U.S. Department of Homeland Security Automated Indicator Sharing
Terms of Use

These Terms of Use ("Terms") set forth the terms and conditions governing the use of Cyber Threat Indicators and Defensive Measures (defined below) and participation in the Department of Homeland Security ("DHS") Automated Indicator Sharing initiative ("AIS" defined below) for Cybersecurity Purposes.

1 DEFINITIONS

In these Terms, the following words and terms shall have the following meanings:

1.1 **"AIS"** means DHS's Automated Indicator Sharing initiative, which includes a technical system that enables automated, bi-directional, Cyber Threat Indicator and Defensive Measure sharing between AIS Participants and Federal Entities, through the NCCIC (defined below). AIS serves as the real-time process described in section 105(c) of the Cybersecurity Information Sharing Act of 2015 ("CISA") (Consolidated Appropriations Act, 2016, Pub. L. No. 114-113, Division N, Title I) for sharing Cyber Threat Indicators and Defensive Measures between AIS Participants and Federal Entities.

1.2 "**AIS Consumer**" means an AIS Participant that receives an Indicator or Defensive Measure through AIS under these Terms.

1.3 "**AIS Producer**" means an AIS Participant that discloses through AIS an Indicator or Defensive Measure under these Terms.

1.4 "**AIS Participant**" means a person, business, organization, other Non-Federal Entity (defined below), or other entity, foreign or domestic, that has accepted these Terms.

1.5 "**Authorized Activities**" means

(i) a Cybersecurity Purpose;

(ii) the purpose of identifying a cybersecurity threat, including the source of such cybersecurity threat; or a security vulnerability;

(iii) the purpose of responding to, or otherwise preventing or mitigating, a specific threat of death, a specific threat of serious bodily harm, or a specific threat of serious economic harm, including a terrorist act or a use of a weapon of mass destruction;

(iv) the purpose of responding to, investigating, prosecuting, or otherwise preventing or mitigating, a serious threat to a minor, including sexual exploitation and threats to physical safety; or

(v) the purpose of preventing, investigating, disrupting, or prosecuting an offense arising out of a threat described in clause (iii) or any of the offenses listed in (I) sections 1028 through 1030 of title 18, United States Code (relating to fraud and identity theft); (II) chapter 37 of such title (relating to espionage and censorship); and (III) chapter 90 of such title (relating to protection of trade secrets).

1.6 "**Cybersecurity Purpose**" means the purpose of protecting an information system (of an AIS Participant, a customer or member of an AIS Participant, or otherwise) or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability. "Cybersecurity Purpose" includes research that is conducted for a Cybersecurity Purpose.

1.7 "**Cybersecurity Threat**" means an action, not protected by the First Amendment to the Constitution of the United States, on or through an information system that may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system; but does not include any action that solely involves a violation of a consumer term of service or a consumer licensing agreement.

1.8 "**Cyber Threat Indicator**" (hereinafter "**Indicator**") means information that is necessary to describe or identify —

(i) 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;

(ii) a method of defeating a security control or exploitation of a security vulnerability;

(iii) a security vulnerability, including anomalous activity that appears to indicate the existence of a security vulnerability;

(iv) 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;

(v) malicious cyber command and control;

(vi) the actual or potential harm caused by an incident, including a description of the information exfiltrated as a result of a particular cybersecurity threat;

(vii) any other attribute of a cybersecurity threat, if disclosure of such attribute is not otherwise prohibited by law; or

(viii) any combination of (i)-(vii).

1.9 "**Defensive Measure**" means 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; but does not include a measure that destroys, renders unusable, provides unauthorized access to, or substantially harms an information system or information stored on, processed by, or transiting such information system not owned by (i) the private entity operating the measure; or (ii) another entity that is authorized to provide consent and has provided consent to that private entity for operation of such measure.

1.10 **"Federal Entity**" means a department or agency of the United States or any component of such department or agency.

1.11 "**Information Handling Levels**" means, for Indicators and Defensive Measure shared through AIS, the requirements for handling, use, and any further sharing that may be permitted. The Information Handling Levels shall be described by the NCCIC and incorporated into AIS, including with updates from time to time, with reasonable notice by the NCCIC made on its website, to be applied by each AIS Participant.

1.12 **"National Cybersecurity & Communications Integration Center"** (hereinafter **"NCCIC"**) is the Federal civilian interface for sharing cybersecurity information with federal and non-Federal entities as defined in statute at 6 U.S.C. § 148. The NCCIC shall not be considered an AIS Participant, Consumer, or Producer under these Terms.

