Critical for Cybersecurity and Privacy:
Franken Amendment No. 2612
Clarifies Definitions of Cybersecurity Threat and Cyber Threat Indicator

Why CISA's Current Definition for Cybersecurity Threat is Vague and Problematic:

CISA's definition for cybersecurity threat is the lynchpin for all of the authorities it creates. Entities may monitor their systems, sharing cyber threat indicators, and deploy defensive measures, in order to protect against a cybersecurity threat. However, CISA's definition of cybersecurity threat includes any *perceived* threat, regardless of whether the action or event would be reasonably likely to cause harm. This definition is so broad that CISA could lead to significant over-sharing, which would undermine security objectives by forcing responders to sift through large quantities of unnecessary information, such as information concerning false positives.

For example, an online banking customer who mistypes their password too many times and gets locked out of their account may initially be perceived as a threat by their bank even though they would not harm the bank or other networks. Nonetheless, under CISA's definition of "cybersecurity threat", the bank would be authorized to share information about that incident with the government or with other private entities, including the customer's personally identifiable information (PII), since it is directly related to that incident. Thus, CISA's broad definition of "cybersecurity threat" and the resulting excessive sharing of useless information could significantly undermine its effectiveness because it could slow down or distract security experts as they try to identify and respond to legitimate threats.

Franken Amendment No. 2612 Clarifies the Definition for Cybersecurity Threat:

Franken's amendment solves this problem by clarifying the definition of cybersecurity threat by establishing that an event or incident constitutes a threat - and triggers CISA's authorizations - only if it is "reasonably likely to result in" harm. This is a better standard than the status quo because it creates flexibility for companies while encouraging efficient sharing: Entities do not need to be *certain* that an incident or event is an attack before sharing information, but they must engage in an analysis to determine that a threat is legitimate, and not a false positive.

Why CISA's Definition of Cyber Threat Indicator is Vague and Problematic:

CISA's definition for cyber threat indicator includes some vague categories related to potential harms and "other attributes" that could lead to companies sharing unnecessary or inactionable content or PII.

Actual or Potential Harm - CISA authorizes companies to share information as cyber threat indicators that is "necessary to describe or identify...actual or potential harm caused by an incident." It is reasonable to authorize sharing pertaining to harms such as information or resources that are targeted, but it is unclear what information would be shared under an authorization to share information about "potential" harms. This could include unnecessary content or PII.

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

Information Necessary to Describe or Identify Any Other Attribute of a Threat - CISA authorizes companies to share any information that is "necessary to describe or identify...any other attribute of a cybersecurity threat, if disclosure of *such attribute* is not otherwise prohibited by law" (emphasis added). This would create a catch-all category in the definition for cyber threat indicators that allows for sharing information about an attribute. The definition allows for information about an attribute to be shared only if it is legal to share the underlying attribute, but there is no restriction on sharing of information that is necessary to describe or identify the attribute, even if that information is not necessary to identify or protect against the underlying threat. This discrepancy could allow for a significant amount of personal information to be shared because there is no requirement that the information describing the attribute be technical in nature.

For example, if an Internet Service Provider (ISP) uncovered a botnet, it might be necessary to share the IP addresses of the botnet victims as an attribute of the threat. But CISA's definition of cyber threat indicator could further authorize the ISP to share data such as the victims' names, billing addresses, or other sensitive information that the ISP claims is necessary to describe or identify the IP addresses, even though that information is unneeded to protect against the threat.

This type of identifying information may, at times, be useful for law enforcement, but it would not be necessary for enhancing cybersecurity. If law enforcement does determine that for an investigation it needs information that describes or identifies an attribute of a threat, such as the identifying information described in the above example, it should be required to follow traditional legal procedures for obtaining it, rather than being given it voluntarily under CISA.

Franken Amendment No. 2612 Clarifies the Definition for Cyber Threat Indicator:

This amendment would improve CISA's operational efficacy and its privacy protections by helping to ensure that the information that is shared is actionable threat data, and that it will include less unnecessary content and PII.

Actual or Potential Harm - The Franken amendment would preserve the authority for a company to share information that is necessary to describe or identify the harm caused by a threat, but would clarify that a company could not speculate as to potential harms and share information associated with those.

Information Necessary to Describe or Identify Any Other Attribute of a Threat - The Franken amendment would narrow the catch-all category in the definition for cyber threat indicator by clarifying that a company could only share information necessary to describe or identify an attribute of a threat if it is already legal to share that descriptive information. In the case of the example above, this amendment would clarify that the identifying information about the botnet victims could only be shared if there is a legal basis to share that information under some other law. Otherwise, it would still be protected under current privacy laws, and could only be shared pursuant to their requirements.

A chart outlining the types of PII that could be included in cyber threat indicators, and what that PII could reveal, is available at http://bit.ly/1Ku4mDF.

A chart analyzing all 22 potential CISA amendments is available at http://bit.ly/1Jd1WZ6.

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