Cross-Sector Catastrophic Incident Planning Council

The Communications Sector is recommending that the Department of Homeland Security (DHS) in partnership with the Department of Treasury (Treasury) and the Department of Energy (DoE), as the sector specific agencies for Communications, IT, Energy and Financial Services, in collaboration with the Communications, IT, Electric Sub-Sector and Financial Services Sector Coordinating Councils, initiate a cross sector initiative focused on the following items:

- Enhance national and economic security by ensuring that operational processes between sectors, and then between Industry and the U.S. government are in place to ensure the resiliency of the nation's critical infrastructure in the communications, IT, financial services and electric sectors in the event of a large scale, catastrophic cyber- or physical incident.

- Develop cross sector crisis response plans and protocols building upon existing physical response protocols, and informed by 1) the cyber escalation process suggested in the National Security Telecommunications Advisory Committee (NSTAC) and Internet and Communications Technology Mobilization (ICT-Mobilization Report), 2) further expanded upon in the Homeland Security Advisory Council (HSAC) report issued in 2016, and 3) other recommendations made by the National Infrastructure Advisory Council (NIAC). As outlined in the HSAC report, this process should be targeted towards planning for significant, national-level events; e.g., large scale cyber attacks, hurricane or New Madrid-type events, and not for routine day-to-day or company/locality-specific incidents.

- Explore the ability to align organizations, systems, processes, and technologies across sectors to enhance information sharing and other tools that may improve situational awareness and response in the event of a crisis.

- Identify policy concerns that may need to be addressed to enhance collaboration or response activities.

In the Communication Sector's view, DHS and its' Federal SSA Partners should convene the suggested sectors to address the issues outlined above in the context of the the National Incident Management System (NIMS) and the National Cyber Incident Response Plan (NCIRP) in order to make progress on past recommendations made by the NSTAC, the NIAC and the HSAC. The purpose of this group is to ensure that a template for a cross-sector, operational playbook is developed between these sectors with the intent to extend this template over time to incorporate all critical sectors. Since this template for cross-sector collaboration will ultimately be used in collaboration with the U.S. Government, it is critical that DHS, DOE and Treasury be engaged in this process, and that DHS convene these meetings under their Critical Infrastructure Protection Advisory Council (CIPAC) Authorities.

Overview and Background

Each critical infrastructure sector has existing organizations and partnerships to improve security and resilience for their own industries.[1] There remains an opportunity, however, to improve strategic collaboration across sectors and to align these efforts with the most senior levels of government.

In March 2015, the NIAC recommended that senior executive decision-makers from the nation's most critical infrastructure sectors should coordinate to identify mutual priorities and to develop joint action plans.[2] Subsequently, an HSAC report from June 2016, brought together leaders from the communications, electricity, and financial services sectors to look at post-cyberattack restoration of critical infrastructure services. This report highlighted not only the obvious interdependencies across these sectors, but suggested opportunities for improved collaboration and incident response across sectors.

This proposal is consistent with these recommendations and builds upon discussions, the Sector Coordinating Councils from communications, electricity and financial services have conducted over the past 18 months. Additionally, industry is participating in a variety of efforts involving all three sectors, including joint exercises that should be informative to this process. While industry is already addressing these topics, DHS can play a vital role by convening a focused effort to bring these activities forward, identify remaining gaps, assess viability of integration with NIMS and NCIRP protocols, and discuss prioritization protocols that may need to be developed in advance of such large-scale events.

Key Points: Why should DHS convene this group?

- **While individual companies and sectors are taking steps to improve security, there is a need for additional cross sector collaboration.** When it comes to common adversaries and threats, the critical infrastructure sectors should work with each other and government partners to determine where efficiencies between sectors can be leveraged (i.e., shared tools, technologies, and information sharing platforms) to better coordinate security, preparedness, response and recovery efforts (i.e., unified incident response plans and exercises). The proposed group can expedite existing efforts without supplanting them. The various existing sector-specific efforts will continue. This initiative can complement those efforts by conducting planning activities to ensure that the necessary resources are assigned, identify gaps and ensure that the necessary process flows are fully developed.

Organizational Structure:

- **Follow an Enduring Security Framework (ESF) like approach**. The ESF has proven to be a successful model for operational collaboration with the communications, IT and Defense Industrial Base (DIB) sectors. The ESF is structured with an Executive Steering Committee that meets annually to set the direction and an operational working level group to develop recommendations and more detailed day-to-day interaction. This same structure could be followed here.

- **Start small.** The HSAC report focused on the communications, electricity, and financial services sectors, not to exclude other critical sectors, but more to serve as a smaller effort that might become a template for the expansion to other sectors. Given the evolving nature of the IP environment, we believe that this effort should also include the IT sector, who also provides an infrastructure role in the

[1] **Presidential Policy Directive:** *Critical Infrastructure Security and Resilience (PPD-21)*
https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

[2] "**Executive Collaboration for the Nation's Strategic Infrastructure:** *Final Report and Recommendations*"
https://www.dhs.gov/sites/default/files/publications/niac-executive-collaboration-final-report-508.pdf

cyber ecosystem. Since DHS is the SSA for both IT and communications, the opportunity to bring this element into the discussions would be useful.

- **Manageable number of representatives for each sector**. In our view, there should be a small number of companies on the Executive Steering Committee, which will set the overall direction, and the group can be expanded at the operational level to include a broader cross section of each sector. The Steering Committee should consist of companies representing each sector with individual companies chosen by the respective Sector Coordinating Councils (SCCs) as representative of the sector. Individual companies should be allowed to determine their representative at the Executive Steering Committee as well as the operational level working groups. The SCCs should also focus on assuring that the operational level working groups have sufficient representation to effectively reflect the dynamics of their Sector.

- **Provide flexibility for each sector to organize itself.** The process outlined above acknowledges that each sector is unique in a number of ways, from their preparedness and security needs, to the make-up of Sector Coordinating Councils (SCCs), to how each interacts with government.

<u>Initial Proposed Path Forward:</u>

- DHS, Treasury and DoE should schedule a kickoff meeting in early 2018. The goal of this kickoff meeting should be to convene the group, gain agreement on the structure, goals and objectives, review existing cross sector activities and determine gaps or where additional resources or support may be needed. As an output of this meeting the operations working group should be formed to review the NIMS and NCIRP protocols, and develop a cross-sector playbook or process flow that could be triggered in the event of major, catastrophic physical or cyber event.

- As the Operations Group work proceeds, a legal and policy working group may be established to address legal or policy issues involved in implementing these processes. Whether this needs to be a separate group or this should be integrated with policy subject matter experts participating with the operations working group should be discussed further in the kickoff meeting.

- The group would be tasked with reporting back to Executive Steering Committee of the CIPAC group within a designated time-frame. Assuming consensus, outputs from this initiative should then be briefed broadly throughout the three Sectors for further concurrence, as well as other relevant Advisory committees such as the NSTAC Principal meeting and the NIAC.

Sincerely,

COMMUNICATIONS SECTOR COORDINATING COUNCIL

Robert Mayer
Chairman
Communications Sector Coordinating Council

Kathryn Condello
Vice Chairman
Communications Sector Coordinating Council