The Asset Management Industry
SERVING INDIVIDUAL INVESTORS
INVESTMENT COMPANY INSTITUTE

MEMO# 29802

March 30, 2016

The Departments of Homeland Security and Justice Publish Guidance Regarding Sharing Cyber Threat Information

[29802]

March 30, 2016

TO:

CHIEF INFORMATION SECURITY OFFICER ADVISORY COMMITTEE
COMPLIANCE MEMBERS No. 7-16
OPERATIONS MEMBERS No. 8-16
SMALL FUNDS MEMBERS No. 11-16
TECHNOLOGY COMMITTEE No. 4-16

RE:

THE DEPARTMENTS OF HOMELAND SECURITY AND JUSTICE PUBLISH GUIDANCE REGARDING SHARING CYBER THREAT INFORMATION

In December 2015, President Obama signed into law the Cybersecurity Act of 2015 (the "Act"). Title I of this Act consists of the Cybersecurity Information Sharing Act, which provides certain legal protections for sharing of specified cybersecurity information between and among the private sector, state and local governments, and the federal government. Title I also directs the U.S. Attorney General and the Secretary of the Department of Homeland Security ("DHS") to jointly develop guidance to promote the sharing of cyber threat indicators with federal entities pursuant to the Act. In February, this joint guidance was published. [*] It is briefly summarized below.

Key Concepts in the Guidance

The Guidance begins by noting that the Act authorizes non-federal entities to share "cyber threat indicators" and "defensive measures" with any other entity – private federal, state, or local – for a "cybersecurity purpose." As defined in the Act:

- "Cyber Threat Indicator" means information necessary to describe or identify matters

such as malicious reconnaissance, exploitations of security vulnerabilities, actual or potential harm caused by a cyber incident, and denial of service exploitations. According to the Guidance, other examples of cyber threat indicators that a private entity could submit to DHS under the Act include reports of: web server log files showing that a particular IP address has sent traffic that appears to be testing whether the company's content management system has not been updated to patch vulnerabilities; discovery of a technique that permits unauthorized access to an industrial control system; vulnerabilities discovered in software; a pattern of domain name lookups that may correspond to a malware infection; unexecuted malware found on a network; domain names or IP addresses associated with botnet commence and control servers; and the use of IP addresses to send malicious traffic.

- "Defensive Measures" means, generally speaking, an action, device , procedure, signature, technique, or other measure applied to an information system or to information stored on a system that detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability. The term does not include a measure that destroys, renders unusable, provides unauthorized access to, or substantially harms the system, information on the system, or information processed by a system that is not owned by the private entity operating the measure. Examples of defensive measures include, among others: computer programs that identify a pattern of malicious activity in the organization's web traffic; firewalls; and algorithms used to find anomalous patterns that might indicate malicious activity.
- "Cybersecurity Purpose" is the purpose of protecting an information system or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or cybersecurity vulnerability.

Information Sharing Protected under the Act

While the Act permits non-federal entities to share information relating to a cyber threat indicator or defensive measure for a cybersecurity purpose, prior to such sharing, the Act requires sharing entities first to remove information that the sharing entity knows at the time of sharing to be personal information of a specific individual or information that identifies a specific individual that is not directly related to the cybersecurity threat. The Guidance includes examples of information protected under privacy laws that are unlikely to be directly related to a cybersecurity threat and that should not be reported to the DHS. The examples include, among others, protected health information; human resource information; information relating to a person's education history; financial information; and identifying information on children under the age of 13.

Sharing Information with the Federal Government

The Guidance next discusses how a non-federal entity may share information relating to cyber threat indicators and defensive measures with federal and private entities. It notes that, unless sharing occurs as permitted by the Act and the Guidance, such sharing may not receive the Act's liability protections. It also notes that sharing in accordance with the Guidance does not relieve an entity from any sharing or reporting required under other provisions of federal law; sharing in accordance with the Guidance is intended to complement, not replace, the prompt reporting of criminal activity, cyber incidents, or reportable events as required by law.

As mentioned above, prior to a non-federal entity sharing cyber threat indicators with a federal entity, the non-federal entity must determine whether the information to be shared contains any information directly related to a cybersecurity threat that the sharer know at the time of the sharing to be personal information of a specific individual or information

that identifies a specific information. If so, the sharer must remove such personal information. Though not required by the Act, the Guidance suggests the sharer conduct a similar review prior to sharing any defensive measures under the Act.

The DHS has developed an “Automated Indicator Sharing” (“AIS”) initiative that enables the timely exchange of cyber threat indicators and defensive measures among the private sector, state and local governments, and the federal government. This AIS portal enables the DHS to receive information shared under the Act and relay such information to other federal entities in an automated manner as required by the Act. The DHS has developed a form that can be used to submit information to DHS through the AIS. This form is available at www.us-cert.gov/forms/share-indicators. According to the Guidance, once the shared information is received, analyzed, and sanitized, AIS will share it with all AIS participants without providing the identity of the submitting entity unless the submitter consents to the sharing of their identity. Persons reporting information through the AIS system in accordance with the Act will receive the Act’s liability protections, which are discussed below. The Guidance discusses how entities may participate in the AIS system.

The Guidance discusses ways, other than the AIS system, that entities may share information under the Act. For example, non-federal entities may also share cyber threat indicators and defensive measures with DHS by sending an email to DHS. More information about how entities may submit information under the Act to DHS is available at www.us-cert.gov/ais.

Protections the Act Provides to Persons Sharing Information

In addition to the liability protections discussed above, the Act also protects an entity sharing information under the Act from: the federal antitrust laws; laws that provide public access to government-held information (e.g., freedom of information laws); waivers of any applicable privilege or protection provided by law (including trade secret protections); and provisions relating to ex parte communications under the Administrative Procedures Act.

* * * * *

The last page of the Guidance consists of a chart that summarizes the Guidance’s discussion of the Means of Sharing, the Authority for Sharing, the Receiving Federal Entity, the Requirements for Sharing, and the Protections Conferred for Sharing Under the Act.

Tamara K. Salmon
Associate General Counsel

endnotes

[*] See Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities under the Cybersecurity Information Sharing Act of 2015, DHS and the Department of Justice (February 16, 2016) (“Guidance”), which is available at: https://www.us-cert.gov/sites/default/files/ais_files/Federal_Government_Sharing_Guidance_(103).pdf.