# Cybersecurity Information Sharing Act of 2015 Guidance

February 2016

Contact:
Jeremy Dalpiaz
AVP, Cyber Security and Data Security Policy
Jeremy.Dalpiaz@icba.org


Independent Community Bankers of America®
www.icba.org

# Cybersecurity Information Sharing Act of 2015 Guidance

## I. BACKGROUND

The Cybersecurity Information Sharing Act of 2015 ("CISA" or "the Act") was passed by Congress and signed into law by President Obama on December 18, 2015.[1] The Act permits voluntary, reciprocal sharing of cyber threat indicators and defensive measures by non-federal entities with the Federal government. Guidance issued jointly by the Departments of Homeland Security (DHS) and Department of Justice on February 16, 2016[2] ("Guidance") detail the methods for identifying and sharing these indicators and measures with the government and explains certain liability and antitrust protections afforded under the Act.

## II. OVERVIEW

Community banks that already share information through the Financial Services Information Sharing and Analysis Center (FS-ISAC) will not need to implement any changes to their current process. For existing FS-ISAC users, the Act provides clarity of the legal protections provided to institutions that voluntarily share cyber threat indicators and defensive measures.

For institutions that do not use the FS-ISAC for these purposes, this Act permits community banks the ability to share cyber threat indicators and defensive measures through a variety of new methods: through the DHS's Automated Indicator Sharing (AIS) initiative,[3] a web form on a DHS National Cybersecurity and Communications Integration Center (NCCIC) website, or through email. Sharing information through these avenues, including via FS-ISAC, will afford community banks certain legal protections, provided that the shared information meets the criteria as set forth in the Guidance and does not include personal information.[4]

## III. SUMMARY

Information sharing is advantageous for the banking community. First, it enables information to be shared consistently across the entire banking sector. Second, it will assist community banks detect and mitigate a broad range of cyber threats which are ever-evolving and quickly changing. In short, information sharing will lead to a more resilient banking community.

---

[1] U.S. Congress. Public Law. 114-113, "Consolidated Appropriations Act, 2016" Division N, Title I. https://www.congress.gov/bill/114th-congress/house-bill/2029/text.

[2] Department of Homeland Security and Department of Justice. "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." 16 February 2016. https://www.us-cert.gov/sites/default/files/ais_files/Non-Federal_Entity_Sharing_Guidance_%28Sec%20105%28a%29%29.pdf. See also: https://www.us-cert.gov/ais. Referred to hereinafter as "Guidance."

[3] DHS AIS uses a "technical specification for the format and exchange of cyber threat indicators and defensive measures using the Structured Threat Information eXchange (STIX) and Trust Automate eXchange of Indicator Information (TAXII)". See page 12 of "Guidance". This mechanism must first be certified by the NCCIC within 90 days of enactment of the law (March 18, 2016) before it is fully implemented.

[4] FS-ISAC operating rules dictate that an institution must remove personal information from threat information before sharing that information with FS-ISAC.

The AIS program provides several methods by which information may be shared, which is narrowly defined by the Act and explained in the Guidance. For instance, a cyber threat indicator is information necessary to describe or identify malicious reconnaissance (abnormal patterns of communication that is transmitting information related to a threat or vulnerability, a method of defeating a security control or exploiting a vulnerability, execution of malware by a legitimate user (i.e. phishing), malicious cyber command and control and others).[5]

A defensive measure, on the other hand, is something that is done to detect, prevent or mitigate a known or suspected cyber threat or vulnerability. This includes actions, devices, procedures, techniques or other measures applied to an information system to accomplish this objective.

Personal Information

In addition to narrowly defining cyber threat indicators and defensive measures, CISA requires the removal of PI from the information being shared. The Guidance specifically addresses this point:

> CISA requires a non-federal entity to remove any information from a cyber threat indicator or defensive measure that it knows at the time of sharing to be personal information of a specific individual or information that identified a specific individual that is not directly related to a cybersecurity threat before sharing it with a federal entity (Section 104(d)(2)).[6]

For example, the email address of a victim may be considered personal information. However, the email and IP address of the attacker may not be personal information as they are threat indicators. Likewise, software vulnerabilities and techniques that allow for unauthorized access to a control system could also be shared.[7]

Impact on Privacy Notices

As the Guidance explain, cyber threat indicators will normally consist of only technical information that describes the cyber threat. It is important for community banks to note, that certain information that is unlikely to be related to a cybersecurity threat may be impacted by other privacy laws, such as Gramm-Leach-Bliley Act ("GLBA") and it's implementing regulations.

ICBA believes that providing cyber threat information under CISA would not constitute a material change in a bank's data security policies and practices and thereby would not trigger an annual privacy notice requirement.

Recent amendments to GLBA provide an exception to the annual privacy notice requirements for banks that have not changed their policies or practices – including their data security policy - since their most recent privacy notice and provide personal information only for certain exceptions, including as required for institutional risk control; to protect the confidentiality or security of the bank's records pertaining to

[5] "Guidance." https://www.us-cert.gov/sites/default/files/ais_files/Non-Federal_Entity_Sharing_Guidance_%28Sec%20105%28a%29%29.pdf. Pages 4-6.
[6] "Guidance". Page 7.
[7] "Guidance". Page 5.

its customers, the service or product, or transactions as well as to protect against or prevent actual or potential fraud, unauthorized transactions, or other liability.[8]

Other Protections

In addition to liability protections afforded to the bank sharing information with the Federal government, other protections are extended as well, such as:[9]

- Antitrust Exemption – Sharing cyber threat indicators and defensive measures with the Federal government or through one of the other accepted methods does not violate federal antitrust laws.
- Exemption from Federal and State Disclosure Laws: Information shared under this Act is not subject to public disclosure (i.e. Freedom of Information Act (FOIA) Requests)
- Exemption from Certain State and Federal Regulatory Uses: Regulators cannot regulate or take enforcement actions against a community bank based on the cyber threat indicators they share. However, regulators may use the shared defensive measures in the development and implementation of regulations.

When Liability Protections Are Not Extended

In most cases, community banks will likely elect to share information by removing PI through the FS-ISAC sharing mechanism or via the DHS AIS initiative. However, if a community bank shares PI information directly with a federal entity other than DHS, for instance with the Department of Treasury, the liability protections under this Act would not apply. In such instances, however, community banks may be protected by way of another law, regulation or guidance. For example, although community banks would not have liability protections under this Act when sharing information with FinCEN and regulatory authorities on money laundering activities, they are protected under the PATRTIOT Act and its implementing regulations.[10]

Sharing Cyber Threat Indicators and Defense Mechanisms Does Not Relieve Other Reporting Requirements

Although community banks should strongly consider using the FS-ISAC or DHS AIS initiative for sharing these types of cyber threat indicators and/or defensive measures if they so elect, such sharing does not relieve a community bank from any other requirement or obligation to report other types of information to federal entities, such as known or suspected cybercrimes directly to appropriate law enforcement agencies, known or suspected cyber incident directly to the National Cybersecurity and Communication Integration Center, or required reporting regulatory agencies," for example, requirements under the Bank Secrecy Act.

[8] Section 75001 of Fixing America's Surface Transportation (FAST) Act, amending 15 U.S.C. 6803
[9] For a full list, see "Guidance" pages 14-16.
[10] 31 USC 5311