Homeland Security

Office of Cybersecurity & Communications

Cybersecurity Information Sharing Act of 2015

June 2016

Cybersecurity Act of 2015

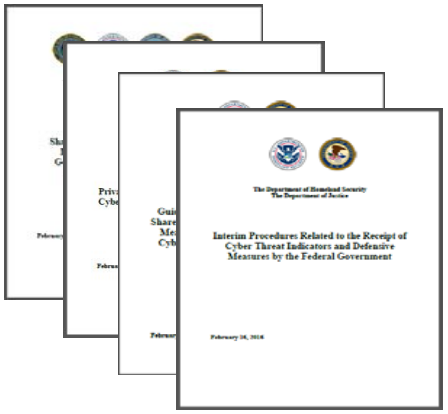
- Title 1: Cybersecurity Information Sharing Act of 2015
  - Establishes procedures, privacy protections, and liability and other legal protections
- Title 2: National Cybersecurity Advancement
  - Enhances NCCIC's intrusion detection and prevention capabilities
  - Further defines NCCIC's information sharing authorities
- Other titles cover
  - Federal cybersecurity workforce assessment
  - DHS mobile device study
  - HHS healthcare sector task force with NIST and DHS
  - Statewide Interoperability Coordinator reporting cybersecurity matters to NCCIC; NCCIC provides analysis and support

Cybersecurity Information Sharing Act of 2015

- Authorizes companies to share cyber threat indicators and defensive measures with each other and with DHS, with liability protection
- Identifies permitted uses of cyber threat indicators and defensive measures
- Authorizes companies to monitor their own information systems and to operate defensive measures on their systems
- Establishes privacy protections required of the sharing entity and receiving government agency

CISA Deliverables

- Four February 16 documents (delivered to Congress and posted online):
  - Guidelines for sharing information by the Federal Government
  - Guidance to companies and non-federal entities for sharing cyber threat indicators and defensive measures with the Federal Government (updated June 15)
  - Interim operational procedures for sharing cyber threat indicators and defensive measures with the Federal Government (updated June 15)
  - Privacy and civil liberties interim guidelines (updated June 15)



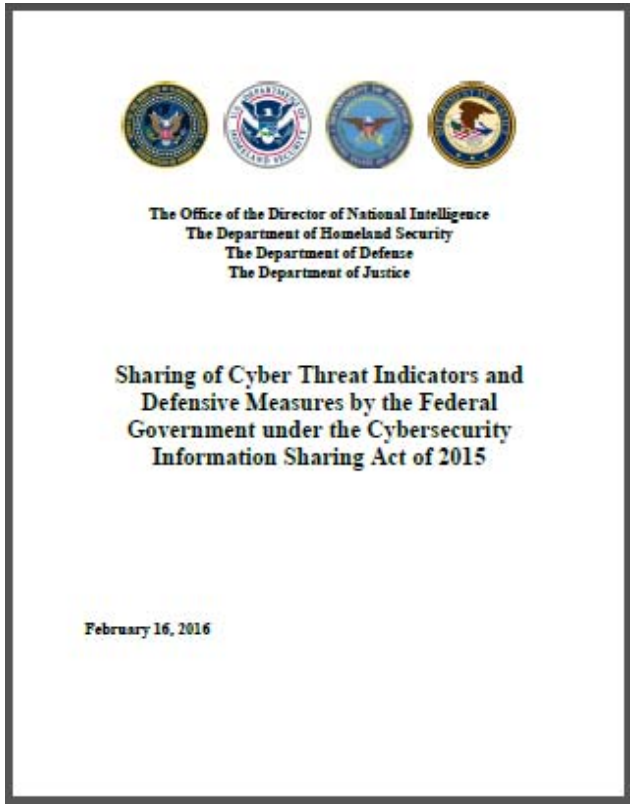
- Secretary of Homeland Security March 17 certification that automated capability authorized by Act is operational

CISA Deliverables

- *Guidelines for sharing information by the Federal Government*

  - Summary: Describes the current mechanisms through which the appropriate Federal entities share information with non-Federal entities.

  - Due Date: Final at 60 days (February 16, 2016) due to Congress.



