June 20, 2012

The Honorable Richard Shelby
U.S. Senator from Alabama
304 Russell Building
Washington, DC 20510

The Honorable Michael Bennet
U.S. Senator from Colorado
458 Russell Building
Washington, DC 20510

The Honorable Jeff Sessions
U.S. Senator from Alabama
326 Russell Building
Washington, DC 20510

The Honorable Mark Udall
U.S. Senator from Colorado
328 Russell Building
Washington, DC 20510

Cyber Huntsville and the Center for Information Age Transformation (CIAT), a chapter of the Rocky Mountain Technology Alliance, are pleased to jointly deliver the enclosed Open Letter to Congress about Cybersecurity Legislation: A Call for a New Approach. We believe the points articulated in the Open Letter merit Congress' attention during this legislative session.

The Open Letter originated through a grassroots collaboration using social networking on the Internet, conducted by cybersecurity specialists in an open exchange of ideas. Many of the participants are pursuing novel information sharing initiatives in their communities. Their input brings fresh perspective to a cybersecurity debate that must be reframed. Cybersecurity is not simply a national security imperative; we must also refocus efforts toward an inward-facing, homeland security integration strategy that delivers national security capability to local and regional levels. From a centralized model that draws upon the national security structure of the Federal Government, we must move toward a decentralized model that provisions capability and integrates with local and regional structures – some of which do not yet exist. The Open Letter articulates the case and the mechanisms needed to implement this new strategy for cybersecurity.

We are especially pleased to bring this Open Letter to you because Cyber Huntsville in partnership with the CIAT are leading efforts to create the community and regional mechanisms necessary to improve cybersecurity resilience at local and regional levels. Cyber Huntsville and the CIAT's Western Cyber Exchange are leading efforts in Alabama and Colorado, respectively, to establish centers of cybersecurity excellence that will improve cybersecurity readiness and capability. We are also collaborating with other community and regional initiatives in grassroots efforts to address the gap in local and regional cybersecurity capability. Accordingly, we support this Open Letter and endorse the call for a new strategy, one that will integrate local and regional programs within a new national strategy.

We forward the Open Letter to you, and ask that the points and recommendations contained therein be considered by Congress during debates about cybersecurity.

Rodney L. Robertson, P.hD.
President
Cyber Huntsville

Michael Semmens
Chairman
Rocky Mountain Technology Alliance

An Open Letter to Congress About Cybersecurity Legislation A Call for a New Approach

THE SIGNATORIES BELOW CALL FOR A NEW STRATEGY FOR CYBERSECURITY THAT DEFINES THE CORE PROBLEM AND ESTABLISHES RESILIENCE MECHANISMS THAT PROVIDE CAPABILITY ACROSS AMERICA

JUNE 2012

Several cybersecurity bills have been debated in Congress over the past sessions. Undoubtedly this debate will continue. We, the signatories to this Open Letter, support the general need for cybersecurity legislation. We join this letter in both individual capacities and as organizations all sharing the belief that a new approach to cybersecurity is necessary. Our backgrounds include network engineering, Internet governance, cybersecurity, military cyberspace operations, government, industry, academia, cyberlaw, and information technology. From the respective experience of the collective joining this Open Letter, we believe a new approach is required. We call upon Congress to fashion legislation that addresses these core needs.

THE INTERNET ITSELF – THE CORE CHALLENGE

A period of transformational change brought about by the Internet is upon us. The Internet, a technology designed to provide connectivity for societal gain, now facilitates connections that bear harm. The cybersecurity threat has been described as one of our Nation's most grave national security risks, and a risk to our global economic competitiveness. Moreover, because this connective fiber which bears such grave risk is integral to the fabric of every American's life, the threat is one that ordinary Americans face daily. The threat is described in national security terms, yet individuals, businesses and communities face that same threat. A national security threat to individuals, businesses, and communities from the Internet is a new paradigm. An integrated strategy to defend individuals, communities, businesses, and critical infrastructure from these national security threats does not exist. National plans and programs exist, but capability at the point of impact from a cyberattack does not exist across America.

The fundamental deficiency of existing national strategy and implementing plans and programs is that strategy has not kept abreast with the rapidly changing Internet environment. In 2003, *The National Strategy to Secure Cyberspace* was released. "Securing Cyberspace" is no longer a viable objective. Absent major architectural changes and a host of related efforts, the Internet itself cannot be secured. Achieving national security and economic competitiveness challenges associated with the modern Internet era will necessitate revisiting and redefining the core challenge.

Much of the debate surrounding cybersecurity legislation focuses on whether to impose all the costs of national security-level cybersecurity upon business through regulation, or whether national security-level cybersecurity is fundamentally a government responsibility which should be funded and implemented by the Federal Government. Neither of these approaches is tenable. Budget, respect for private property, privacy, and the cost of over-regulation are all reasons that render the respective approaches untenable. Instead, we propose a new model that threads the needle between regulation and incentives for the private sector.

