NCI Remarks at ISAC/ISAO Summit

Background

Good Morning. My name is Scott Algeier. I am the Executive Director of the IT-ISAC but am speaking here now as the Vice Chair of the National Council of ISACs, or NCI. Denise Anderson, the NCI Chair, regrets that a long standing travel engagement prevents her from attending today.

I want to thank Mike Echols for the opportunity to offer these remarks on behalf of the National Council of ISACs. Taken together, the collective experience, expertise and success of the members of the Council is unmatched.

The NCI is a voluntary organization of ISACs formed in 2003 in recognition of the need for the ISACs to share information with each other about common threats and issues. The mission of the NCI is to advance the physical and cyber security of the critical infrastructure of North America by establishing and maintaining a framework for valuable interaction among and between the ISACs and with government. The members of the NCI are the 18 individual ISACs that represent their respective sectors or subsectors. The NCI also works closely with the other critical infrastructure sectors that have operational arms including chemical, (reforming its ISAC) automotive (currently forming an ISAC) and critical manufacturing, among others. Our mission is to be inclusive of each sector's and subsector's designated operational arm.

The ISACs collaborate with each other daily through the NCI daily operations centers cyber call, the NCI secure portal and the NCI listserve. The NCI also hosts a weekly operations centers physical call and meets monthly to discuss issues and threats. The organization is a true cross-sector partnership engaged in sharing cyber and physical threats, mitigation strategies and working together and with government partners during incidents requiring cross-sector response as well as addressing issues affecting the critical infrastructure community. In addition to the secure portal, the NCI conducts and participates in cross-sector exercises, works with the National Infrastructure Coordinating Center (NICC) and the National Cybersecurity and Communications Integration Center (NCCIC) during steady-state and incidents, holds emergency calls as needed and develops joint white papers around threats.

ISACs AND GOVERNMENT PARTNERSHIPS

ISACs work closely with various government agencies including their respective Sector Specific Agencies, intelligence agencies, law enforcement and state and local governments. The ISACS also serve as liaisons to the National Infrastructure Integration Center and play a vital role in incident response and collaboration under the Critical Infrastructure Partner Annex to the Incident Management Plan. In addition, ISAC representatives sit on the Cyber Unified Coordination Group (Cyber UCG). The ISACs have long been engaged in the national public-private partnership participating in the development of various versions of the National Infrastructure Protection Plan, the Cyber Incident Response Plan, and CyberStorm and National Level Exercises, among other initiatives.

However, it must be noted that government engagement with and support for the ISACs has been inconsistent at best. There are some instances where government SSAs actively encourage companies in their sectors to join their sector ISAC. Other ISACs receive substantial government funding or provide operating capabilities to their sector ISAC. In contrast, other government agencies, including agencies within the Department of Homeland Security, refuse to even encourage companies in their sector to join their industry ISAC. I know first-hand this is the experience of the IT-ISAC, where our SSA has consistently refused for a number of years to encourage companies to join the IT-ISAC and has ignored specific proposals from us on how we can partner to meet mutually stated goals. The ISACs and nation as whole would be well served by more consistent engagement and support of ISACs from government agencies.

The solution to this is very simple. It should be federal policy to call out, recognize and support the unique role ISACs play in critical infrastructure protection and resilience. Government should support private sector efforts to form ISACs in those very few critical infrastructure sectors where ISACs do not currently exist, and where they do, regularly and consistently encourage owner/operators to join their respective ISACs. This has been very effective in the financial sector where the United States Department of the Treasury, the regulators and state agencies have been strongly encouraging membership in the FS-ISAC as a best practice. Unfortunately, not all SSAs support their sector designated ISACs in this same way.

THE FEBRUARY 2015 EXECUTIVE ORDER AND ISAOs

The members of the National Council of ISACs have decided that the National Council of ISACs will work collaboratively with our partners in implementing the President's Executive Order. While we are committed to doing this, we also have been seeking clarity as to how the EO impacts the ISACs. While the Fact Sheet released with the EO states the goal is to “not limit effective existing relationships that exist between the government and the private sector,” the recent EO and prominent coverage of ISAOs has led to some confusion within industry as to the impacts to ISACs. It is absolutely essential that the successful efforts that the ISACs have established over the years should not be disrupted. It is clear that the ISACs by their success meet the distinct and unique needs of each of their sectors and the owner and operator members of those sectors.

DHS has apparently told some organizations that sector ISACs are exempt or grandfathered from the EO, but we as a Council have not been able to get this confirmation from DHS. This is not a small point, since ISACs are much more than ISAOs. They serve a special role in critical infrastructure protection and resilience and play a unique role in the sector partnership model.

While it is true that cyberattacks are not limited to critical infrastructure sectors, the private sector is already organizing efforts in this area. Members of the National Council of ISACs are engaged in many of the key industry segments currently experiencing significant attacks. Members of the NCI as a whole are generally willing to share their expertise with those seeking to start information sharing forums.

We think it is particularly important to note that the goal the ISACs strive for is not simply to share information, but instead to create enhanced situational awareness. Through our efforts internal to our specific ISACs and working through the NCI and with other partners, our goal is to provide our individual members with situational awareness (in most cases, all Hazards situational awareness) members need to manage risks to their enterprises. Information sharing is a tool that we use to enable this, but the goal is not information sharing in and of itself. This is a point the National Council of ISACs and its members have made repeatedly, but it is worth repeating here.

CREATING STANDARDS FOR ISAOs

The NCI believes that having an established set of capabilities is important and currently has a baseline set of criteria that ISACs must meet in order to be members of the Council. But it is essential that information sharing organizations have the flexibility and ability to meet the unique needs and threats of its sector and members. Although all ISACs have similar missions, no two ISACs are the same.

While once again expressing our intent to engage constructively, it is appropriate to note that ISACs are self-governed, self-organized and self-led. Any attempt to oversee or mandate what these organizations produce and how they collaborate would risk eliminating information sharing and almost two decades of progress. In the face of growing, targeted and sophisticated threats, rendering proven information sharing efforts ineffective would not only be a grave consequence, it would run contrary to the spirit of the drafting of the EO: to promote private sector cybersecurity information sharing.

CONCLUSION

Since 2003 the National Council of ISACs and its members have participated with industry and government partners in the true spirit of partnership. History demonstrates that we develop better and more effective policies and solutions when industry and government work in collaboration, rather than when solutions developed in closed, government only forums, are imposed. The National Council of ISACs remains committed to working in partnership with our federal partners on behalf of our members and the citizens of this country.

Thank you for your consideration, time and attention.