The Office of the Director of National Intelligence
The Department of Homeland Security
The Department of Defense
The Department of Justice

Sharing of Cyber Threat Indicators and Defensive Measures by the Federal Government under the Cybersecurity Information Sharing Act of 2015

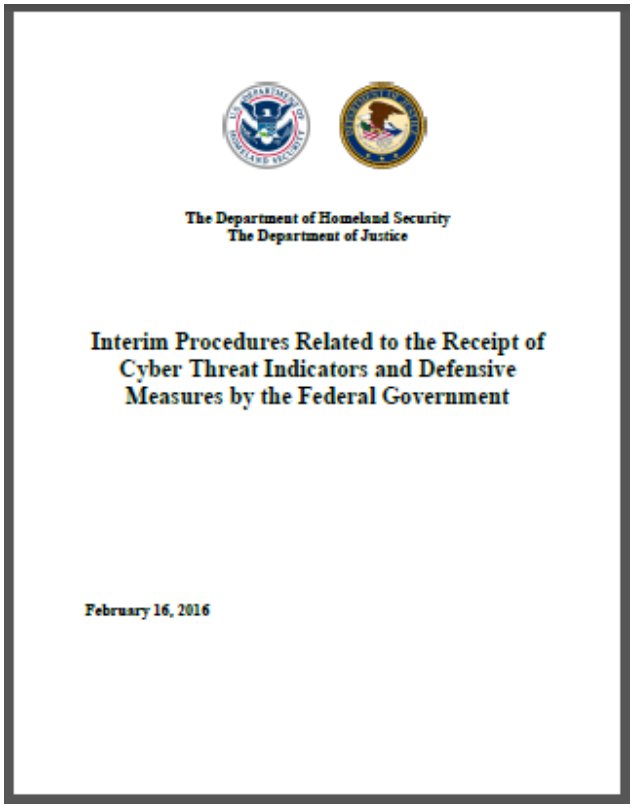
February 16, 2016

CISA Deliverables

- *Interim operational procedures for sharing cyber threat indicators and defensive measures with the Federal Government*

  - Summary: Establishes procedures relating to the receipt of certain cyber threat indicators and defensive measures by all Federal entities under CISA. Describes the processes for receiving, handling, and disseminating information that is shared pursuant to CISA, including through operation of the DHS Automated Indicator Sharing capability.

  - Due Date: Interim at 60 days (February 16, 2016) submitted to Congress, Final at 180 days (June 15, 2016) made publicly available.



The Department of Homeland Security
The Department of Justice

Interim Procedures Related to the Receipt of Cyber Threat Indicators and Defensive Measures by the Federal Government

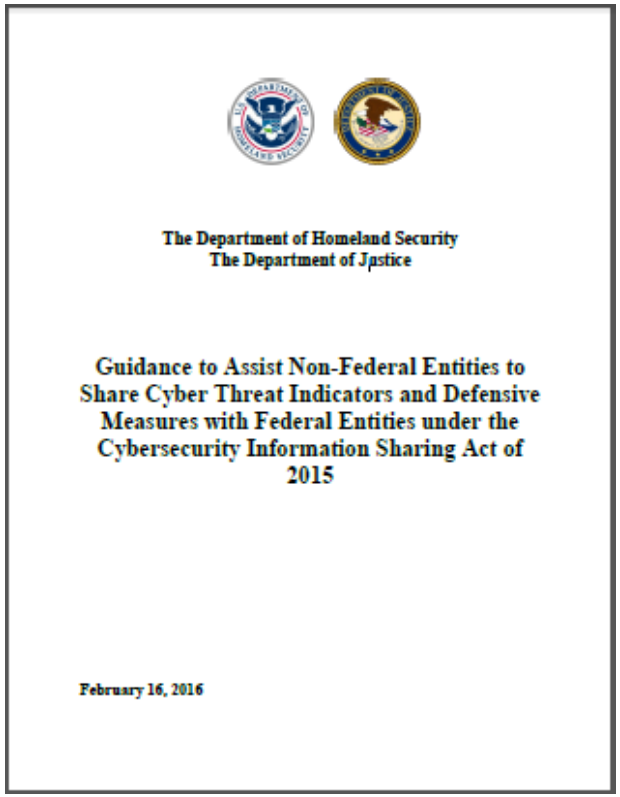
February 16, 2016

CISA Deliverables

- *Guidance to companies and other non-federal entities for sharing cyber threat indicators and defensive measures with the Federal Government*

  - Summary: Provides information to assist non-federal entities who voluntarily elect to share cyber threat indicators with the federal government to do so in accordance with CISA. Assists non-federal entities to identify defensive measures and explain how to share them with federal entities as provided by CISA. Describes the protections non-federal entities receive under CISA.

  - Due Date: Final at 60 days (February 16, 2016) made publicly available; ; updated June 15.

