Written Testimony of Mr. Mark G. Clancy, Chief Executive Officer, Soltra Before the Committee on Homeland Security United States House of Representatives "Oversight of the Cybersecurity Act of 2015" June 15, 2016

Chairman Ratcliffe, Ranking Member Richmond and members of the Committee, thank you for scheduling today's hearing on industry perspectives on the Cybersecurity Act of 2015 (CISA). My name is Mark Clancy, and I am the Chief Executive Officer of Soltra. Soltra's mission is to design and deliver solutions that shorten the time from awareness, to decision to action, in addressing cyber threats.

First, thank you for all of your efforts and dedication to addressing key cybersecurity concerns and for successfully passing cybersecurity information sharing legislation. As our nation continues to confront serious cybersecurity threats to our critical infrastructure, cybersecurity information sharing is one critical way to address these challenges.

CYBERSECURITY INFORMATION SHARING

Cybersecurity information sharing has been a cornerstone of various aspects of my career, beginning in 2004. At that time, I was running Citigroup's Global Security Incident Response Team. Twelve years ago, we worked to combat the menace of phishing attacks targeting our customers. We quickly learned that the criminals were using the same approaches to target customers of other financial institutions; and by bi-directional sharing of the technical observations of those attacks with our competitors, we all were better able to minimize the impacts of these incidents. That first generation model of sharing was born out of personal trust between individual practitioners who met face to face frequently.

By 2008, a new sharing model was needed as the Financial Services Information Sharing and Analysis Center (FS-ISAC) started to grow significantly. This second generation trust model had widened to a larger number of institutions and individuals who still met face to face on occasion, but now had moved to using electronic mail lists as the primary method of exchanging information between face-to-face meetings.

By 2010, when I was the Chief Information Security Officer at The Depository Trust and Clearing Corporation (DTCC), we realized the scale of the community and the tonnage of information being shared grew to the point we could not utilize all the information, and that a third generation approach to sharing was required to use standardization and automation. This led to us exploring standards that described a cyber threat in such a way that a human could understand it, but a machine could process it.

SOLTRA CREATION: DTCC AND THE FS-ISAC COLLABORATION

Soltra is the financial industry's answer to the third generation information sharing model. Soltra is a joint venture created by DTCC and the FS-ISAC that leverages the unique expertise of both entities, bringing together the best and brightest of the industry.

DTCC is a participant-owned and governed cooperative that serves as the critical infrastructure for the U.S. capital markets as well as financial markets globally. At its core, it develops and harnesses technology to provide a variety of risk management and data services to the financial services industry. More than 40 years ago the firm was created largely out of the need to leverage technology and automation in order to ensure securities transactions were more efficiently settled, thereby

reducing risk of loss in the event of a counterparty default. In this respect, DTCC presently is among the most sophisticated financial technology or "FinTech" companies.

Today, DTCC continues to deploy evolving and improving technology in service to its mission as the primary financial market infrastructure for the securities industry. DTCC simplifies the complexities of clearing, settlement, asset servicing, data management and information services across multiple asset classes. In 2014, DTCC's subsidiaries processed securities transactions valued at approximately US$1.6 quadrillion.

The FS-ISAC is a 501(c)6 nonprofit organization and is funded entirely by its nearly 7,000 member firms and sponsors. It was formed in 1999 in response to 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. The FS-ISAC expanded its role to encompass physical threats after the attacks on 9/11, and in response to Homeland Security Presidential Directive (HSPD) 7 (and its 2013 successor, Presidential Policy Directive (PPD) 21) and the Homeland Security Act.

The FS-ISAC has grown rapidly in recent years. In 2004, there were only 68 members which were mostly large financial services firms. Today, FS-ISAC has nearly 7,000 member organizations, including commercial banks and credit unions of all sizes; markets and equities firms; brokerage firms; insurance companies; payments processors; and 40 trade associations representing all of the U.S. financial services sector. Because today's cyber-criminal activities transcend country borders, the FS-ISAC has expanded globally and has active members in over 37 countries.

SOLTRA

Soltra advances cybersecurity capabilities and increases resilience of critical infrastructure organizations by collecting and distilling cybersecurity threat intelligence from a myriad of sources to help safeguard against cyber attacks and deliver automated services at "computer speed," cutting down the hundreds of human hours that are currently needed to distill cyber threat information.

