ROCKEFELLER-SNOWE CYBERSECURITY ACT
SUBSTITUTE AMENDMENT FOR S.773

March 17, 2010

BACKGROUND & WHY THIS LEGISLATION IS IMPORTANT:
Our nation is at risk. The networks that American families and businesses rely on for basic day-to-day activities are being hacked and attacked every day. At this very moment, sophisticated cyber criminals, hackers and attackers are trying to steal our identities, our money, our business innovations, our commercial intellectual property, and our national security secrets. Too often these cyber enemies are successful. Their methods are growing more sinister and elusive. These cyber enemies seek not only to steal our secrets, but to disrupt and disable America's networks and destroy our way of life.

This 21st century threat calls for a collaborative 21st century response from our government, our private sector, and our citizens. Even the most high-tech companies can't defend themselves against the most sophisticated attackers. Everyone must get involved. The Rockefeller-Snowe Cybersecurity Act along with its companion legislation, the National Cybersecurity Advisor Act* – provides a robust, collaborative response to the growing cyber threat.

**The National Cybersecurity Advisor Act, S.778, which is pending before the Senate Committee on Homeland Security and Government Affairs, would create a Senate-confirmed National Cybersecurity Advisor within the Executive Office of the President. The Advisor would report directly to the President and would be the lead U.S. government official on all cybersecurity matters, responsible for coordinating the missions of the intelligence and defense agencies with those of civilian agencies, and for coordinating public-private teamwork on cybersecurity. The Advisor is the executive agent for most of the initiatives contemplated in S.773, the Cybersecurity Act of 2009. Together, S.773 and S.778 constitute the comprehensive Rockefeller-Snowe cybersecurity legislation.*

WHAT THE ROCKEFELLER-SNOWE CYBERSECURITY ACT WILL DO:

- Significantly raise the priority of cybersecurity throughout the federal government and streamline cybersecurity-related government functions, authorities and laws.

- Protect civil liberties, intellectual property and business proprietary information.

- Promote cybersecurity public awareness, education, and research and development.

- Foster market-driven cybersecurity innovation and creativity to develop long-term technology solutions and train the next generation of cybersecurity professionals.

The Rockefeller-Snowe Cybersecurity Act's central guiding principle is to modernize the government-private sector relationship on cybersecurity. Nearly 90 percent of our nation's networks are owned and operated by the private sector. Securing cyberspace must be a collaborative effort between our government and private sector.

Reactive, ad hoc responses to the cyber threat leave our country, our businesses and our civil liberties at risk. The Rockefeller-Snowe Cybersecurity Act provides a framework for proactive engagement, collaboration and teamwork between the government and the private sector on cybersecurity.

OVERVIEW OF THE ROCKEFELLER-SNOWE SUBSTITUTE AMENDMENT:
The vast majority of the bill's provisions have strong support from a wide variety of cybersecurity experts and have remained largely unchanged from earlier drafts. These provisions increase and improve cybersecurity awareness and education, research and development, and professional career development.

The substantial revisions in the substitute amendment are contained in five provisions that have benefited from extensive consultation, suggestions, and advice from cybersecurity experts in government, the private sector, and the civil liberties community through four drafts of the bill. These provisions promote proactive collaboration and engagement between the private sector and the government on cybersecurity (sections 101, 201, 204, 208, and 403), and two new provisions that are critical to this government-private sector teamwork (Sections 4 and 209).

NEW PROVISIONS:

Collaborative Designation of Critical Infrastructure Information Systems (Section 4)
Unlike physical critical infrastructure such as chemical plants and airports, it is not obvious where the "critical" aspects of IT systems begin and end. **Section 4** creates a process in which the President and the critical infrastructure sectors collaborate, through the existing sector coordinating councils, to designate the specific IT systems whose disruption or incapacitation would threaten strategic national interests. The process is an administrative rulemaking governed by the Administrative Procedure Act and provides for notice and comment regarding criteria for designation; adjudicative review, modification, and appeal; and protection of confidential, proprietary, and classified information.

Private Sector Access to Classified Information (Section 209)
Private sector owners and operators of critical infrastructure are responsible for securing a large percentage of the IT systems that our country relies on for basic day-to-day activities, but they often do not have sufficient access to classified information regarding threats to these IT systems. Therefore, Section 5 requires the President to provide security clearances to key private sector officials and to facilitate the sharing of classified threat information with these officials.

REVISIONS IN THE PROPOSED SUBSTITUTE AMENDMENT:

Market-Driven Innovation and Excellence (Sections 101, 204, and 208)

Sections 101 and 204 bolster market incentives for innovation and excellence in cybersecurity professional training and cybersecurity products and services by encouraging, coordinating and building on private sector initiatives. They create a dynamic, ever-improving cycle of market-driven innovation – not a static checklist administered by a slow-moving bureaucracy. **Section 208** puts the purchasing power of the Federal government behind these innovations by requiring them to be part of every Federal contract for IT products and services.

These sections require the President to collaborate with private sector critical infrastructure companies to identify the world's best private sector training programs and industry best practices for IT products and services. Then they require those same companies to report the results of independent audits of their compliance with these standards – their own standards.

Companies that comply with these standards will receive public recognition. This positive recognition is similar conceptually to initiatives like the public-private EnergyStar program that recognizes energy efficient electrical appliances and other products.

Companies that fail to comply with these standards through two consecutive audits will be required to work collaboratively with the government and private sector colleagues within their critical infrastructure sector (via existing sector coordinating councils) to develop and implement a collaborative remediation plan. In practice, this would effectively be a government-coordinated private sector intervention to prevent a failing company from damaging the entire industry sector – and the country's security along with it.