We believe that the core challenge of cybersecurity, from a national strategy perspective, is the decentralized and distributed nature of the Internet. As a Nation, traditional national security thinking and methodology starts from a centralized government model. That approach is reminiscent of a static, Maginot Line strategy while today is an age of agile, asymmetric attackers. The Internet era requires national security strategies that provision and mobilize from the ground up at local and regional levels and that create distributed capability centers across the Nation's footprint. This is fundamentally a decentralized approach that would be responsive to a decentralized attack, and which provisions resources at local levels where the greatest risk to critical infrastructure exists.

Moreover, the provisioning of capability centers across the Nation's footprint enables Federal funding to trigger an ultimately sustainable model whereby businesses and communities contribute as well as receive within a cooperative model. This cooperative model pools capability and delivers security services, thereby becoming a cybersecurity catalyst within the community. This sort of community and regional capability center, engaged in information sharing and other cybersecurity functions, with participation from industry, will ultimately trigger market forces by bringing together supply and demand, and improving awareness, changing behavior, and improving resiliency.

We call upon Congress to establish authorities, institutions, and mechanisms that enable and facilitate growth of cybersecurity resilience and capability at local and regional levels across the United States. We offer the following recommendations regarding the features and underlying precursors that would yield such a modern resilience environment across the Nation.

FEATURES AND ATTRIBUTES OF A CYBERSECURITY STRATEGY OF INFORMATION SHARING

The threat from cyberspace ignores boundaries, sectors, and other vertical structures. This asymmetric threat cuts across the vertical structures our society has created: government and industry, state and federal, intelligence and law enforcement, and sector-specific compliance regimes. These are all vertical structures. Attacks are enabled by the lack of coordination between these vertical structures in society. To combat this gap, mechanisms must be established to facilitate horizontal information sharing about Internet threats.

Horizontal information sharing mechanisms must also integrate all of society. The information sharing frameworks created since 9/11 do little to integrate local to state to federal, including both government and industry. A small business in a small town supplying technology to the federal government needs the same exquisite security that big business and national security organizations possess. Information sharing mechanisms must be established that provision exquisite cybersecurity down to community levels.

INFORMATION SHARING MECHANISMS AND INSTITUTIONS

While removing obstacles to information sharing are helpful, authorizing and promoting information sharing in the abstract does not go far enough. The horizontal structures mentioned here do not presently exist. Mechanisms for information sharing, not merely granting authority, are necessary for an information sharing strategy to become effective in affording broad situational awareness and preparedness across the Nation. At the same time, robust and effective privacy safeguards must go hand-in-hand with improved methods of information-sharing.

ACADEMIC RESEARCH

National security and economic competitiveness challenges from the untrustworthiness of the Internet are key dimensions of the challenge that has been termed "cybersecurity". These dimensions of the cybersecurity challenge involve broad societal questions, not merely technical controls or scientific advances. The change in national strategy called for here implicates major societal equities, such as privacy, government – to – industry relationships, evident legal changes, and other major changes in the structure of society. Structural changes are difficult. Academia must play a leading role in studying and shaping a new discipline, so that society better understands the issues associated with refashioning societal structures in response to Internet-driven changes to produce a more resilient environment.

Academic research, study, and analysis should include these characteristics and objectives:

- Applying interdisciplinary approaches to understanding fundamental changes that the modern Internet poses to security strategy, security institutions and frameworks, government and commercial roles in security, and society at large.
- Establishing academic and public-private centers of excellence that study, model, and organize structures focused on cybersecurity and cyber-physical systems as distinct disciplines of academic and vocational pursuit, and which facilitate better understanding of these as distinct disciplines for the betterment of society.
- Providing definition to cybersecurity and cyber-physical system terms, taxonomy and objectives, leading to a new disciplinary construct, and supporting the strategy development called for in this Open Letter.

ACADEMIC PROGRAMS AND EDUCATION

The academic research, taxonomy development, and resulting disciplinary construct must also lead to improved education programs. The Internet emerged as a major economic force around the turn of the century – long after most educators entered the workforce. Teachers have to teach about a revolutionary force that they did not grow up with, and which society continues to grapple with – as evidenced by the calls for legislation and the positions in this Open Letter. Accordingly, education needs new tools, content, and methodologies to empower educators. Moreover, the Internet itself should be leveraged as a platform to improve the way we teach our kids. Mechanisms must be established to

improve Internet-related education in a systemic way. Academic research should be integrated with academic program development. This requires new funding. Achieving efficiencies and integration can be accomplished from a new strategic approach, which is the core need called for in this Open Letter.

NEW STRATEGY – ROOT CAUSE ANALYSIS

The 9/11 Commission, responding to a national imperative to "get to the bottom" of the 9/11 tragedy, pursued its charter without preconceptions about the causes. Its findings, based on extensive study of the facts and government institutional dynamics, were profound. Congress should revisit many of those findings in the current debate over cybersecurity legislation because there are many parallels between the asymmetric threat of terrorism and the asymmetric threat from cyberspace. A sampling of relevant Commission assessments includes:

- We propose that information be shared horizontally, across new networks that transcend individual agencies.
- The current system is structured on an old mainframe, or hub-and-spoke, concept.
- A decentralized network model, the concept behind much of the information revolution, shares data horizontally...
- No one agency can do it alone.
- White House leadership is also needed because the policy and legal issues are harder than the technical ones.
- "This is government acting in new ways, to face new threats" (citing the Markle report)
- The importance of integrated, all-source analysis cannot be overstated. Without it, it is not possible to "connect the dots". No one component holds all the relevant information.