Soltra began as a true cross-industry initiative that included a live prototype involving over 125 security practitioners that included FS-ISAC members, private sector representatives from other critical sectors, and government entities to refine the requirements, architecture and design of Soltra's automation software, which is known as Soltra Edge.™ Soltra Edge provides for a free platform that users can access, and after less than a year and a half, Soltra Edge has been downloaded by over 2,600 organizations in 75 countries spanning 25 industries to consume, utilize, and share cyber threat intelligence using open standards.

The Soltra Edge platform sends, receives, and stores messages of Cyber Threat Intelligence (CTI) in a standardized way. It hides the complexity of the underlying technical specification so that end users can setup and start receiving threat information in under 15 minutes in most cases, changing the paradigm where it could take months or millions of dollars to change internal systems if companies wanted to do it on its own. The information that is received can be used to push instructions to other security tools to perform detection and mitigation of those threats. To support the widest possible adoption, we also made a highly functional version of the platform available at no cost to end user organizations to defend themselves. We also offer a low-cost or no-cost solution to ISAC and ISAO community organizations to act as the community hub for machine to machine threat sharing if they lack an existing operational capability. For organizations with additional needs, we also offer a paid membership which includes system integrations for platforms that have not adopted standards, enterprise grade operational features, and technical support.

SOLTRA CREATES THE FIRST EVER INTEROPERABLE INFORMATION SHARING PLATFORM: PROVIDES CROSS-SECTOR SHARING TO BETTER COMBAT THREATS

Soltra has built a threat sharing ecosystem using three open standards first developed by DHS and MITRE called the Structured Threat Information eXpression (STIX) and the Trusted Automated eXchange of Indicator Information (TAXII), and the Cyber Observable eXpression (CybOX). STIX, TAXII, and CybOX have been transitioned into an international standards body, OASIS. These open standards are foundational for the interoperability and machine processing that are key to address-

ing complexity, and acting on information quickly. The OASIS CTI Technical Committee, which maintain these standards, has the largest amount of corporate and individual members of any technical committee in the standards body.

Soltra utilizes these open standards and has the unique ability to be the "glue" between different sectors and to provide connectivity for those who do not have the time or infrastructure to manage the transition to STIX/TAXII. This common standard also allows a defender of networks to use CTI from community sources like ISACs and ISAOs; government sources such as the U.S. Departments of Homeland Security (DHS) and Treasury, along with the Federal Bureau of Investigation (FBI); and utilize that information in a variety of commercial and open source security tools. It also addresses the problems companies currently have when using multiple vendors whose bundling of CTIs may only work with that same vendor's tools. Soltra fixes this problem and allows for the use and scalability of information from multiple sources to be utilized in multiple tools that detect or defend the network.

Soltra also helps break down barriers between and amongst key sectors of the economy, providing the bridge from financial services to key sectors like health, energy, retail, as well as state, local, tribal and territorial (SLTT) governments. Historically, sectors only shared information within that sector. While important and effective to do, it also stovepipes the fact that the attackers are using the same Tactics, Techniques and Procedures (TTPs) against all sectors and allows them to effectively use the same tool to attack all sectors. Soltra breaks down the barriers to sharing by ultimately providing the "utility platform" and enabling interchange of information already in the STIX/TAXII format. We see this today with firms that are members of multiple ISAC/ISAO organizations and with ISACs that have sharing relationships with each other. Both of these act as cross sector bridges since it is simple to share information. Friction is greatly reduced when using Soltra to connect organizations – the same standard format, communications method, and access controls are used to respond to the data-handling instructions driven from the Traffic Light Protocol markings of content.

SOLTRA AND INFORMATION SHARING BRING GREATER SECURITY

Sharing information about threats remains essential as Mandiant reports[1] that for 2015 the median number of days from compromise to discovery was 146 days. This improved from a median of 229 days from the 2014 Mandiant report[2], but is still an extensive window. The 47% of firms that detected a breach themselves took 56 days to discover the breach, but the 53% of firms notified by an external party had a median of 320 days from compromise to detection.

This is directly relevant to information sharing in two ways. First, the delta between the time of an internal and external notification are likely a symptom of poor access to information about threats or ability to act on that information. Second, information shared about threats may represent intrusion sets recently identified that had been in situ for a long time. We need to both increase the percentage of internally discovered breaches and shorten the time to detect them. Sharing CTI data is one such way these discoveries are made and timely sharing leads to timely discovery. Soltra is working to solve this problem by widening the access to CTI data and shortening the time to act on it over manual methods. It is hard to know with certainty why the industry improved the lag in compromise to discovery, but it is highly likely information sharing tipping defenders on what to look for was a part of the improvement.

