Essential for Cybersecurity and Privacy:
Wyden Amendment No. 2621 is the Best Path Forward
Strengthens the Requirement for Companies to Remove Personal Information

"In 20 years of doing cybersecurity...I have never seen a package of threat intelligence that's actionable that also includes personally identifiable information." -**Kevin Mandia, CEO of Mandiant**, testifying on cybersecurity information sharing legislation before the House Permanent Select Committee on Intelligence (February 14, 2013).

"Private information about individual users is often a detriment in developing threat signatures...Any bill that allows for and results in significant sharing of personal information could decrease the signal to noise ratio and make IoCs less actionable." -Letter on information sharing legislation from **77 leading cybersecurity experts** (April 16, 2015).

Unnecessary sharing and dissemination of PII "would fail to mitigate and in fact would contribute to the compromise of personally identifiable information by spreading it further." -**Alejandro Mayorkas, DHS Deputy Secretary**, letter to Sen. Franken (July 31, 2015).

The Senate Must Strengthen the Requirement for Companies to Remove PII

The most important improvement the Senate can make to CISA during the amendment and debate process it to enhance the front-end protections for communications content and personally identifiable information (PII) by strengthening the requirement to remove that sensitive and unnecessary information. Strengthening this requirement would reduce all other privacy and civil liberties concerns, since there would be less PII to be mishandled or misused by the government or by companies.

Because of how broadly CISA defines the term "cyber threat indicator" is defined, the information that is shared could include a tremendous amount of unnecessary personal information. A chart outlining the some of the types of "cyber threat indicators" that could be shared which could have the most personal information, and what that information could reveal, is available here and is available at the end of this document.

There are two amendments that address this important issue - the Wyden amendment (No. 2621) and the Heller amendment (No. 2548). OTI strongly supports the Wyden amendment because it will significantly enhance both cybersecurity and privacy. OTI is neutral on the Heller amendment because, while it would be an improvement upon the status quo, that improvement would be marginal and incomplete.

Why Removal of PII is Important for Cybersecurity and for Privacy

As is evident from the above quotes from leading cybersecurity experts, PII is generally not useful information for preventing or defending against cyber threats. In fact, when companies share more PII, cyber threat indicators will become less useful and the cybersecurity threat will increase. First, sharing unnecessary PII makes protecting against cyber threats harder because it makes actionable information less obvious, since security experts will have to sift through those excess data to identify the threat. Second, the more widely PII is distributed, the more those sensitive data - and the companies and government entities that hold it - will be targeted by malicious actors who seek to improperly access and use that information.

FOR MORE INFORMATION, CONTACT ROBYN GREENE, POLICY COUNSEL AT
NEW AMERICA'S OPEN TECHNOLOGY INSTITUTE: greene@opentechinstitute.org.

Why CISA's Current Requirement to Remove PII is Dangerously Weak:

CISA requires only that companies review cyber threat indicators and remove personal or identifiable information if they know at the time of sharing that it is not directly related to the threat. This is problematic in three ways:

1. There is no standard established for what would constitute a sufficient review of the information to identify PII, so companies could engage in cursory reviews that would not be sufficient to identify the majority of the PII that might be improperly or unnecessarily shared, and then share that information nonetheless.

2. By requiring only that PII be removed if the company *knows* at the time of sharing that it is not directly related to the cyber threat, CISA allows most - if not all - PII to be shared. This is because a company can default to leaving all PII in indicators that it shares, asserting that it does not have complete situational awareness of all cyber threats and thus does not "know" if PII is not directly related to one.

3. While in rare instances there may be some PII that is helpful in identifying or protecting against a cyber threat, most PII is unnecessary. By allowing PII to be shared so long as it is directly related to a threat, CISA may allow vast amounts of unnecessary personal information to be shared, including victim information.

OTI Supports Wyden Amendment No. 2621:

Senator Wyden's amendment would improve cybersecurity and better protect privacy by reducing the amount of unnecessary and inactionable PII that could be shared, and increasing how useful "cyber threat indicators" would be. This amendment effectively addresses all three concerns with how CISA's current requirement to remove PII is drafted.

- **Effective Protection for PII:** This amendment would allow only actionable or useful PII to be shared since it would only permit PII to be shared if it is "necessary to describe or identify a cybersecurity threat."

- **Reasonable and Flexible Efficacy Standard for Companies:** This amendment requires that companies review cyber threat indicators to identify and remove unnecessary PII "to the extent feasible." This is a good standard. It does not call for perfection, but rather is flexible, asking companies to protect their users' information by removing PII to the degree possible given their resources and capabilities. Thus, under this standard, a major tech company would be expected to be better able to identify and remove unnecessary PII than a small business or a start-up company.

OTI is Neutral on Heller Amendment No. 2548:

Senator Heller's amendment would make a small improvement over the status quo. Its positive impact on cybersecurity and privacy would not be nearly as significant as that of the Wyden amendment.

