§ 18933. Software security and authentication

(a) Vulnerabilities in open source software

The Director shall assign severity metrics to identified vulnerabilities with open source software and produce voluntary guidance to assist the entities that maintain open source software repositories to discover and mitigate vulnerabilities.

(b) Artificial intelligence-enabled defenses

The Director shall carry out research and testing to improve the effectiveness of artificial intelligence-enabled cybersecurity, including by generating optimized data sets to train artificial intelligence defense systems and evaluating the performance of varying network architectures at strengthening network security.

(c) Authentication of Institute software

The Director shall ensure all software released by the Institute is digitally signed and maintained to enable stakeholders to verify its authenticity and integrity upon installation and execution.

(d) Assistance to Inspectors General

Subject to available funding, the Director shall provide technical assistance to improve the education and training of individual Federal agency Inspectors General and staff who are responsible for the annual independent evaluation they are required to perform of the information security program and practices of Federal agencies under section 3555 of title 44.

(e) Software supply chain security practices

(1) In general

The Director shall, in coordination with industry, academia, and other Federal agencies, as appropriate, develop a set of security outcomes and practices, including security controls, control enhancements, supplemental guidance, or other supporting information to enable software developers and operators to identify, assess, and manage cybersecurity risks over the full lifecycle of software products.

(2) Outreach

The Director shall conduct outreach and coordination activities to share technical expertise with Federal agencies, relevant industry stakeholders, and standards development organizations, as appropriate, to encourage the voluntary adoption of the software lifecycle security practices by Federal agencies and industry stakeholders.

(Pub. L. 117–167, div. B, title II, §10224, Aug. 9, 2022, 136 Stat. 1478.)

§ 18934. Biometrics research and testing

(a) In general

The Secretary, acting through the Director, shall establish a program to support measurement research to inform the development of best practices, benchmarks, methodologies, procedures, and voluntary, consensus-based technical standards for biometric identification systems, including facial recognition systems, to assess and improve the performance of such systems. In carrying out such program, the Director may—

(1) conduct measurement research to support efforts to improve the performance of biometric identification systems, including in areas related to conformity assessment, image quality and interoperability, contactless biometric capture technologies, and human-in-the-loop biometric identification systems and processes;

(2) convene and engage with relevant stakeholders to establish common definitions and characterizations for biometric identification systems, which may include accuracy, fairness, bias, privacy, consent, and other properties, taking into account definitions in relevant international technical standards and other publications;

(3) carry out measurement research and testing on a range of biometric modalities, such as fingerprints, voice, iris, face, vein, behavioral biometrics, genetics, multimodal biometrics, and emerging applications of biometric identification technology;

(4) study the use of privacy-enhancing technologies and other technical protective controls to facilitate access, as appropriate, to public data sets for biometric research;

(5) conduct outreach and coordination to share technical expertise with relevant industry and nonindustry stakeholders and standards development organizations to assist such entities in the development of best practices and voluntary technical standards; and

(6) develop such standard reference artifacts as the Director determines is necessary to further the development of such voluntary technical standards.

(b) Biometrics test program

(1) In general

The Secretary, acting through the Director, shall carry out a test program to provide biometrics vendors the opportunity to test biometric identification technologies across a range of modalities.

(2) Activities

In carrying out the program under this subsection, the Director shall—

(A) conduct research and regular testing to improve and benchmark the accuracy, efficacy, and bias of biometric identification technologies, which may include research and testing on demographic variations, capture devices, presentation attack detection, partially occluded or computer generated images, privacy and security designs and controls, template protection, de-identification, and comparison of algorithm, human, and combined algorithm-human recognition capability;

(B) develop an approach for testing software and cloud-based biometrics applications, including remote systems, in Institute test facilities;

(C) establish reference use cases for biometric identification technologies and performance criteria for assessing each use case, including accuracy, efficacy, and bias metrics;