1.13 **"Non-Federal Entity"** means any private entity, non-Federal government agency or department, or State, tribal, or local government (including a political subdivision, department, or component thereof); but does not include a foreign power as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

2 GENERAL RESPONSIBILITIES

2.1 DHS encourages AIS Participants to share Indicators and Defensive Measures broadly for a Cybersecurity Purpose. Each AIS Participant shall ensure that its use and disclosure of Indicators and Defensive Measures is in accordance with these Terms, applicable law, and any specified Information Handling Levels for Indicators and Defensive Measures. The disclosure of Indicators and Defensive Measures by an AIS Producer or the NCCIC shall in no way be construed to imply any kind of license for any intellectual property rights, patents, copyrights, trademarks or trade secrets, without limitation, other than the minimum use necessary for a Cybersecurity Purpose or as otherwise required by law.

2.2 AIS Participants shall strive to not disclose, advertise, or publicize, absent legal compulsion or other legal requirement, the identity of any other AIS Participant absent that AIS Participant's prior written consent.

2.3 Each AIS Participant and the NCCIC, to the maximum extent permitted by law, provide no representations or warranties regarding any Indicators or Defensive Measures provided through AIS or any other use of AIS.

2.4 An AIS Participant may allow others acting on its behalf to support its responsibilities under these Terms, provided those actors have agreed in writing to comply with these Terms.

3 AIS PRODUCERS

3.1 An AIS Producer may supply Indicators and Defensive Measures through AIS for a Cybersecurity Purpose. All submissions of Indicators and Defensive Measures through AIS by a Non-Federal Entity are deemed to be submitted under section 104(c) of CISA. An AIS Producer may or may not own the Indicator or Defensive Measure or be the source of the Indicator or Defensive Measure it produces.

3.2 An AIS Producer shall use reasonable efforts to ensure that any Indicator or Defensive Measure shared is accurate at the time that it is supplied. Further, the AIS Producer will associate any Indicators or Defensive Measures it produces with the appropriate Information Handling Level as defined by the NCCIC.

3.3 Each AIS Producer will use reasonable efforts to remove from any Indicators or Defensive Measures provided to the NCCIC any information not directly related to a cybersecurity threat that the AIS Producer knows at the time of sharing to be personal information of a specific individual or information that identifies a specific individual.

3.4 Each AIS Producer agrees that, in the event that it discloses Indicators or Defensive Measures by mistake, in error, or without their appropriate Information Handling Level (through mismarking or a failure to mark), it shall promptly notify the NCCIC and take all reasonable steps to mitigate, including sending a versioning update, as soon as it is able.

3.5 Each AIS Producer agrees that Federal Entities may disclose, use and retain Indicators and Defensive Measures provided to the NCCIC for an Authorized Activity.

4 AIS CONSUMERS

4.1 Each AIS Consumer shall use, handle, and disclose Indicators and Defensive Measures only for a Cybersecurity Purpose and in accordance with their associated Information Handling Level.

4.2 Each AIS Consumer agrees to use reasonable efforts to promptly apply any provided versioning updates.

4.3 If requested to do so by the NCCIC, an AIS Consumer shall provide a written description of the technical measures and/or protections it has implemented to ensure each Indicator and Defensive Measure is shared only in accordance with its associated Information Handling Level.

5 NCCIC RESPONSIBILITIES

5.1 The NCCIC shall provide notice on its website regarding the process by which an entity may become an AIS Participant. This process may be updated by the NCCIC from time to time, with reasonable prior notice on its website.

5.2 The NCCIC will anonymize the identity of the AIS Producer of any Indicator or Defensive Measure before sharing the Indicator or Defensive Measure among Federal Entities or with AIS Consumers, unless the AIS Producer consents affirmatively to disclosure of its identity.

6 TERMINATION

6.1 The NCCIC reserves the right to take any reasonable and lawful action it deems appropriate, including termination of an AIS Participant's ability to produce or consume Indicators and Defensive Measures for any reason, including the AIS Participant's response to an NCCIC inquiry, inadequate response, lack of a response, or continued violation of these Terms.

6.2 An AIS Participant may terminate its participation in AIS with written notice to the NCCIC through an email sent to taxiiadmins@us-cert.gov.

6.3 All rights and obligations with respect to the disclosure and use of Indicators and Defensive Measures shall survive the termination of these Terms.

7 SIGNATURE

By signing below, you agree to these Terms as a duly authorized representative of your company, organization, or firm or in your individual capacity if you are not affiliated with a company, organization or firm.

SIGNED**:** _____

DATE: _____

NAME: _____

TITLE: _____

ORGANIZATION NAME: _____