- **Marginally Better Protection for PII:** The Heller amendment requires the government to remove PII if, at the time of sharing, they "reasonably believe" that PII is not directly related to a cyber threat. This addresses the concern that if companies to unnecessarily leave PII in cyber threat indicators when sharing it, some of that PII will be removed before the cyber threat indicators are further shared with the government. However, it does not raise the standard to ensure that companies will remove unnecessary PII, and allows them to default to sharing that PII unless they *know* that it is not directly related to the threat.

- **No Efficacy Standard:** The Heller amendment does not establish a standard for how effective the government's processes for identifying and removing PII must be. Thus, the government could engage in a mere cursory review to identify and remove PII before sharing the information.

A chart analyzing CISA amendments is available at http://tinyurl.com/qg6ntcp.

FOR MORE INFORMATION, CONTACT ROBYN GREENE, POLICY COUNSEL AT
NEW AMERICA'S OPEN TECHNOLOGY INSTITUTE: greene@opentechinstitute.org.

Table of Personally Identifiable Information (PII) in Likely "Cyber Threat Indicators"

Cyber Threat Indicator	Included Personally Identifiable Information (PII)	What the PII Could Enable
Network Captures (also includes the remaining categories)	Internet Protocol (IP) Address	• Estimating the user's location • Identifying the user's online activity, including web browsing behavior o "These bits of individuals' online history may reveal their political inclinations, state of health, sexuality, religious sentiments and a range of other personal characteristics, preoccupations and individual interests"[i]

	Media Access Control (MAC) Address[ii]	• Identifying the user's physical movements
		  o Example: retail stores track shoppers using their MAC addresses
		• Identifying the user's online activity
		  o Example: hotspots record user MAC addresses

	Hostname[iii]	• Identifying the user's online activity o By default, major operating systems include an individual user's name in the computer hostname
Webserver Logs	Browser User-Agent String[iv]	• Identifying the user's online activity o User-Agent strings contribute to unique and trackable browser "fingerprints"[v]

	Cookies[vi]	• Identifying the user's online activity
		  o Cookies can include an individual user's name or username, location, gender, interests, and more
		• Accessing the user's online accounts without their permission
		  o Example: "session cookie stealing" attacks

	Requests and Responses	• Identifying the user's online activity
		  o Example: requested URLs often include a user's name or username
		  o Example: response HTML often includes a user's name or username

Emails[vii]	Headers	• Identifying the user's online activity • Identifying the user's contacts Drawing inferences about the user's behavior based on email time and length patterns
	Subject Line	• Understanding the substance of the user's communications
	Content	• Reading the substance of the user's communications
Documents (e.g. DOC and PDF), Media Files (e.g. images and video)[viii]	Metadata	• Identifying the authors and editors of the content • Associating particular revisions and saves with specific individuals, locations, devices, and device configurations • Learning the locations of related files • Learning who has viewed the file and when
	Content	• Viewing the substance of the document or media
Data Backup (Full, Differential, Incremental, and Delta [a.k.a. Database Dump])[ix]	Contents of database	Contents and metadata associated with every file/item in database, and could include, but is not limited to, all of the information contained in users accounts, or Word, PDF, and image and video files

[i] Tech. Analysis Branch, Office of the Privacy Comm'n of Canada, *What an IP Address Can Reveal About You* (2013), https://www.priv.gc.ca/information/research-recherche/2013/ip_201305_e.asp.

[ii] Definition of: MAC Address, Encyclopedia, PCMag, http://www.pcmag.com/encyclopedia/term/46422/mac-address (*last visited* Oct. 6, 2014); *see also* Simon Sharwood, *Snowden: Canadian spooks used free airport WiFi to track travellers*, The Register, Jan. 31, 2014, http://www.theregister.co.uk/2014/01/31/snowden_canadian_spooks_used_free_airport_wifi_to_track_travellers/.

[iii] Definition of: Hostname, Encyclopedia, PCMag, http://www.pcmag.com/encyclopedia/term/44378/hostname (*last visited* Oct. 6, 2014).

[iv] Peter Eckersley, *A Primer on Information Theory and Privacy*, Electronic Frontier Found., Jan. 26, 2010, https://www.eff.org/deeplinks/2010/01/primer-information-theory-and-privacy.

[v] Peter Eckersley, *Browser Versions Carry 10.5 Bits of Identifying Information on Average*, Electronic Frontier Found., Jan. 27, 2010, https://www.eff.org/deeplinks/2010/01/tracking-by-user-agent.

[vi] Definition of: Cookie, Encyclopedia, PCMag, http://www.pcmag.com/encyclopedia/term/40334/cookie (*last visited* Oct. 6, 2014).

[vii] Definition of: E-mail Header, Encyclopedia, PCMag, http://www.pcmag.com/encyclopedia/term/42243/e-mail-header (*last visited* Oct. 6, 2014); *see also* Larry Pesce, *Document Metadata: The Silent Killer…*, SANS Inst. (March 2008) http://www.sans.org/reading-room/whitepapers/privacy/document-metadata-silent-killer-32974.

[viii] Id.

[ix] Definition of: backup types, PCMag, http://www.pcmag.com/encyclopedia/term/38377/backup-types (*last visited* Oct. 6, 2014).