Homeland Security

If It's Worth Sharing, It's Worth Sharing Right— Technical, Policy and Legal Considerations of Cyber Threat Intelligence Sharing

Richard Struse
Chief Advanced Technology Officer, NCCIC
US Department of Homeland Security

Chair,
OASIS Cyber Threat Intelligence Technical Committee

Disclaimer

This presentation is intended for informational and discussion purposes only.

The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding this information. In no event shall the United States Government or its contractors or subcontractors be liable for any damages, including but not limited to, direct, indirect, special or consequential damages, arising out of, resulting from, or in any way connected with this information, whether or not based upon warranty, contract, tort, or otherwise, whether or not arising out of negligence, and whether or not injury was sustained from, or arose out of the results of, or reliance upon the information.

The display of the DHS official seal or other DHS visual identities, including the US-CERT or ICS-CERT name or logo shall not be interpreted to provide any person or organization the authorization to use the official seal, insignia or other visual identities of the Department of Homeland Security, including US-CERT and ICS-CERT. The DHS seal, insignia, or other visual identities shall not be used in any manner to imply endorsement of any commercial product or activity by DHS, US-CERT, ICS-CERT or the United States Government. Use of the DHS seal without proper authorization violates federal law (e.g., 18 U.S.C. §§ 506, 701, 1017), and is against DHS policies governing usage of its seal.

This presentation is Traffic Light Protocol (TLP): WHITE. Recipients may share TLP: WHITE information without restriction, subject to copyright controls. For more information on the TLP, see *http://www.us-cert.gov/tlp*.

DHS does not endorse any commercial product or service, including any subjects of analysis. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply their endorsement, recommendation, or favoring by DHS.

NCCIC

- Strives for a safer, strong Internet for all Americans by responding to major incidents, analyzing threats, and **exchanging critical cybersecurity information with trusted partners around the world**
- We are *not* regulators or law enforcement or intelligence or defense
- We are specially trained in handling private, sensitive and proprietary data, protecting it and sharing it appropriately to improve cybersecurity and infrastructure protection

Some Assumptions…

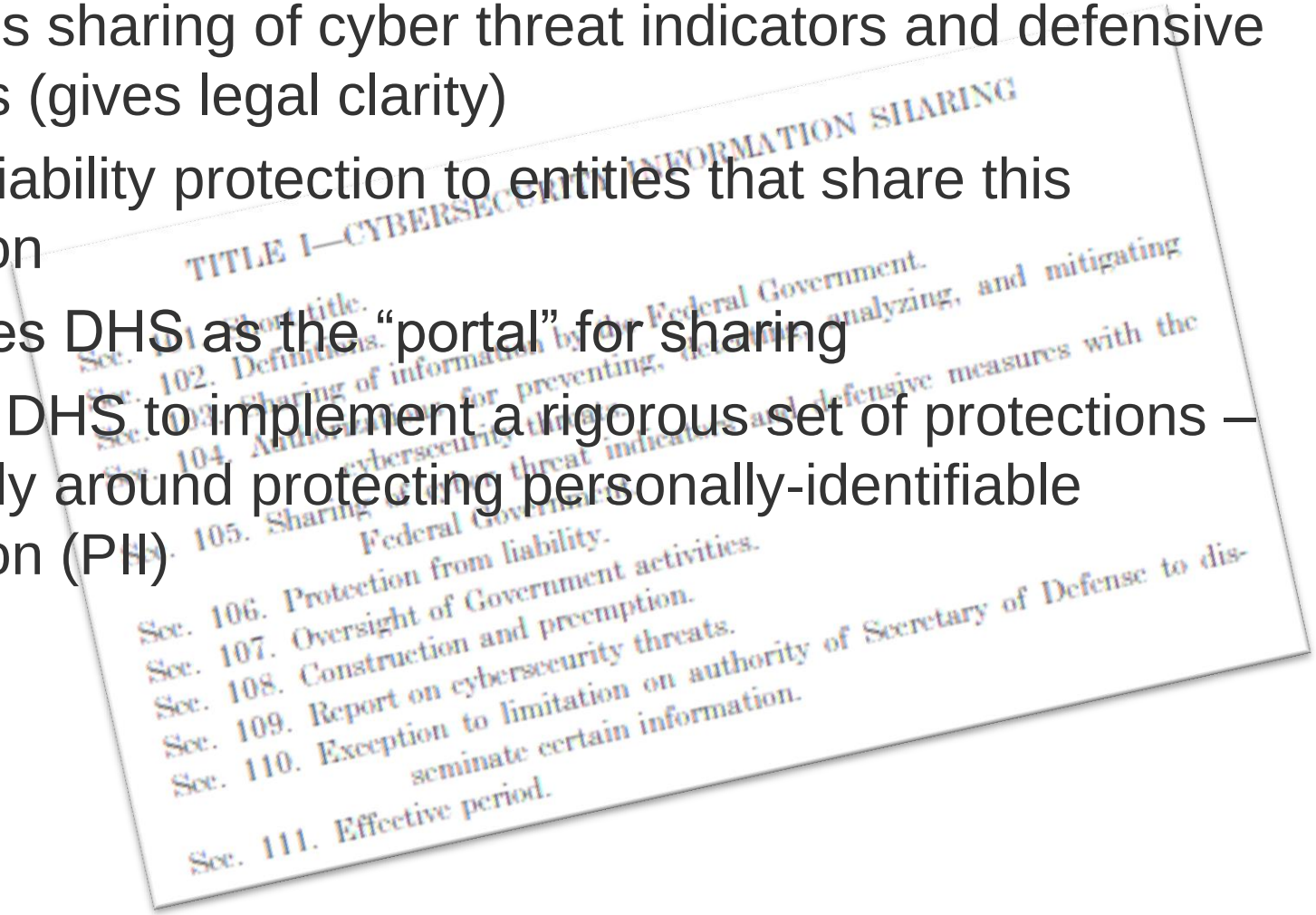
- You already know you *need* to share cyber threat intelligence (CTI)
- You already know you *want* to share CTI
- You want to benefit from the lessons learned by others

