

“Cyber Threat Indicator,” as defined by the Cybersecurity Information Sharing Act of 2015 (CISA)

CISA defines “cyber threat indicator” as “information that is necessary to describe or identify—

- (A) malicious reconnaissance, including anomalous patterns of communications that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat or security vulnerability;
- (B) a method of defeating a security control or exploitation of a security vulnerability;
- (C) a security vulnerability, including anomalous activity that appears to indicate the existence of a security vulnerability;
- (D) a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to unwittingly enable the defeat of a security control or exploitation of a security vulnerability;
- (E) malicious cyber command and control;
- (F) the actual or potential harm caused by an incident, including a description of the information exfiltrated as a result of a particular cybersecurity threat;
- (G) any other attribute of a cybersecurity threat, if disclosure of such attribute is not otherwise prohibited by law; or
- (H) any combination thereof.” (S.754 §102(7)).

“Defensive Measure,” as defined by CISA

CISA defines a “defensive measure” as “an action, device, procedure, signature, technique, or other measure applied to an information system or information that is stored on, processed by, or transiting an information system that detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability.” However, the bill excludes from the definition any measure that “destroys, renders unusable, provides unauthorized access to, or substantially harms an information system or data on an information system not belonging to the private entity operating the measure; or another entity or Federal entity that is authorized to provide consent and has provided consent to that private entity for operation of such measure.” (S.754 §102(7)).