Third, there are some important lessons learned about the benefits of sharing information that, quite simply, will vary based upon the maturity of the institution participating in the program. However, a few things are universal:

First, initially when a company receives CTI data, it is purely a consumer of that information. It might find that it has limited technical or operational capabilities to utilize some or all of the information in an effective way. For example, it may receive indicator information about malware on endpoint, but not have a capability to scan end points for such files. At that juncture, the company will begin to realize that it needs to better understand what is in the data to actually be able to utilize it. For example, understanding how to use information when the temporal context is of an intrusion 300 days ago is important. If it then looks for that activity from the moment the CTI is received, it could miss the event that precipitated the intrusion several hundred days earlier. If it was just recently reported, the original victim may have just identified it and that data, even if it is a year old, might be the clue needed to ascertain if the same incident had occurred in your infrastructure. As a company

1 https://www2.fireeye.com/rs/848-DID-242/images/Mtrends2016.pdf

2 http://dl.mandiant.com/EE/library/WP_M-Trends2014_140409.pdf

moves up the maturity curve, it also moves from primarily utilizing the telemetry which is represented by the CTIs and starts to utilize insights and contextual information to anticipate hazards down the road. Even in mature sectors the bulk of the activity is around the telemetry CTI data.

As a company matures into using CTI data that was shared, it starts to realize that some data lacks sufficient context and may appear to be a false positive. This comes about between the very natural tension between sharing quickly when information is fresh, but could still be incomplete. This also occurs by the very nature of the investigative process that produces information and observations of activity that may have occurred during an attack but could be unrelated to the attacker's actions and are an artifact of normal IT system behavior. In order to address this, a company will want to have a method to ask the producing source to confirm details, or perhaps after its own research it will understand the context was lost or the CTI data is, in fact, inaccurate. A company will need to have a mechanism to share these results back to the producing source so they can adjust the content and send out a revision to the community.

This is important to note because as a company builds information sharing products it will need to support a range of needs and maturity levels. It will also need to have the capability to receive feedback on existing products in addition to the ability to consume new submissions from the community. Finally, a company will also need to create methods to address the level of trust needed between members of a community as that community scales and the parties become more remote to each other.

CISA IMPLEMENTATION

It has only been six months since CISA was signed into law, and while there has been a rapid fire of activity in that time, more work certainly remains to be done. Guidance issued on how to submit information under CISA by DHS/DOJ adhered to the letter of the law and described private to government sharing, but was silent on private to private sharing. This created some confusion concerning the scope of liability or when protections might apply. As an example, the FS-ISAC had to send a memo to all its members to clarify that the protection in the law did apply to private-to-private communications within the FS-ISAC membership. As recently as Thursday, June 9, 2016, DHS advised that CISA covers private to private sharing and that it would be included in the revised guidance required by Congress on June 15, 2016.

Soltra is one of the handful of companies that already has enrolled to DHS's Automated Indicator Sharing (AIS) program. As required by law, in March 2016 DHS opened access to its AIS platform along with the procedural documents of how to submit data to comply with the requirement in the law related to personal information. DHS has been a helpful partner in this process, and as is normally the case in any program, there are a number of areas that would benefit from clarification at this juncture. They include:

1. **Additional guidance is needed from DHS on the definition of Personally Identifiable Information (PII).** Thus far, the definition of PII in the AIS submission guidance differs from the definition of PII in other DHS programs and was not defined in the Act. The vast majority of information sharing about cyber threats does not involve any personal information, but the lack of clarity as to which definition would be used for personal information across DHS programs needs to be made clear. The financial sector sent a letter on May 11, 2016 to DHS and the U.S. Department of Justice asking for clarification on this matter.

2. **Current "Lessons Learned" Using the AIS System:**

    - **Streamline the process for signing up for AIS**: To enroll in the AIS program, participants need to execute two agreements with DHS, enroll to get an authentication certificate from an approved FedBRIDGE provider, submit network address information and technical details of the sharing platform to be used.

