on a limited body of knowledge this will lead to a false sense of trust in the underlying system. It is also the case that many—if not most—security incidents occur because of user errors, insufficient budget for proper resources, and exploitation of previously unknown flaws: none of these problems will be rectified by certification!

As an example illustrating several of our concerns, consider the Windows operating system. It has been built over time by thousands of programmers, many of whom are outside the US. If used in critical infrastructure any flaws in the code (or in add-ons) will still be present whether or not the operators of that code are certified. Microsoft is highly unlikely to undergo the expense and effort to get all its programmers around the world certified to US government standards, and even if they did they could not afford to rebuild their products from first principles. Their most feasible response might well be to change licensing to state that Microsoft products should not be used in critical infrastructure. Then what? How has the situation been made safer for the public? Having the operators certified will not fix the flaws, and there are no economically viable alternatives in most cases.

(Note that Microsoft has some of the best and most state-of-the-art training and testing programs for security engineering in the industry, globally. It is almost certain that any certification regime imposed by the government would be met and exceeded by Microsoft engineers. Yet, despite that effort and use of the latest commercially viable technologies, there is still a regular succession of security flaws in their products. Rather than reflect negatively on Microsoft, this reinforces our professional conclusion that the field is too immature to support a useful certification regime.)

We note that *training* and *education* are two different processes, and the outcome of these processes is also different. A strong education can subsume the material needed for certifications as well as provide a basis for a career and innovation. Training seldom provides any education or skills beyond the need to master a particular process. Certification based on training is directed to ensuring that individuals have familiarity with current tools, standards, attacks and responses. Certification based on education is more generally intended to ensure that individuals have the deep technical and field background necessary to understand emerging issues, context, interaction with other fields, and long-term trends. Although a few preliminary standards for some training might be developed in the short term, articulation and implementation of materials for educational institutions will take considerably longer, and will also require support for equipment and staffing. Training for certification ages quickly and requires regular expenditure of funds to renew, thus driving up costs for the overall fields. That overall expenditure would be better made in research and increasing the educational infrastructure.

As another issue, requiring certification courses for individuals who have many years of experience—but no recent formal education in the field—runs the risk of forcing out those valuable practitioners because their abilities cannot be assessed in the same way as a new graduate of a particular program. Alternatively, requiring them to take new, repetitive training to meet certification requirements could impose an economic burden, as well as taking them away from critical job functions. This suggests that the NRC study include examination of both a practical "grandfathering" scheme as well as some form of waivers based on a combination of experience and educational background.

The potential logistical and legal challenges to establishing and managing a national certification system are also troubling. The software development process now spans the globe, often with teams working in multiple countries on different components of a larger project. Technology is enabling this flexible work environment and segmentation of productive development is likely to grow. Mandatory certification of U.S. workers would encumber this process and likely erect unintended trade barriers that could make U.S. products and workers less competitive in this growing international market sector. This should be considered carefully before establishing any certification program that will be, de facto or de jure, mandatory.

Certification of cybersecurity professionals is unlikely to affect safety significantly as most software is built by large teams of people who do not know the end use of their product. Often that software is built from other components, or built on COTS/GOTS[1] – products that were not developed as critical technology (or are explicitly labeled as not to be used in critical infrastructure). Thus, when an end-user buys or licenses a product, it may not matter whether the operators of that product are certified—the flaws are already present (and laws, such as the DMCA[2], criminalize examination for any such flaws).

In summary, we endorse the need for a significant study of this complex issue, but we assert that the proposed legislation is flawed by including language requiring establishment of a certification regime before the study results are known. Additionally, the time and scope given for performance of the study are too compressed—given the potential complexity of what must be examined—to ensure that there is

[1] COTS is Commercial Off-the-Shelf and GOTS is Government Off-the-Shelf. Both refer to software that has already been developed and is available for deployment with no customization and minimal configuration.

[2] DMCA is the Digital Millennium Copyright Act of 1998, Public Law 105-304.

real benefit from any near-term Federal action on this topic. Furthermore, we find the implication that any such certification will eventually become mandatory to be quite worrisome.

Scholarship for Service (Section 102)

We support the provisions to codify and expand the Scholarship for Service (SFS) program that is administered by the National Science Foundation. Our members have been very pleased with the quality of students who participate in the program and support its expansion. We want to ensure that universities retain their ability to select students for the program, which is current practice.

We applaud the explicit acknowledgement of resources to fund security clearances. This has been a difficult with the existing program. We note that there is also an issue in ensuring that the educational institutions involved have funding for course development, and for procurement of current, standard commercial cybersecurity products to be used in instruction. We encourage the committee to direct that some of the money authorized under this section may be used for program and infrastructure development in direct support of the educational goals of the program.

We note that the current SFS program has allowed graduates to meet their employment obligation by entering employment at FFRDCs[3] and state government (especially law enforcement agencies), with approval of the appropriate program manager at NSF. We encourage you to include this in the legislation.

Dashboard Pilot Project (Section 203)

The need to see the status of a network, including threats and vulnerabilities, is clear. However, the project described in Section 203 could create more vulnerabilities than it addresses, particularly if it is a real-time system. Making the Dashboard a real-time system will expose it and the network it runs on to outside threats and vulnerabilities: It is not possible to obtain immediate status of the components of a network without having the dashboard connected (in at least a semi-privileged manner) with all elements of that network. The dashboard and all the data streams used to generate it then become targets for exploits because they provide a single focus for access to the rest of the network, and they provide data about where to find current vulnerabilities and shortfalls. Additionally, this combination provides a convenient avenue to provide misleading (and possibly dangerous) information into the systems.

