NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE

Ms. Maggie Wilderotter
Frontier Communications, Inc.
3 High Ridge Park
Stamford, CT 06903

November 5, 2012

The Honorable Barack H. Obama
The White House
Washington, D.C. 20500

Dear Mr. President:

The National Security Telecommunications Advisory Committee's (NSTAC) 2011 *Report to the President on Communications Resiliency* examined the Nation's resiliency in ensuring essential levels of operability for an array of communications services, ranging from traditional analog voice communications to digitally integrated voice, data, and video applications, including Internet functions. Our report provided recommendations on options for investments or actions the Government could take to enhance the survivability or availability of communications for emergency response personnel, critical infrastructure and key resource (CIKR) owners and operators, and State and local authorities during a time of natural disaster, man-made attack, or crisis. One of the recommendations asked the President to:

[Accelerate] efforts to fulfill the Department of Homeland Security's (DHS) National Cybersecurity and Communications Integration Center (NCCIC) mission and, to ensure that this significant mission is fully operational by the 2015 timeframe, direct DHS to accomplish the following as soon as possible:

- *Leverage the success of the existing NCCIC incident response mechanism by ensuring sufficient funding levels are dedicated to the mission; and*
- *Direct the rapid expansion of personnel resources, including training, to guarantee that the cyber and communications incident response mechanisms are absolutely viable and fully mission-capable by 2015.*

In May 2012, Mr. Howard A. Schmidt, then Cybersecurity Coordinator and Special Assistant to the President, asked the NSTAC to examine DHS' progress to fully operationalize the NCCIC. Specifically, Mr. Schmidt asked the NSTAC to review the NCCIC's progress towards:

- The expansion of partnerships with public and private sector operation centers;
- The maintenance of a national common operating picture (COP);
- The production and dissemination of daily cyber reporting to key public and private sector stakeholders;
- The analytic products used for near-term and long-term threats against critical infrastructure and key resources; and

- Enhanced operational support for residential partners on the floor.

To derive its response, the NSTAC leveraged its work from the 2009 *NSTAC Cybersecurity Collaboration Report*, which outlined steps for the Government, in collaboration with industry, to create a joint, integrated, public-private 24/7, cyber incident detection, prevention, mitigation, and response operational capability. The committee also met with several DHS officials from the Office of Cybersecurity and Communications (CS&C), including the NCCIC, to learn about their progress and challenges first hand.

While the committee recognizes that the Government has made progress against its NCCIC mission, there remains a significant amount of work to be done to ensure the NCCIC is operating at the capacity envisioned in the 2009 NSTAC report. Most importantly, the committee believes that by better leveraging industry expertise to supplement the Government's intelligence and law enforcement capabilities our Nation's cyber defenses will be bolstered and we can reduce the risks produced by a variety of cybersecurity threats.

Legal barriers to bi-directional information sharing and increasing private sector integration into the NCCIC's operations are two barriers the NSTAC recommends that the Administration continue to examine. Once these and other barriers are addressed, the NSTAC believes the NCCIC's overall operating capability, including its ability to gather and disseminate analytical products, will be enhanced. This will create meaningful situational awareness and will maintain a national COP, both during times of steady state operations and during different phases of escalation. (See the attachment for greater detail on each of the items presented by Mr. Schmidt.)

The NSTAC also recognized and examined the President's issuance of Executive Order (E.O.) 13618, *Assignment of National Security and Emergency Preparedness Communications Functions*, and the corresponding realignment of CS&C, which houses the NCCIC. The NSTAC believes that until the full impact of the E.O. and the realignment on the NCCIC's operations is known, the committee cannot truly gauge the NCCIC's overall effectiveness and progress toward its mission. The NSTAC recommends that the NCCIC develop a short- and long-term strategy with benchmarks to fully achieve its mission by 2015, collaborating with industry early and throughout its development.

On behalf of the NSTAC members, I thank you for the opportunity to provide additional insights on this recommendation. I am happy to discuss this matter with you further should you have any additional questions. We are partners in this fight to protect our Nation's cyber infrastructure and our combined efforts to increase information sharing will strengthen our cyber defenses and help us detect, prevent and respond to attacks.

Sincerely,

Maggie Wilderotter
NSTAC Chair

Attachment

Attachment
Additional NSTAC Findings and Observations

The President's National Security Telecommunications Advisory Committee (NSTAC) made the following observations regarding the Government's progress in establishing the National Cybersecurity and Communications Integration Center (NCCIC). The observations have been categorized to address the specific items requested by Mr. Howard A. Schmidt, then Cybersecurity Coordinator and Special Assistant to the President, in May 2012.

- **The expansion of partnerships with public and private sector operation centers:**

  - While recognized as the owners and operators of the cyber infrastructure and an important source for information, the private sector is still not a significant partner in the NCCIC's operations. For example, the NCCIC has not yet sought private sector involvement as it begins to develop operational playbooks that were slated to augment the draft *National Cyber Incident Response Plan*. The NCCIC should leverage the extensive Government-industry partnership framework set forth in the *National Infrastructure Protection Plan* to ensure that private sector critical infrastructure owners and operators can contribute to the process.