    - **Digital Certificates**: The AIS process requires all users to obtain a digital certificate from one of the three FedBRIDGE providers which has become a cumbersome process. As background, these certificates are traditionally issued to individuals to support strong authentication and email encryption whereas the use case for AIS is to authenticate a machine used for sharing within a company. At this juncture, the AIS system requires a single person within the company to obtain the certificate which then has to be loaded into the server to communicate

with the AIS system. That automated process actually requires paper documentation that has to be sent to DHS via the U.S. mail system. While the need for the authentication is critical, there is an inherent disconnect between the ultimate goal of the AIS system which is machine-to-machine. Going forward, it would be more helpful for a system to be created that allows for an organization level credential to be issued to the server used by the company to participate in the program. Other submission methods such as the web form and fax do not have the same authentication requirements.

- **AIS Changes to STIX/TAXII Fields**: Various aspects of the law as well as implementation have caused DHS to modify aspects of the STIX/TAXII fields. AIS also includes a series of "required" fields in STIX data submitted to the department which if not included, will reject any attempted submission from a company. It would be helpful for DHS to specify those up-front in order to help companies understand what needs to be done in advance of connecting to the AIS system.

- **Clarify how CISA protections apply to CISCP**: The AIS program does not support submissions of Proprietary Information (PROPIN) nor Protected Critical Infrastructure Information (PCII), although DHS does indicate information submitted under the CISCP program can receive protections for PROPIN or PCII. Many companies are used to submitting both PROPIN and PCII related information and it would be critical to ensure that companies can continue to do so, hopefully using the AIS system for sake of ease. DHS should also issue guidance on how the CISCP program fits under CISA to provide for greater clarifications.

- **Add a Test Environment Where Companies Can Ensure Its AIS Interface Works Effectively:** As is the case with many systems, it is preferable to be able to test whether or not a company's systems are interoperable with the AIS platform. Short deadlines in the law required the AIS system to be stood up quickly, and at this point, DHS does not have a system integration or test environment available. As a result, a company must attempt to work out the various issues in a live production environment. Moving forward, a test environment would be helpful for other companies and may allow for greater participation and ease of use in the future.

NEW DATA POINTS TO ADD TO AIS

There are three main data points that the private sector would like to see added to the AIS system to help increase the effectiveness of the AIS system:

1. Types of Threat Actors

It would be exceptionally helpful if the AIS data could include an assessment of the type of threat actor behind the activity when that is known. It is clear that there are practical challenges of "naming names" in an unclassified context. However, examples exist, including in the 2013 Defense Science Board report, "Resilient Military Systems and the Advanced Cyber Threat,"[3] that includes a six tier scale that would provide sufficient context to companies without naming specific actors.

2. Defensive Measures

One of CISA's objectives was to support the development of "defensive measures". While more work will be needed to get to that point, AIS could add in recommendations to how recipients might use the AIS data sets. For example if a set of AIS information was to include the suggested defensive measure of "block, mitigate, or monitor" it would inform consumers the best type of "defensive measure" to employ even if detailed recommendations are unavailable. This would be an important benefit to the AIS system that could bring a greater number of participants into the system.

3. Feedback Loop and Context to Data

Context is important for all companies who participate in the AIS program. As the AIS system continues to be fine-tuned, there are a number of issues that would be helpful to review and clarify which may increase greater connectivity and participation overall. As we know, the spectrum of possible participants will bring with them different skills, capabilities, and

3 http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf

maturities so for those submitting to AIS the downstream recipients want to understand the context and credibility of the information from AIS. These types of questions are foundational issues that have come from the variety of sectors Soltra supports, including those that are participating in the AIS program or those who have indicated they intend to participate in the near future. In the near future, industry participants will want to be able to select the type of data they want to receive from AIS which could include sector-specific or even cross-sector information. Levels of "trust" associated with the data will be important and industry participants will want to understand what process DHS will use if AIS members ask for more specific information from the AIS system, including the ability for DHS to reach back out to the original submitter of the data. Ultimately, DHS will need to be able to communicate how its internal process is set up to identify and vet the data submitted, a challenge that many ISACs have gone through themselves. The DHS guidance does mention a process that will be put in place to deal with false positives and mechanisms to address updating data and it will be critical that DHS provide clarity on that quickly.