DHS Automated Indicator Sharing (AIS) Initiative

- Automated, near real-time indicator sharing ecosystem built on STIX/TAXII
- Designed to foster widespread sharing of CTI – specifically indicators
- Launched in 2014
- Updated as a result of the Cybersecurity Information Sharing Act of 2015 (CISA)

CISA Highlights

- Authorizes sharing of cyber threat indicators and defensive measures (gives legal clarity)
- Extends liability protection to entities that share this information
- Designates DHS as the "portal" for sharing
- Requires DHS to implement a rigorous set of protections – specifically around protecting personally-identifiable information (PII)


TITLE I—CYBERSECURITY INFORMATION SHARING

Sec. 102. Definitions.

Sec. 104.

Federal Government

Sec. 105. Sharing

Sec. 106. Protection from liability.

Sec. 107. Oversight of Government activities.

Sec. 108. Construction and preemption.

Sec. 109. Report on cybersecurity threats.

Sec. 110. Exception to limitation on authority of Secretary of Defense to disseminate certain information.

Sec. 111. Effective period.

Protecting Privacy and Civil Liberties

DHS has taken careful measures to ensure appropriate privacy and civil liberties protections are fully implemented in AIS and are regularly tested. The Department has published a Privacy Impact Assessment of AIS.

To ensure that personally identifiable information (PII) is protected, AIS has processes which:

- Perform automated analyses and technical mitigations to delete PII that is not directly related to a cyber threat;
- Incorporate elements of human review on select fields of certain indicators to ensure that automated processes are functioning appropriately;
- Minimize the amount of data included in a cyber threat indicator to information that is directly related to a cyber threat;
- Retain only information needed to address cyber threats; and
- Ensure any information collected is used only for network defense or limited law enforcement purposes

So What Did We Learn?

- Everything depends on trust
- The technical stuff is important but must serve the legal/policy-based goals
- Designing and documenting scalable and repeatable processes is essential
- Metrics, metrics, metrics

The Legal Front…

- Engage counsel early in the process
- Don't pre-judge what are “legal issues” – explain the whole process
- Be clear on what you are sharing, who you are sharing with and the purpose of the sharing
- Be on the lookout for intellectual property concerns
- Craft agreements that set out general principles and guidelines where possible (avoid excessive specificity)

The Policy Front…

- Some key questions:
  - Who “owns” the data you want to share?
  - Who decides what to share and who to share it with?
  - What do you want recipients of the data to be able to do with it – what restrictions apply?
  - What about anonymization?
  - Are there restrictions on what data you can/will accept from others?

The Technical Front…

- Need to implement according to legal and policy decisions
- Build on top of open standards
- Public Key Infrastructure (PKI) will be harder than you think
- Your sharing infrastructure will be a target – build security in from the beginning and at every layer of the stack (you will spend more on security than you expected to)
- Engineer to collect/generate metrics from the beginning
- But be careful about logging and how it might run afoul of policy
- Think ahead about how the system will be audited

Connecting to AIS

AIS is available for free to all private sector entities; federal departments and agencies; state, local, tribal, and territorial governments; information sharing and analysis centers (ISACs) and information sharing and analysis organizations (ISAOs); and foreign partners and companies.

Steps:

- Agree to a short Terms of Use.
- Set up a TAXII client: organizations that do not already have a TAXII capability can use the specification documentation to build their own, use the open-source DHS TAXII client available on GitHub or purchase a commercial capability.
- Technical connectivity activities: purchase a PKI certificate from a commercial provider, provide your IP address to DHS, and sign an Interconnection Security Agreement.
- Connect directly to the DHS-managed system. You can also share indicators with DHS through a participating ISAC or ISAO.

For More Information…

www.us-cert.gov/ais

Homeland Security