Testimony for the record of

Denise Anderson

On Behalf of the

The Financial Services Information Sharing & Analysis Center and the

National Council of Information Sharing and Analysis Centers

Before the

United States House of Representatives

Cybersecurity, Infrastructure Protection and Security Technologies

Subcommittee

March 4, 2015

FS-ISAC BACKGROUND

Chairman Ratcliffe and members of the Subcommittee, my name is Denise Anderson. I am Vice President, FS-ISAC, Government and Cross Sector Programs at the Financial Services Information Sharing & Analysis Center (FS-ISAC) and Chair of the National Council of ISACs (NCI). I want to thank you for this opportunity to address the Cybersecurity, Infrastructure Protection and Security Technologies Subcommittee about the industry perspective on "Cybersecurity and Information Sharing". I am submitting this testimony for the record as I am on travel and regret my inability to take part in this proceeding.

The FS-ISAC was formed in 1999 in response to the 1998 Presidential Decision Directive 63 (PDD 63), which called for the public and private sectors to work together to address cyber threats to the nation's critical infrastructures. After 9/11, in response to Homeland Security Presidential Directive 7 (its 2013 successor, Presidential Policy Directive 21) and the Homeland Security Act, the FS-ISAC expanded its role to encompass physical threats to the sector.

The FS-ISAC is a 501(c)6 nonprofit organization and is funded entirely by its member firms and sponsors. In 2004, there were only 68 members of the FS-ISAC, mostly larger financial services firms. Since that time the membership has expanded to almost 5,500 organizations including commercial banks and credit unions of all sizes, markets and equities firms, brokerage firms, insurance companies, payments processors, and 24 trade associations representing virtually all of the U.S. financial services sector. The FS-ISAC is a global organization and has members in 38 different countries.

NCI Background

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 membership of the NCI is the 18 individual ISACs that represent their respective sectors or sub-sectors. The NCI also works closely with the other critical infrastructure sectors (CI) that have operational arms including chemical, (reforming its ISAC) automotive (currently forming an ISAC) and critical manufacturing, among others. The NCI has made it a goal to be inclusive of each critical infrastructure sector and sub-sector's operational arm.

The ISACs collaborate with each other daily through the NCI daily operations centers cyber call, the NCI secure portal and the NCI listserver. 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 industry. In addition to the secure portal, the NCI hosts an ISAC threat level dash board, 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. The ISACs have been instrumental in embracing, developing and advancing the automatic exchange of data within their memberships and across the ISACs, as well as with government as possible.

ISACs AND GOVERNMENT PARTNERSHIPS

ISACs, which are not-for-profit organizations, work closely with various government agencies including their respective Sector Specific Agencies (SSAs) where they exist, intelligence agencies, law enforcement and state and local governments. In partnership with the Department of Homeland Security (DHS), several ISACs participate in the National Cybersecurity and Communications Integration Center (NCCIC) watch floor. ISAC representatives, cleared at the Top Secret / Sensitive Compartmented Information (TS/SCI) level, attend the daily briefs and other NCCIC meetings to share information on threats, vulnerabilities, incidents, and potential or known impacts to the critical infrastructure sectors. Having ISACs on the floor has allowed for effective collaboration on threats and incidents and there have been many examples of successful information sharing. The ISACs also serve as liaisons to the National Infrastructure Coordinating Center (NICC) 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). This group was set up under authority of the National Cyber Incident Response Plan (NCIRP) and has been actively engaged in incident response.

Finally, it should be noted that the ISACs collaborate with their sector coordinating councils as applicable and work with other critical infrastructure partners during steady state and incidents.

THE FEBRUARY 2015 EXECUTIVE ORDER AND ISAOs

The Executive Order, Promoting Private Sector Cybersecurity Information Sharing, signed February 15, 2013 by President Obama and recently announced information sharing legislative proposal are commendable in their intent to foster information sharing. Information Sharing and Analysis Organizations (ISAOs) were first defined in the Homeland Security Act of 2002. ISACs were created under Presidential Decision Directive 63 (PDD-63). Effectively ISACs were the original ISAOs, are the subject matter experts in information sharing and a majority of ISACs have been in existence for over a decade or more.

Indeed there is a need for many groups that may not fall in with the critical infrastructure sectors such as legal and media and entertainment organizations, who are increasingly becoming targets for cyber incidents and attacks, to share information. The private sector is already organizing efforts in this area and as an example; the FS-ISAC has been working with the legal industry for almost a year now to form an ISAO. Many of the other ISACs, such as the Multi-State ISAC (MS-ISAC) and Information Technology ISAC (IT-ISAC) have also been engaging industries that do not have established information sharing forums such as the Retail sector, which is actively forming an ISAC.