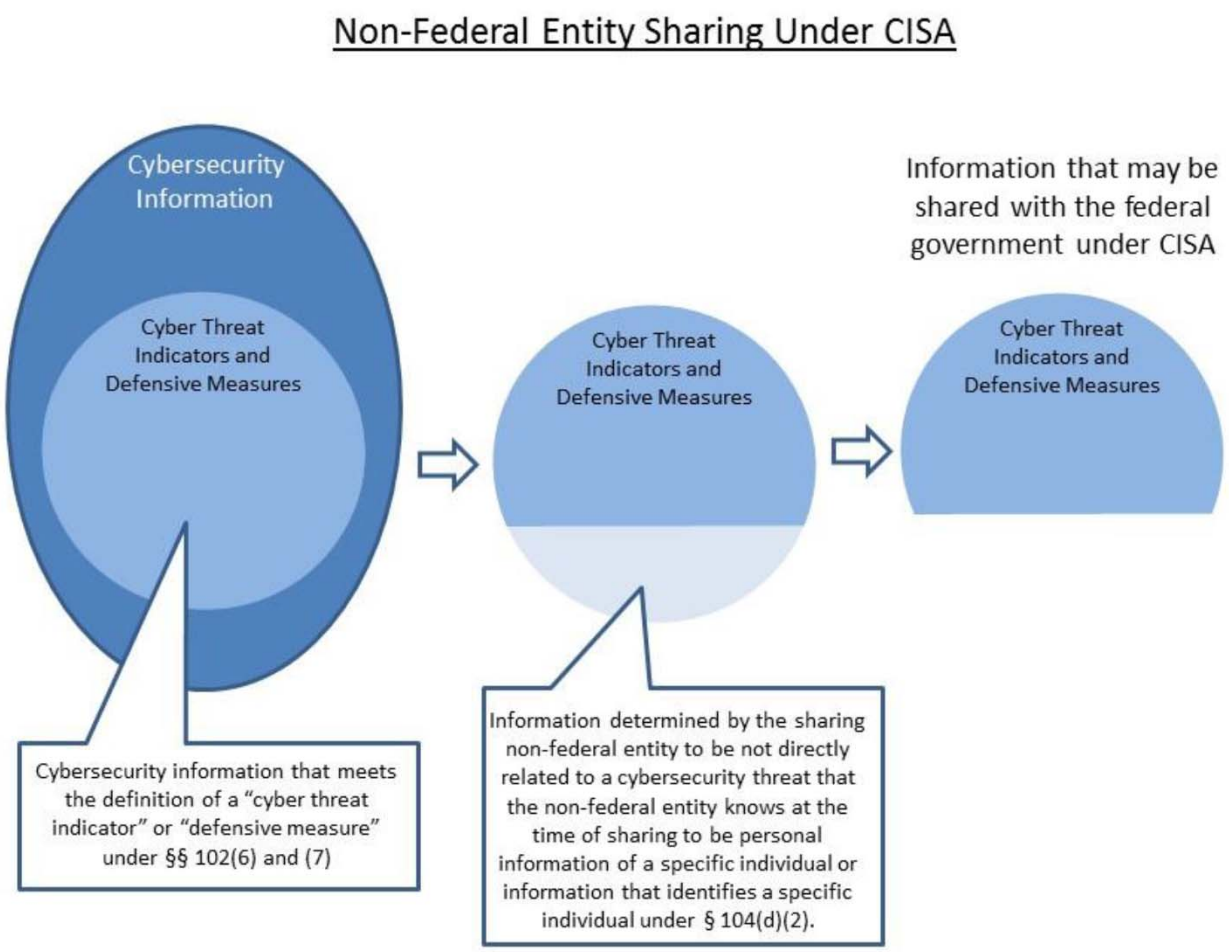


The Department of Homeland Security
The Department of Justice

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

February 16, 2016

Cyber Threat Indicators and Defensive Measures



Liability Protection

- CISA extends liability protection to private entities for sharing of a cyber threat indicator or defensive measure through the Federal government's capability and process operated by DHS
  - As long as the sharing is conducted in accordance with the Act.

- For more information please 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 (available at www.us-cert.gov/ais) or
  - Section 106 of CISA.

SLTT-Specific Provisions

- Law Enforcement Use
  - SLTT government that receives a cyber threat indicator or defensive measure under CISA may use it for specified purposes, such as a cybersecurity purpose, identifying a cybersecurity threat, identifying a security vulnerability, responding to or preventing/mitigating a specific threat of death, serious bodily harm serious threat to a minor or serious economic harm, or prosecuting offenses under 18 U.S.C. 1028-1030

- Exemption from Disclosure
  - A cyber threat indicator or defensive measure shared by or with an SLTT government, including a component of such government that is a private entity, under CISA is deemed voluntarily shared information and exempt from disclosure under State, tribal or local freedom of information, open government, open records, sunshine or similar laws

- Regulatory Authority
  - Cyber threat indicator or defensive measure cannot be used to regulate the lawful activity of a non-Federal entity
  - Exception: They may be used consistent with a regulatory authority specifically relating to the prevention of mitigation of cybersecurity threats to inform development or implementation of such regulation

Privacy Protections in CISA

- CISA includes various privacy protections for the receipt, retention, use and dissemination of cyber threat indicators.

