WILMERHALE

DHS and DOJ Release Updated Guidance for Sharing Cyber Threat Indicators and Defensive Measures

JUNE 22, 2016

On June 15, in response to feedback from non-federal entities on guidance released in February, the Departments of Homeland Security (DHS) and Justice (DOJ) issued updated guidance for companies about sharing cyber threat indicators and defensive measures with the federal government under the Cybersecurity Information Sharing Act (CISA).

The new guidance identifies:

- the types of information that qualify as a cyber threat indicator that would be unlikely to include information that is not directly related to a cybersecurity threat and is personal information of a specific individual or information that identifies a specific individual; and
- information protected under otherwise applicable privacy laws that are unlikely to be directly related to a cybersecurity threat.

The guidance explains how companies can share such information with the federal government, both through the principal channel created by DHS and through other routes allowed by CISA. The guidance also explains how to identify and share cyber defensive measures. Finally, it recaps the different kinds of legal authorization and liability protection CISA provides for these activities.

Identifying Cyber Threat Indicators and Defensive Measures

CISA defines a cyber threat indicator as information that is necessary to describe or identify:

- malicious reconnaissance, including anomalous patterns of communications that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat or security vulnerability;
- a method of defeating a security control or exploitation of a security vulnerability;
- a security vulnerability, including anomalous activity that appears to indicate the existence of a security vulnerability;
- a method of causing a user with legitimate access to an information system or information that is stored on, processed by or transiting an information system to unwittingly enable the defeat of a security control or exploitation of a security vulnerability;
- malicious cyber command and control;

- the actual or potential harm caused by an incident, including a description of the information exfiltrated as a result of a particular cybersecurity threat;
- any other attribute of a cybersecurity threat, if disclosure of such attribute is not otherwise prohibited by law; or
- any combination thereof.

The guidance provides the following example to illustrate how some of the pieces of information in an email may constitute cyber threat indicators and some may not:

> Information is not directly related to a cybersecurity threat if it is not necessary to detect, prevent, or mitigate the cybersecurity threat. For example, a cyber threat indicator could be centered on a spear phishing email. For a phishing email, personal information about the sender of email ("From"/"Sender" address), a malicious URL in the e-mail, malware files attached to the e-mail, the content of the e-mail, and additional email information related to the malicious email or potential cybersecurity threat actor, such as Subject Line, Message ID, and X-Mailer, could be considered directly related to a cybersecurity threat. The name and e-mail address of the targets of the email (i.e., the "To" address), however, would be personal information not directly related to a cybersecurity threat and therefore should not typically be included as part of the cyber threat indicator.

The guidance identifies a number of examples of information that would contain cyber threat indicators that a private entity could submit to DHS and other federal entities under CISA:

- a company could report that its web server log files show that a particular IP address has sent web traffic that appears to be testing whether the company's content management system has not been updated to patch a recent vulnerability;
- a security researcher could report on her discovery of a technique that permits unauthorized access to an industrial control system;
- a software publisher could report a vulnerability it has discovered in its software;
- a managed security service company could report a pattern of domain name lookups that it believes correspond to malware infection;
- a manufacturer could report unexecuted malware found on its network;
- a researcher could report on the domain names or IP addresses associated with botnet command and control servers;
- an engineering company that suffers a computer intrusion could describe the types of engineering files that appear to have been exfiltrated, as a way of warning other companies with similar assets; and
- a newspaper suffering a distributed denial of service attack to its web site could report the IP addresses that are sending malicious traffic.

To help ensure consistency with CISA's definitions and requirements, the guidance recommends using standard fields of information, such as those developed for the Structured Threat Information eXchange (STIX).

The guidance also provides a number of illustrative examples of defensive measures:

- a computer program that identifies a pattern of malicious activity in web traffic flowing into an organization;
- a signature that could be loaded into a company's intrusion detection system in order to detect a spear phishing campaign with particular characteristics;
- a firewall rule that disallows a type of malicious traffic from entering a network;
- an algorithm that can search through a cache of network traffic to discover anomalous patterns that may indicate malicious activity; and
- a technique for quickly matching, in an automated manner, the content of an organization's incoming Simple Mail Transfer Protocol (SMTP, a protocol commonly used for email) traffic against a set of content known to be associated with a specific cybersecurity threat without unacceptably degrading the speed of email delivery to end users.

Categories of Information Unlikely to be Directly Related to a Cybersecurity Threat

CISA requires non-federal entities to remove any information from a cyber threat indicator or defensive measure that the 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 a cybersecurity threat before sharing that cyber threat indicator or defensive measure with a federal entity. Cyber threat indicators and defensive measures will typically consist of technical information that describes attributes of a cybersecurity threat and thus usually will not include various categories of information that are protected by privacy laws. In order to assist sharing entities discharge their obligation to remove personal information, the guidance describes several categories of information that are unlikely to be directly related to a cybersecurity threat and protected under otherwise applicable privacy law. These include:

- protected health information;
- employee personnel files;
- consumer information relating to an individual's purchases, preferences, complaints, or credit;
- student education records, including transcripts and professional certifications;
- financial information;
- information concerning property ownership; and
- information identifying children under the age of 13.

Because the contents of communications are particularly likely to include information from these protected categories, the guidance recommends that companies "exercise particular care when reviewing such information before sharing it with a federal entity." Nevertheless, it also admits that some of these categories can be used in connection with threats such as social engineering attacks, and may be shareable as a result.

Information-Sharing Mechanisms

CISA envisions three processes for sharing information:

1. sharing via a DHS "capability or process";

2. sharing with federal entities outside this method; and
3. sharing among industry (or “non-governmental entities”).

Each process involves different methods for sharing and provides different legal protections.

The first method takes advantage of mechanisms operated by DHS pursuant to Section 105(c)(1)(B) of CISA. These includes DHS’s Automated Indicator Sharing (AIS) initiative, which was certified for deployment and made “ open for business” in March 2016. Other sharing methods under Section 105(c)(1)(B) include sending an email to or using a web form provided by DHS’s National Cybersecurity and Communications Integration Center (NCCIC). Information shared with NCCIC through other electronic means may also be covered. Information companies share with private Information Sharing and Analysis Centers (ISACs) or Information Sharing and Analysis Organizations (ISAOs) that is then shared with DHS on their behalf is also covered. Section 105(c)(1)(B) sharing receives both liability protection and other statutory protections under CISA.

The second method involves sharing outside this framework with DHS or with other federal entities, such as the FBI, the Treasury Department or the Defense Department. This kind of sharing, authorized under Section 104(c) of CISA, does not receive liability protection, but does get other statutory protections, including:

- antitrust exemption;
- exemption from federal and state disclosure laws;
- exemption from certain federal and state regulatory uses;
- no waiver of privilege;
- treatment as commercial, financial, and proprietary information; and
- *ex parte* communications waiver.

Finally, while the guidance notes that CISA does not direct the federal government to produce guidance on how companies may share information among themselves under CISA, Section 104(c) also authorizes the sharing of cyber threat indicators and defensive measures among private entities and such sharing receives both liability and antitrust protection. However, sharing between private entities (including ISACs and cybersecurity and managed security services providers) is subject to CISA’s requirements that only cyber threat indicators and defensive measures are shared and personal information be removed.