We believe that the struggle to find a tenable path for improved cybersecurity that integrates the public and private sectors stems from strategy failing to identify the root problem. Admittedly, the problem may have changed as the Internet has changed. Certainly our understanding of the problem has improved with time. Despite the promulgation of several strategies, Presidential findings and executive orders, and national implementation plans, we do not believe that any commission has been assembled and chartered with the sort of mission given to the 9/11 Commission. As a result, the Comprehensive National Cybersecurity Initiative and the White House 60-day Cyberspace Policy Review did not **identify the core problem** around which a counter-strategy should be devised. Both were worthwhile and impressive efforts, resulting in meritorious implementation programs. However, they did not produce the sort of structural changes that the 9/11 Commission triggered because **no core problem statement was fashioned, and thus no Grand Strategy has ensued.**

We believe that a major component of the core problem, perhaps the core itself, is the decentralized, horizontal, and asymmetric nature of the Internet threat, whereas government structures tend to be centralized and vertical. However, only through a root cause analysis, involving an inter-disciplinary

team of experts, assembled without special interests, can a core problem be specified. Unlike other national strategy assessments, this team must include experts both inside and outside of government. We therefore propose a legislative initiative as follows:

- ➔ Commission a Blue-Ribbon Commission, reporting to the President, tasked with conducting a 360-degree, fresh and unconstrained assessment of modern risks from cyberspace, and recommending the contours of a new national cybersecurity strategy. The commission should include distinguished experts from government, foundations and nonprofit organizations, prominent thought leaders, academia, industry, and local and regional cybersecurity leaders. The commission should include inter-disciplinary expertise, and should pursue a problem-solving methodology that incorporates root cause analysis. While this assessment may review existing strategy, the objective is not to assess that strategy, but rather to identify the problem or problems presented by the modern Internet and to recommend solutions that strategically target modern cybersecurity challenges. We offer the views and analysis contained in this Open Letter to Congress and to the proposed Blue-Ribbon Commission.

We, the undersigned, call upon Congress to pass legislation that addresses the objectives and includes the features described in this Open Letter.

Respectfully Submitted,

Douglas M. DePeppe
Co-Founder, Center for Information Age Transformation
Partner, i2 Information Security
Colorado Springs, Colorado

Michael G. Semmens
President, Rocky Mountain Technology Alliance
Co-Founder, Imprimis, Inc.
Colorado Springs, Colorado

Kurt A. Johnson
Director, Center for Homeland Security
National Institute of Science, Space & Security Centers
University of Colorado Colorado Springs

Jennifer M. Taylor
Vice President - Local Industry
Greater Colorado Springs Chamber and EDC
Colorado Springs, Colorado

Todd Morris
Vice President Commercial Division
CB Insurance, LLC
An Affiliate of Central Bancorp
Colorado Springs, Colorado

Jim Furnier
Owner – JRF Systems
San Angelo, Texas

Richard C. LaMagna
Principal, Trust Anchor LLC
Gaithersburg, Maryland

Derek Padden
President
Blue Glacier Management Group
Fairfax, Virginia

John Mencer
Denver, Colorado

Bob Lally
Dean of Homeland Security
Colorado Technical University
Colorado Springs, Colorado

Michael K. Lavine, Ph.D.
Managing Director, Cyber Security Associates
Owings Mills, Maryland

Jared Owensby
Cybersecurity Consultant
Colorado Springs, Colorado

Edward Rios
President/CEO, CyberSpace Operations
Consulting, LLC
Colorado Springs, Colorado

Matthew Pirko
President, JesRico Consultants
Consultant to Cyber City USA
San Antonio, Texas

Jacques Francoeur
Executive Director, Union of Concerned
Cybersecurity Leaders
Los Gatos, California

Jeff Beauprez
President and CEO
Colorado Networks
Colorado Springs, Colorado

Dev Mishra, M.D.
Burlingame, California

Jeanie M. Larson
Director Risk Management - Government
agency
Washington, DC

Peter Gregory
Chairman and CTO, Green Energy Corp
Denver, Colorado

Robert Clark
Former Legal Advisor
US-CERT, DHS
Washington, DC

Rick Schaal
Vice President – Engineering
Viridity Energy Inc.
Philadelphia, Pennsylvania

Penny Whitney
Pikes Peak Cleantech
Colorado Springs, Colorado

Bob Johnson
Vice President for Acquisition Programs
System Studies and Simulation Corporation
Huntsville, AL

Randy Vickers
Former US-CERT Director
Cybersecurity Consultant
Stafford, Virginia

Rodney L. Robertson, Ph.D.
Executive Director, Auburn University Huntsville
Research Center
President, Cyber Huntsville
Huntsville, Alabama