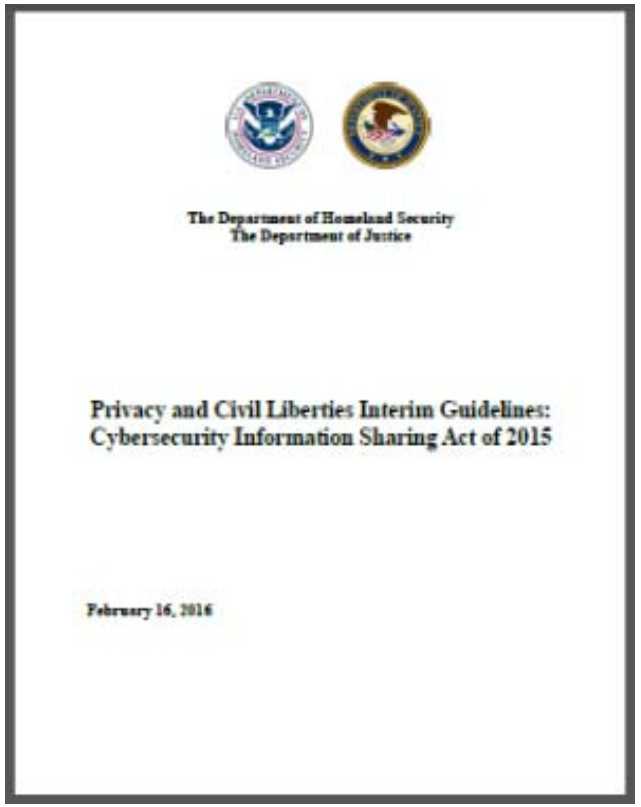
- One main privacy protection requires Federal and Non-Federal entities, prior to sharing to:

  - Review such cyber threat indicator to assess whether such cyber threat indicator contains any information not directly related to a cybersecurity threat that such Federal/Non-Federal entity knows at the time of sharing to be personal information of a specific individual or information that identifies a specific individual and remove such information; or

  - Implement and utilize a technical capability configured to remove any information not directly related to a cybersecurity threat that the Federal/non-Federal entity knows at the time of sharing to be personal information of a specific individual or information that identifies a specific individual.

CISA Deliverables

- *Privacy and civil liberties interim guidelines*
  - Summary: Establishes privacy and civil liberties guidelines for the receipt, retention, use, and dissemination of cyber threat indicators by a Federal entity obtained in connection with the activities authorized by CISA, consistent with the need to protect information systems from cybersecurity threats, any other applicable provisions of law, and the Fair Information Practice Principles.
  - Due Date: Interim at 60 days (February 16, 2016) to Congress and made publicly available, Final at 180 days (June 15, 2016) made publicly available.
    Require review every 2 years.


The Department of Homeland Security
The Department of Justice

Privacy and Civil Liberties Interim Guidelines:
Cybersecurity Information Sharing Act of 2015

February 16, 2016

DHS AIS Privacy Scrub

- Under AIS, DHS will receive cyber threat indicators and defensive measures through that portal in a standard, automated format and apply unanimously agreed upon controls as described in the Section 105(a)(1)-(3) procedures.

- DHS will use automated processing for mitigation of remaining personal information risks through schema restrictions, controlled vocabulary, regular expressions (i.e., pattern matching), known good values, and auto-generated text.

- Any fields that do not meet certain predetermined criteria defined through the AIS Profile and in the submission guidance will be referred for human review to ensure the field does not contain personal information of specific individuals or information that identifies specific individuals not directly related to the cybersecurity threat.

- When a field within a cyber threat indicator or defensive measure is referred for human review, DHS will still transmit the fields that do not require human review to the appropriate Federal entities without delay.