However 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 the White House has noted that the EO seeks 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.

The solution to easing this confusion is very simple. The White House, SSAs – including DHS – and other relevant agencies need to call out, recognize and support the unique role ISACs play in critical infrastructure protection and resilience. For instance, ISACs have the responsibility to maintain sector wide threat awareness within their respective sectors. It is critical that our federal partners continue to respect and support that role to avoid undermining one of the main duties of ISACs to their members and sectors. It is vital that the process is not diluted and remains streamlined to facilitate effective situational awareness and response activities particularly when an incident occurs.

One of the greatest strengths of ISACs is the productive information sharing that occurs by having robust trusted networks of members. 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. Currently, not all of the SSAs support their sector designated ISACs in the same manner.

Attached is an appendix, which lists out some 20 points as to why ISACs are more than ISAOs.

CREATING STANDARDS FOR ISAOs

The Executive Order also calls for the drafting of a set of voluntary standards. 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 of its sector and members. Although all ISACs have similar missions, no two ISACs are exactly alike.

Any criteria that are developed must be done in concert with the private sector and must be upheld by the private sector in order to be effective. ISACs and ensuing ISAOs are private sector organizations. Any attempt by government to oversee or mandate what these organizations produce and how they collaborate would eliminate 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.

The NCI has a strong history of mentoring and supporting the establishment of several new ISACs such as Aviation, Retail and Automotive and the re-formation of the Oil and Gas ISAC. ISACs fostered by activities developed and sponsored by the NCI are robustly sharing among their peer ISACs and partners, items such as best practice guides and toolkits that ISACs can replicate and provide to their members for free.

These activities reflect a powerful force in organizational information sharing and collaboration that the EO fails to contemplate and appears to attempt to recreate through the development of a standards organization. Any focus on ISAOs and ISAO standards must be implemented carefully as not only to encourage and foster information sharing and analytical maturity among newly established organizations, but also clearly publish, highlight and fully leverage and emulate aspects of the status quo that are working and have been working for quite some time.

EFFECTIVE INFORMATION SHARING

It is important to note that the goal of information sharing is not to share information in and of itself but to create situational awareness in order to inform risk based decisions as well as allow operational components within owner/operation organizations that have direct actionable control over the content they are sharing, to perform an action. The focus needs to be on enhancing the ability of operational groups to work closely with each other.

The ISACs are successful organizations with almost two decades of proven cases studies of information sharing and collaboration. They are the subject matter experts on information sharing. In order for information sharing to be effective it must be:

- Voluntary – not mandated or regulated
- Industry Driven
- Actionable, Timely and Relevant
- Bi-directional and Collaborative

Government can help this effort by:

- Recognizing ISACs and the special operational role that they play in critical infrastructure protection and resilience
- Supporting private sector efforts to form ISACs in the very few critical infrastructure sectors where they do not currently exist
- Encourage owners and operators of critical infrastructure to join their respective sector ISACs
- Facilitate getting all of the ISACs on the NCCIC floor. After four years this still has not been accomplished
- Recognize the NCI as the coordinating body for the ISACs

This concludes my written statement for the record. Thank you again for the opportunity to present this testimony and I look forward to your questions.

APPENDIX: 20 REASONS WHY ISACS ARE MORE THAN ISAOS

- ISACs are all-hazards and address both cyber and physical threats and incidents
- ISACs are the designated operational arms of their sectors
- ISACs play a critical industry and government recognized role in critical infrastructure incident response
- ISACs have reach into their sectors and in many cases are relied upon as the threat and incident communications channel for their respective sectors
- ISACs provide annonymization and aggregation of data for their sectors
- ISACs provide a sector perspective on threats and incidents and provide sector specific analysis
- ISACs set or manage threat levels for their respective sectors
- ISACs perform structured collaboration across the sectors
- ISACs conduct joint analysis to develop joint products on specific threats and incidents
- ISACs serve an operational role in the national partnership framework
- Many ISACs have security operations centers that monitor threats, vulnerabilities and incidents and provide analysis for sector threat potential and impact
- ISACs are not-for-profit organizations that are not in the business to sell information but to facilitate it
- ISACs meet the unique needs of their respective members/sectors
- Most ISACs are global and are not just focused on the United States. Many have global partnerships
- ISACs have a vetting process for members to qualify to join

- ISACs are organized and run by the owners and operators of critical infrastructure
- ISACs have a formal governance structure
- ISACS facilitate bi-directional information sharing on incidents, information and intelligence within and among the sectors.
- ISACs are designated operational entities within sectors to enhance efficiency and coordination of information sharing and incident response.