AN OPEN LETTER CALLING FOR CYBER RESILIENCE AND NATIONAL FOCUS ON LOCALITY-BASED CYBER CAPACITY

The purpose of this letter, offered through the collaborative efforts of a number of community-based cybersecurity organizations in ten states, is to inform the Federal Government of the strong capability emerging from regional and local cybersecurity public-private partnerships, and to seek support that these organizations be included as part of the national cybersecurity plan.

Across the country, a number of innovative community initiatives, extending across regions, have been established to address cyberspace threats to critical infrastructure. The initiatives integrate government and private efforts through public-private partnerships, promote research, and support the education and training of both cyber professionals and the user population at large. These organizations are developing the ability to share information by establishing a ‘trusted entity’ to improve intelligence and preparedness. They are bringing resources that are essential to deal with the threats brought about by the Cyber Age. They are building new aspects of the economy built on the IT industry, which is a critical market in the United States. If properly supported and integrated with other national efforts, regional and local cyber initiatives will form the foundation for a new cyber resilience and preparedness framework for the nation.

Facing risk of cyberattack, the resilience of critical infrastructure is a national imperative, as announced by the White House in February this year. The community-based cyber initiatives align perfectly with the emerging national strategy to build cyber resilience. Preparedness, response, and recovery capability is needed at the point of impact of a cyberattack. The community cyber initiatives should therefore be central to the capacity building that is needed to improve preparedness and emergency response within the locality of the critical infrastructure that is being targeted. Failure to integrate these regional and local cyber initiatives in the emerging cyber framework would leave the nation vulnerable.

There are several existing regional and local public-private partnership cyber initiatives in this country, while others are emerging. The following groups have joined in this Open Letter to call for greater national engagement, collaboration, and promotion of this now-established movement toward cyber resilience building at community and regional levels:

- Western Cyber Exchange – WCX (Colorado, New Mexico, and Wyoming)
- Cyber City USA in San Antonio, Texas
- Cyber Huntsville in Huntsville, Alabama and supporting organizations
- Public Regional Security Information Management (PRISEM) project in the Puget Sound region of Washington State
- Cyber Incident Response Coalition and Analysis Sharing (CIRCAS) of the Pacific Northwest
- State of Oklahoma Cyber Security Operations Center (SOC2) and supporting organizations
- Stephenson Disaster Management Institute at LSU and supporting organizations
- Alabama Cyber Research Consortium and supporting organizations
- Advanced Cyber Security Center – ACSC (Boston and Greater New England)
- Pacific NorthWest Economic Region (PNWER)

If properly utilized, such initiatives can serve an invaluable function in our national effort to bolster U.S. cyber defenses. These organizations facilitate local and regional information-sharing, break down barriers between the public and private sector, and ensure the establishment of strong regional partnerships. These partnerships allow businesses, law enforcement, state and local government, and other entities to
more efficiently exchange threat-information and thwart digital intrusions and attacks before they compromise entire networks and cause significant economic damage. They are moving beyond simple “information sharing” towards collective, real-time situational awareness and collective response to shared threats. These regional and local efforts are an important first line of defense for U.S. critical infrastructure in the escalating cyber battles of the 21st century; and, as more of these entities stand up, they can help take pressure off DHS, NSA, FBI, DOD and other federal authorities who currently are perceived as the country’s primary defenders of cyberspace. However, for this to work, the Administration has to proactively reach out to these organizations now, and engage with them as key stakeholders as DHS, NIST, and other departments and agencies move forward on implementation of President Obama’s cybersecurity executive directives on cybersecurity and critical infrastructure protection.

Moreover, these initiatives represent fledgling cyber market ecosystems that, if properly supported, will generate economic growth, jobs, research, education, and improve the overall cyber hygiene across communities. National cybersecurity programs can, and should, be channeled through them to reach targeted audiences. Academia, already involved in the initiatives, can conduct research into a nascent market segment. Collaboration, information sharing, and public-private partnerships will foster centers of excellence within participating communities. Put simply, the economic development advantages of these models complement the security dimensions of the overall value proposition.

US Government departments and agencies were specifically tasked by the President’s cybersecurity and critical infrastructure directives with establishing new mechanisms and frameworks for cybersecurity. Accordingly, the undersigned hereby call in this Open Letter for government collaboration with the regional and local initiatives and for their express incorporation in the National Infrastructure Protection Plan.

The participating organizations backing this Open Letter welcome the support of Congress in furthering the strategic objectives contained herein. Contact with any of the named organizations may be made through the respective Congressional delegation or information contained on each initiative’s website. The participating organizations additionally welcome coordination across this regionally diverse collective that may be facilitated by The Regional Consortium Coordinating Council (RC3), a DHS-affiliated coordinating council, and particularly seek the submission of this Open Letter by RC3 for consideration by the Critical Infrastructure Protection Advisory Council. Collective coordination among the initiatives may also be accomplished through the RC3, with contact information available at http://triplec.wordpress.com.

**Regional and Community Initiatives Supporting this Open Letter**

- **CIRCAS**
  - Contact: David Matthews
  - dmatthews@expedia.com

- **SOC²**
  - Contact: Mark Hogan
  - MHOGAN@cityoftulsa.org

- **Pittsburg**
  - Contact: Rodney Robertson
  - RLR0012@auburn.edu

- **PACIFIC NORTHWEST ECONOMIC REGION**
  - Contact: Brandon Hardenbrook
  - Brandon@pnwer.org

- **SDMI**
  - Contact: Joseph Booth
  - Jbooth7@lsu.edu

- **WESTERN CYBER EXCHANGE**
  - Contact: Doug DePeppe
  - doug.depeppe@cyberjurist.net

- **cyber city usa**
  - Contact: Chris Cook
  - chris@bexarmetro.com

- **PRISM**
  - Contact: Michael Hamilton
  - Michael.Hamilton@seattle.gov

- **ACSC**
  - Contact: Charles Benway
  - cbenway@ACSCenter.org

- **SDMI**
  - Contact: Ronald Burgess
  - rlb0029@auburn.edu

- **Advanced Cyber Security Center**
  - Contact: Michael Hamilton
  - Michael.Hamilton@seattle.gov