If the real-time dashboard is to be retained in the bill, we urge that the timeline for design and implementation of the pilot be extended. The project, real-time or not, will be complex and our experience leads us to conclude that more than 90 days will be required to develop an effective plan, and more than one year will be necessary to effectively implement the plan. We note that compressed

[3] FFRDC is Federally Funded Research and Development Center; examples include MITRE, Rand, IDA, JPL, and the National Laboratories.

deadlines are often the cause of rushed designs that are put into operation with vulnerabilities from oversight and forced choices.

Cybersecurity Standards (Section 204)

The establishment of cybersecurity standards should be handled with great care. Given the different kinds of challenges in different sectors of cybersecurity practice, any effort to establish effective standards will need to take those many differences into account. The language in Section 204 (b) encouraging the establishment of standards based on risk profiles is the right way to approach such an effort, but the bill should be more explicit about recognizing the differences between systems; different sets of standards for different systems will be more effective than one set of standards to handle all relevant systems. There is a real danger that a single set of standards could result in a "ceiling" rather than a useful "floor" for systems development.

By analogy, consider that firefighting is an important area to have standards, but different standards are needed for fighting chemical storage fires versus forest fires, for fire prevention, and for arson investigation. A single, simple standard would not likely be specific enough to be useful for all these purposes, as well as unusual, but critical, cases.

Study on Identity Management and Authentication Program (Section 209)

Authorization, making sure that an individual trying to do something has been granted the authority to do it, is a critical part of security policies. Security threats that fake or spoof someone's authority to access or use a system can succeed independent of the identity—authenticated or not—of the individual involved. Of the three concepts—identification, authentication, and authorization—research and practice is much more advanced on effective identification and authentication compared to authorization. We recommend that this section be expanded to require the party designated in Section 209 to also examine the interplay of identity, authentication and authorization and whether additional attention needs to be given to authorization issues.

Emphasis on Federal Research and Development (Section 302)

This is an excellent initiative, and we support it. We do wish to make a few suggestions, however. Foremost, we suggest that the wording be changed to *encourage* the Director of the NSF to provide additional emphasis rather than *require* that cybersecurity be given priority. The NSF is an outstanding national resource that provides funding for a large variety of areas of public and national interest. We strongly recommend that the Director, with advice from Congress and the National Science Board, be allowed to continue to determine agency priorities year to year in support of the entire Foundation's mission.

Second, we suggest adding three items to the list in paragraph (a):

9) How to collect and analyze evidence of electronic crimes for law enforcement and response purposes, and how to design and build systems that enable such collection and analysis;

10) How to provide more effective education and training in issues of cybersecurity, cybercrime response, and privacy;

11) Research to develop metrics and decision tools to support better understanding of cyber risk, security tradeoffs, and consequences of cyber incidents.

Paragraphs (b) and (c) on secure coding seem to be appropriate, at least if one observes the quantity of recent problems attributable to flaws in code. However, this is a surface symptom of a deeper problem: little is taught about overall quality issues and secure designs to most students working in programming. As a result, code that is produced is often buggy (and some bugs are used for attacks), and there are often deep flaws in the privacy, authorization, and communications mechanisms. Thus, we urge that these sections be recast to provide emphasis on issues of careful software engineering and design for security, rather than on the rather narrow and simplistic issue of secure coding. This is included in the list in paragraph (e) but should also be included here.

Paragraph (e) should have its list amended to include our items 9 and 10 as suggested above for paragraph (a); our suggested item 11 is already in that list.

Cybersecurity Advisory Panel (Section 401)

Some of the mandate of this panel might well include efforts being conducted under classification by (at least) the Department of Defense, the Department of Energy, the Department of Homeland Security, the Director of National Intelligence, and the Department of Justice. For a comprehensive view of the Federal effort, at least a subset of the panel would need to be cleared and authorized to access appropriate materials and supported in the preparation of a classified (TS/SCI[4]) annex to the main report. We simply note that there are many experts in cybersecurity and privacy in academia and nonprofit organizations who could meet this standard. We leave it to the committee to determine if this should be an explicit item in this provision.

[4] TS/SCI is Top Secret/Sensitive Compartmented Information. SCI is "above top secret" that requires special permission for access and is an intelligence community designation. SAP/SAR (Special Access Program/ Special Access Required) is a similar designation in the Department of Defense.

We appreciate your consideration, and look forward to working with you and your staff in providing expertise in computing and computer science. We would be happy to provide additional response, if asked. We may also assist you in finding experts should you wish to hold any further hearings in this area. If you have any questions, please feel free to contact us directly, or through Cameron Wilson, Director of Public Policy for ACM, at 202-659-9711, cameron.wilson@acm.org.

Sincerely,

Eugene H. Spafford, Ph.D., D.Sc. Chair U.S. Public Policy Council of the Association for Computing Machinery	Stuart S. Shapiro, Ph.D. Chair Committee on Security and Privacy USACM

Eric Grimson, Ph.D.
Chair
Computing Research Association Board of Directors

ABOUT ACM AND USACM

ACM, the Association for Computing Machinery is the world's oldest and largest educational and scientific computing society, uniting computing educators, researchers and professionals to inspire dialogue, share resources and address the field's challenges.

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. USACM responds to requests for information and technical expertise from U.S. government agencies and departments, seeks to influence relevant U.S. government policies on behalf of the computing community and the public, and provides information to ACM on relevant U.S. government activities.

ABOUT CRA

The Computing Research Association is an association of more than 200 North American academic departments of computer science, computer engineering, and related fields; laboratories and centers in industry, government, and academia engaging in basic computing research; and affiliated professional societies. CRA's mission is to strengthen research and advanced education in the computing fields, expand opportunities for women and minorities, and improve public and policy maker understanding of the criticality of computing research in our society.