  - The Department of Homeland Security (DHS) is currently implementing cooperative research and development agreements (CRADAs) to coordinate and share information directly with industry partners. The NSTAC is concerned that while CRADAs are useful, they are bilateral in nature, and therefore may not be sufficient for sharing information between and across all appropriate private sector entities. At the same time, we are aware of the legal issues associated with sharing sensitive information more broadly with the private sector. In the interests of furthering the broadest dissemination of critical information and situational awareness, it is our belief that DHS should continue to focus on reaching agreements with sector-level operational organizations, such as the information sharing and analysis centers (ISAC) as recommended in the 2009 *NSTAC Cybersecurity Collaboration Report*. Once the ISACs become more broadly involved, the range of expertise and contributions from member companies will be more evident, leading to greater, more effective collaboration.

  - The NCCIC continues to emphasize the value of building trusted relationships between key individuals supporting various cyber elements within Government and industry; however, industry NCCIC participants lack awareness of which NCCIC officials are responsible for collecting sensitive threat information. Additionally, while recognizing the importance of these key relationships to the successful operation of the varying missions and objectives within the NCCIC, they should be supplemented by appropriate technologies and well-established operational protocols. Moving towards process and technologies would better allow the NCCIC to scale, either between times of steady state and during times of increased activity, or to be able to effectively manage, the steady increase of data available for analysis as information sharing processes and methodologies are improved.

- **The maintenance of a national common operating picture (COP):**

  - Regarding a cybersecurity and communications-focused national COP, the NCCIC has

not developed an effective way to monitor the current cybersecurity environment and ensure that relevant information is presented to the appropriate individuals or entities. The NSTAC believes that the NCCIC should begin to collaboratively develop an initial draft national COP for dissemination and revise it according to stakeholder needs and feedback, instead of building it first and then presenting the result.

- **The production and dissemination of daily cyber reporting to key public and private sector stakeholders; and the analytic products used for near-term and long-term threats against critical infrastructure and key resources:**

  - One of the NCCIC's key missions is to gather, analyze, and disseminate threat information to its stakeholders, including other Federal Government agencies. In order to disseminate relevant and actionable attack information as soon as possible, the NSTAC urges the NCCIC to initially focus on the attack's impacts and consequences, rather than focusing solely on the attack's origin. Additionally, the NSTAC recognizes that one of the Government's most valuable contributions in the cybersecurity collaboration process is its intelligence capability and unique data streams, such as National Cybersecurity Protection System data received by United States Computer Emergency Readiness Team (US-CERT). The NCCIC should continue to work with its partners, such as law enforcement and intelligence agencies, to declassify information so that it can be broadly received, correlated, and analyzed in a cross-sector process. Currently, achieving near-real time information sharing is hindered by lack of cleared personnel from the private sector and concerns around privacy of customer data shared with the Government. Industry partners need access to information about tactics, techniques, and procedures (not sources and methods) on cyber events or network anomalies to make informed risk management decisions and effectively mitigate a threat.

  - There continue to be legal impediments that prohibit timely, reliable, and actionable bi-directional information sharing between the Government and private sector critical infrastructure owner/operator community. Current law does not appear to support the collaboration necessary between government and the private sector to share information in an effective manner. The need remains for an environment that more easily integrates open source, private sector, and Government-owned data sets that removes the classification and policy-based impediments for information sharing.

- **Enhanced operational support for partners resident on the floor:**

  - The NSTAC identified several impediments to full sector integration into the NCCIC, including high costs of providing a dedicated analyst on the NCCIC floor. The Government may want to consider whether financial support to the various sector-level organizations might minimize the financial burden and enhance the NCCIC's effectiveness.

- **Additional observations:**

  - The NCCIC does not yet have a strategic plan with benchmarks and metrics for success to help guide its operations. During this review, the NCCIC director indicated that a plan

is being developed but will not be finalized until the realignment of the Office of Cybersecurity and Communications is complete. Until this plan is developed and shared with the NSTAC, the committee cannot comment on the NCCIC's overall status.

- While the NCCIC has begun to physically integrate the National Coordinating Center (NCC), US-CERT, Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), and its liaison partners, the operational integration of NCCIC components is still lacking, partially due to the historically-different focuses and mission objectives of each component (e.g., the NCC typically examines physical events, natural or manmade, affecting the cyber and communications infrastructure, rather than US-CERT or ICS-CERT, which generally has a greater focus on the impacts of events occurring in cyberspace).

- NCCIC liaisons have testified that the NCCIC has made progress decreasing the amount of time required to coordinate details of a cyber attack or investigation across the Government. The NCCIC should continue to examine ways to automate these processes so that they can occur as close to real-time as possible. These processes should also be scalable to provide an aggregated view of threats and events occurring across every sector, which can be used to share insights between sectors and correlate data from different perspectives.