May 11, 2016

Dr. Andrew Ozment
Assistant Secretary, Office of Cybersecurity & Communications
U.S. Department of Homeland Security
Washington, D.C. 20528

Mr. Scott Ferber
Senior Counsel to the Deputy Attorney General
U.S. Department of Justice
Washington, D.C. 20530

Dear Dr. Ozment and Mr. Ferber,

The undersigned financial services trade associations, on behalf of their member institutions, sincerely appreciate the significant amount of effort that the Departments of Homeland Security and Justice have devoted to developing the guidance documents required to implement the cybersecurity information sharing enhancement provisions of Public Law 114-113 (CISA). Our member institutions have found these documents useful as they build their systems and work to enhance the cyber threat information sharing processes within the sector, across sectors, and with their government partners. That being said, we do believe there are clarifications to the guidance documents that should be provided that would create a better roadmap for organizations who wish to expand or enhance the sharing of cyber threat information under this new framework.

Specifically, we urge you to:

1) More clearly explain how the liability protections are specifically afforded under CISA by publishing a table such as the example below:

"The following table applies to sharing that is conducted under the CISA framework and adheres to the requirements set forth in PL 114-113."

Sharing Entity	Receiving Entity	Disclosure Protections Received	Liability Protections Received	Antitrust Exemption Applied
Firm	Firm	Yes	Yes	Yes
Firm	ISAC or ISAO	Yes	Yes	Yes
Firm	DHS/NCCIC	Yes	Yes	N/A
Firm	U.S. government agency other than DHS/NCCIC	Yes	No	N/A
ISAC or ISAO	Firm	Yes	Yes	Yes

2) Clarify that the liability protections earned for sharing information with DHS/NCCIC apply to information shared using the following mechanisms:

- Automated Indicator Sharing (AIS) capability
- Web-form
- Email

3) Explain how this new framework for information sharing aligns with existing information sharing programs that DHS administers including: the Cyber Information Sharing and Collaboration Program (CISCP); the Protected Critical Infrastructure Information (PCII) program; and others.

4) Clarify language around sharing information with ISACs and ISAOs by making the following changes (highlighted in red and bolded) to the existing guidance:

> "Non-federal entities may also share cyber threat indicators and defensive measures with federal entities through Information Sharing and Analysis Centers or Information Sharing and Analysis Organizations, which **~~will~~ may** share them with federal entities through DHS on their behalf. Non-federal entities that share a cyber threat indicator or defensive measure with an Information Sharing and Analysis Center or Information Sharing and Analysis Organization—or any other non-federal entity—in accordance with the Act's requirements receive liability **and other protections and exemptions** for such sharing under section 106(b) of the Act. See Section 106(b)(1)."

5) CISA authorizes the sharing of classified cyber threat indicators however there is ambiguity about how that information will be shared. We would like to see the final procedures outline the following:

- How will classified information be shared with cleared members of the private sector?
- Which mechanisms will be utilized?

6) Provide further description about the AIS capability, now that it has been certified. Specifically, our sector would like additional clarification on:

- How will DHS be identifying/vetting who is providing data into AIS?
- How will DHS be validating/vetting the data being entered into AIS?
- How will AIS subscribers be able to select the data they want to receive from AIS, for example, will there be options for sector-based, cross-sector, trusted vs. untrusted sources, etc?

7) Provide further clarification on the definition of the term "personal information" because that term is undefined in the Act. For example, consider whether firms should interpret "personal information" as DHS has defined the term "personally identifiable information" (PII) across many of its programs as, "any information that permits the identity of an individual to be directly or indirectly inferred, including any other information that is linked or linkable to that individual regardless of whether the individual is a United States citizen, legal permanent resident, or a visitor to the United States."

As a related item, provide further clarification, with examples and a decision table, on which fraud/crime indicators are authorized to be shared or not shared under CISA. For example, cases exist in which fraud/crime (ex. 1Q16 spoofed CEO email fraud) is perpetuated via a cyber means, but the interim procedures are not clear if non-Federal entities may share this type of fraud/crime indicator and receive CISA protections.

Areas for Continued Collaboration

The financial services sector has built strong relationships with our partners at DHS and Treasury on cybersecurity information sharing over several years, and we would like to continue this through further collaboration on the following specific areas related to CISA implementation:

A) Classified cyber threat indicator sharing

- How will security clearances be granted (i.e. through the private sector clearance program or a new mechanism)?
- Will DHS develop a participation and reference guide related to this process? If so, will the guide include timelines and service-level agreement (SLA)-like mechanisms to ensure adherence to timelines?

B) Defensive Measures

- CISA also authorizes use and sharing of defensive measures. We would like to work with DHS to develop a decision framework for determining whether a measure is a "defensive measure" under CISA.

C) Strong Analytics

- One of the key benefits of increased information sharing is improved situational awareness of the cyber threats facing the critical infrastructure community. With the increased amount of information being shared with DHS, it is critical that DHS have the capacity to deliver analytic products reflecting this greater situational awareness to information sharing partners. In addition, we believe that given the variety of mechanisms that entities can use to share information, it is important that DHS develop the ability to identify duplicate indicators. For example, if a non-Federal entity shares an indicator with its ISAC (which subsequently shares it with DHS) and shares the same indicator directly with DHS, DHS will need to identify that it received the same indicator twice from a single originator, through two different sources.

The undersigned trade associations commend you for developing and publishing these guidance documents and appreciate your consideration of our request for further clarification. These recommendations demonstrate the sector's desire to work together to improve information sharing across the critical infrastructure community to ultimately strengthen the cybersecurity of the nation. We look forward to working with you on these topics.

Sincerely,

American Bankers Association
BITS | Financial Services Roundtable
Securities Industry and Financial Markets Association

Cc: Mr. Amias Gerety, Acting Assistant Secretary for Financial Institutions, U.S. Department of the Treasury