Collaborative Emergency Preparedness and Response (Sections 201 and 403)

Sections 201 and 403 require a collaborative effort to promote effective, well-coordinated government-private sector teamwork – and protect civil liberties, proprietary rights, and confidential and classified information – before, during and after a cybersecurity emergency.

Section 201 requires the President to collaborate with owners and operators of critical infrastructure IT systems, through the existing sector coordinating councils, to develop and rehearse detailed cybersecurity emergency response and restoration plans. The explicit purpose of this section is to clarify roles, responsibilities, and authorities of government and private sector actors in the event of a cybersecurity emergency that threatens strategic national interests. (That is, a cyber event that is equivalent to an act of war, a terrorist attack, or a major natural disaster.) The President's declaration of a cybersecurity emergency would trigger the implementation of the collaborative emergency response and restoration plans.

Section 201 states explicitly that nothing in the section authorizes new or expanded Presidential authorities – it simply seeks to avoid the type of deadly bureaucratic confusion that left New Orleans to drown in the aftermath of Hurricane Katrina. To establish greater accountability for the President's actions during a declared emergency, the section also requires the President to report to Congress in writing within 48 hours of the declaration regarding the circumstances necessitating the declaration, and the estimated scope and duration of the emergency.

Section 403 complements this emergency response provision by creating a public-private information sharing clearinghouse in which government and private officials would share classified and/or confidential cybersecurity threat and vulnerability information. The concept is to create an "op-center" type of facility to deal with incidents like the recent high-profile cyber intrusions as they happen – or, preferably, to spot problems early and prevent them from developing into major cybersecurity incidents in the first place.

PROVISIONS LARGELY UNCHANGED FROM EARLIER DRAFTS:

Federal Cyber Scholarship-For-Service Program (Section 102)
This section would create in statute the Scholarship-For-Service program at the National Science Foundation, which is focused on recruiting students into a cybersecurity curriculum program. Upon graduation, these students would enter public service, joining an agency or department and leveraging the skills they've learned. This section would increase the number of students from 300 to 1000 annually.

Cybersecurity Competition and Challenge (Section 103)
This section would authorize the NIST Director to establish cybersecurity competitions and challenges to attract, identify, and recruit talented individuals to the cybersecurity field.

Cybersecurity Workforce Plan (Section 104)
This section would require the head of each federal agency to annually complete a cybersecurity workforce plan that details recruitment, hiring, and training of cybersecurity employees and contractors. Each agency would make their hiring projections publicly available on their website.

Measures of Cybersecurity Hiring Effectiveness (Section 105)
This section would require each federal agency to measure cybersecurity hiring effectiveness with respect to recruiting and hiring, from the perspective of hiring managers, applicants, and new hires. This information would be reported annually to Congress and the public.

Biennial Cyber Review (Section 202)

This section directs the President to conduct a biennial review of the U.S. cyber program. The review will examine cyber strategy, budget, plans, and policies and is modeled after the Department of Defense's Quadrennial Defense Review.

Cybersecurity Dashboard Pilot Project (Section 203)
This section would require the Secretary of Commerce to plan and implement a system to provide the cybersecurity status of all federal information systems and networks within the Department of Commerce. The lack of real-time visibility into the state of an information system or network is a key limitation of improving cybersecurity. This visual tool will aid major decision makers, such as the Secretary, in identifying needs and marshaling resources.

Legal Framework Review and Report (Section 205)
This section would require the GAO to complete a comprehensive review of the federal statutory and legal framework applicable to cybersecurity, and to make recommendations regarding changes needed to advance cybersecurity and protect civil liberties.

Joint Intelligence, Threat and Vulnerability Assessment (Section 206)
This section requires the Director of National Intelligence, the Attorney General, and the Secretaries of Commerce, Homeland Security, Defense, and State to provide assessments on threats to and vulnerabilities of Federal information systems and critical infrastructure information systems.

International Norms and Cybersecurity Deterrence Measures (Section 207)
This section would require the President to promote the development of international norms, standards and techniques for improving cybersecurity.

Authentication and Civil Liberties Report (Section 210)
This section would require the President to review the feasibility of an identity management and authentication program. The anonymous nature of the Internet is one of its major vulnerabilities. Experts believe that incorporating identity management and authentication will improve overall security, but this must be done with strict attention to civil liberties.

Promoting Cybersecurity Awareness and Education (Section 301)
This section would authorize a cybersecurity awareness campaign to educate the general public about cybersecurity risks and countermeasures they can implement to better protect themselves. It would also direct the Secretary of Education to consult with State authorities, private sector companies and non-governmental organizations to develop guidelines for K-12 curriculum regarding cyber safety, security, and ethics.

Federal Cybersecurity Research and Development (Section 302)

This section would increase Federal support for cybersecurity research and development at the National Science Foundation. This section would also highlight important areas of research that need to be conducted, including secure coding and design.

Cybersecurity Advisory Panel (Section 401)

This section would require the President to establish or designate a Cybersecurity Advisory Panel consisting of outside experts in cybersecurity from industry, academia, and non-profit advocacy organizations who will advise the President on cybersecurity related matters. This Panel would provide industry, academia, and civil liberty groups an opportunity to review the Federal cybersecurity effort and provide advice on its direction and progress. The Panel would provide a report to the President every two years with recommendations on how the Federal cybersecurity effort should be improved.

State and Regional Cybersecurity Enhancement Program (Section 402)

This provision would create state and regional cybersecurity centers to assist small- and medium-sized companies in addressing cybersecurity issues. This program is modeled off of the Manufacturing Extension Partnership (MEP). Large companies have the resources and expertise to address cybersecurity issues, but small- and medium-sized companies often do not. This program would help address that gap.

Cybersecurity Risk Management Report (Section 404)

This section would require the President to report on how to create a market for cybersecurity risk management including civil liability and insurance.