AI Security Strategy - Sample Policy Language

The language listed below is not intended to be comprehensive but rather representative of policy elements needed to implement a new national AI security strategy.

https://aisecuritypolicy.org

Section Definitions

1) Artificial intelligence

The term artificial intelligence means a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environments. Artificial intelligence systems use machine and human-based inputs to—

(A)perceive real and virtual environments;(B)abstract such perceptions into models through analysis in an automated manner; and(C)use model inference to formulate options for information or action.

2) Artificial Intelligence Covered Providers

Within the context of this act, artificial intelligence covered providers refers to persons who may offer Artificial Intelligence in areas that are not related to military or intelligence use.

3) Artificial Intelligence Solution

A service offered by an Artificial Intelligence Covered Provider.

4) Artificial Intelligence Attack

An intentional malicious utilization of an Artificial Intelligence Solution to cause it to perform in an unplanned or undesirable manner.

Rules of construction

Nothing in this act shall be construed as—

(1)modifying any authority or responsibility, including any operational authority or responsibility of any head of a Federal department or agency, with respect to intelligence or the intelligence community, as those terms are defined in 50 U.S.C. 3003;(2)authorizing the Initiative, or anyone associated with its derivative efforts to approve, interfere with, direct or to conduct an intelligence activity, resource, or operation; or(3)authorizing the Initiative, or anyone associated with its derivative efforts to modify the classification of intelligence information.

Appointment and Administration

(a)Artificial Intelligence Regulatory Commission; establishment

There is established an independent regulatory commission to be known as the Artificial Intelligence Regulatory Commission.

(b)Composition; term of office; conflict of interest; expiration of terms

1) *The Board is composed of 5 members appointed by the President, by and with the advice and consent of the Senate. Not more than 3 members may be appointed from the same political party. At least 3 members shall be appointed on the basis of technical qualification, professional standing, and demonstrated knowledge in artificial intelligence, artificial intelligence security, machine learning or data privacy. Members of the Commission shall not engage in any other business, vocation, or employment while serving on the Commission.*

General Powers Of The Commision

The Commission is authorized and empowered—--

a) **National Artificial Intelligence Registry**

To select, collect, record required data by Artificial Intelligence Covered Providers prior to the introduction of new artificial intelligence solutions including 1) data needed to classify artificial intelligence solutions based on risk (b), 2) data related to

attestation of conformance with associated artificial intelligence security standards(c), 3) other data as determined by the commission to meet these objectives.

b) Artificial Intelligence Risk Management Standard

To collaboratively develop and promulgate an artificial intelligence risk management standard that classifies artificial intelligence solutions based on the degree of risk associated with potential artificial intelligence attacks or failures of the solutions to perform as designed.

c) Artificial Intelligence Risk Aligned Security Standard

To collaboratively develop, oversee, and enforce conformance with artificial intelligence security standards that are associated with particular risk classes as defined in (b).

d) **Conformance Audits**

To select and perform audits of artificial intelligence solutions that fall within risk classes associated with greater risks including 1) the accuracy of reporting by solution providers in the national artificial intelligence registry, 2) the accuracy of attestation of controls provided by vendors in relation to associated risk aligned security standards.

e) Investigations

To make investigations and collect and record information related to potential failures or attacks against artificial intelligence systems to ascertain if related security standards were being appropriately followed.

National Artificial Intelligence Registry

(a)In general

(1)The Artificial Intelligence Regulatory Commission shall, using the provisions of this section, require Artificial Intelligence Covered Providers to submit specified information into the National Artificial Intelligence Solution Registry.

Enforcement

(a)Civil Actions by the Commission

The Artificial Intelligence Security Regulatory Commission may bring a civil action in a district court of the United States against a person to enforce regulation prescribed or order issued under any of these sections. An action under this subsection may be brought in the judicial district in which the person does business or the violation occurred.