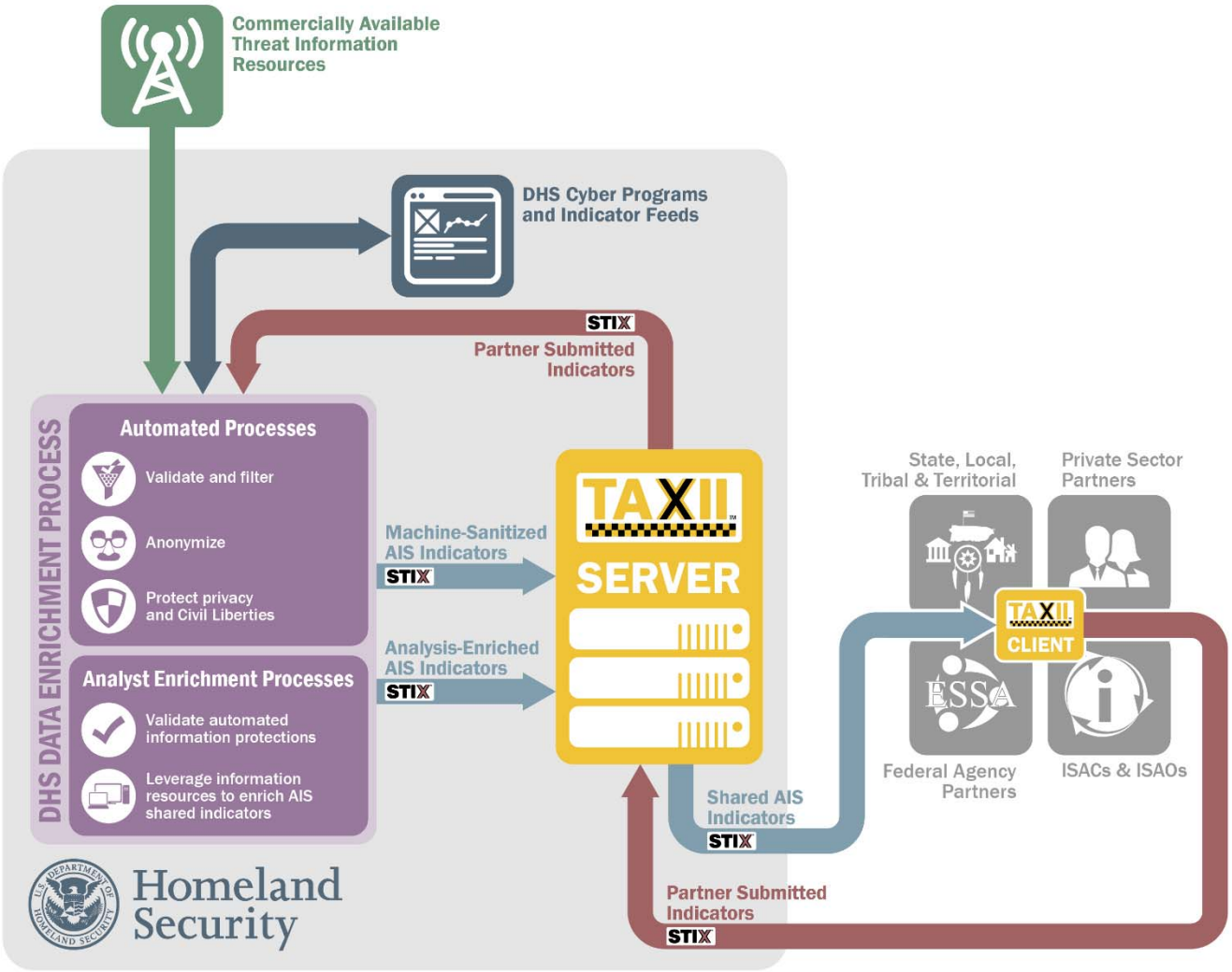
CISA Capabilities

- Automated Real-Time Capability: Automated Indicator Sharing (AIS)
  - Uses the Structured Threat Information eXpression (STIX) standard (xml format with a series of machine-readable fields) and Trusted Automated eXchange of Indication Information (TAXII) protocol

- Web Form and Email options
  - www.us-cert.gov/ais

- Privacy Scrub

Automated Indicator Sharing



How to Sign Up for AIS

1. Sign and return the appropriate participation agreement.
   - Terms of Use (non-federal entities)
   - Multilateral Information Sharing Agreement (for Federal D/As)
2. Next, have something that can talk TAXII.
   - You can use the DHS TAXII client, an open source implementation or purchase a commercial solution.
3. Sign an Interconnection Security Agreement to document the connection and capture relevant security information.
4. Finally, we exchange certificates and you give us the IP(s) you're coming from so it can get whitelisted.



CS&C Contact Information

For more information:

- www.DHS.gov/AIS
- www.us-cert.gov/AIS

Additional Questions?

- CSCExternalAffairs@HQ.DHS.gov