CYBERSECURITY INFORMATION SHARING AND COLLABORATION PROGRAM (CISCP) AND PRIVATE SECTOR SECURITY CLEARANCES UNDER CISCP

Many of Soltra's customers and community members participate in the CISCP program, which is widely viewed as a beneficial program that facilitates cross-sector engagement with government. It brings private-sector and government analysts together at quarterly in-person meetings, the Advanced Technical Threat Exchanges (ATTE). CISCP also allows the private sector to work on the National Cybersecurity and Communications Integration Center (NCCIC) floor, giving participants access to DHS, LE and IC analysts. We are seeing an increase in production around CISCP analysts turning FS-ISAC reports into CISCP Indicator Bulletins.

CHANGES TO SECURITY CLEARANCES NEEDED

Challenges continue to exist in obtaining security clearances for companies. First, after the cybersecurity attack on the Office of Personnel Management (OPM), clearance times are much longer.

Second, it would be helpful if there was more transparency into the process with key performance metrics being made available to Critical Infrastructure and Key Resources (CIKR) members or their ISACs. It should include monthly breakdowns by sector and clearance types of the number of new clearances requested, the number of investigations completed, the aging of applications by stage, the number of reinvestigations initiated/completed per month, as well as median times for each stage.

Third, there have been a number of changes to the security clearance program that has caused challenges to many companies, including those who have historically had individuals on the NCCIC floor. As background, private sector companies have two routes to have essential personnel cleared for access to Classified Information. The first is the Private Sector Clearance Program (PSCP) initiated via the sector specific agency and sponsored/operated by DHS, and which holds clearances to the Secret level. The second route is by executing a Cooperative Research and Development Agreement (CRADA) with DHS. With a CRADA in place the firm needs to have a Facilities Clearance (FCL), which allows it to hold staff clearances up to Top Secret and have access to the NCCIC floor.

A recent change that greatly impacted a number of ISACs was the requirement to have the FCL in place for their company. This was not a previous requirement of the CRADA process for CISCP as DHS rolled it out and was added at a later date by the Defense Security Service (DSS.) A number of ISACs did not have FCLs current and therefore were removed from the NCCIC floor leaving no representation in the coordination process for those sectors. These ISACs do not have classified work areas in their offices and were using the NCCIC floor for any handling of classified materials. The requirements for obtaining the FCL are determined by the DSS. One attribute of this process is a requirement to clear top executives or board directors for companies. This program requirement made a lot of sense in the Defense Sector when the main objective of the FCL was managing contractors working on defense system projects. With the cybersecurity threat, the majority of the attack surface is in the private sector and many of the companies are multinationals with non-US citizens on corporate boards or executive management, rendering the existing scheme less tailored for successful application to today's environment.

The CISCP program with DHS requires a CRADA be in place for the receipt of unclassified information such as Cyber Threat Indicators. As a direct result of the change requiring the FCL for the CISCP CRADA, a number of financial sector firms are in

the process of ending their CRADA with DHS and going back to using the PSCP program to avoid the entanglement of having top executives or board members without cybersecurity responsibilities having to hold clearances which are orthogonal to their duties for the company. Again, this is to receive unclassified information from the DHS CISCP program.

The ISAC's that have an FCL will participate in CISCP via the CRADA and then be able to share unclassified information from CISCP with their members. As a practical matter, when classified information is shared with the private sector, this is done in a U.S. Government Facility with the appropriate FCL in place. It is unclear how ISACs that do not have the FCL will participate in the CISCP program going forward.

In addition to the problems with the CRADA and FCL, the problems and frustration with the clearance processes remain.

NEXT STEPS

Implementation of the Cybersecurity Information Sharing Act is moving forward quickly and DHS, DOJ and Congress are to be commended for how quickly the AIS system has been stood up, and the various guidance documents issued on time. As with every system, there are lessons learned and items that can be improved, and we look forward to working closely with DHS and others to achieve our collective goal.

Soltra and Soltra Edge are bringing cutting edge innovation and technical capabilities to the cybersecurity information sharing process. Soltra Edge is providing a simple and easy solution by providing the core backbone and technical processes that have previously prohibited many companies from sharing, thinking that the process is too cumbersome or difficult just to get started. Soltra is helping companies in all sectors to increase the ability and likelihood that information sharing can help provide vastly improved cybersecurity defenses and ultimately make it harder and more expensive for attackers. We look forward to working with this Committee, Congress and the Executive Branch, as well as with all of our private sector partners to achieve our collective goals.