§ 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;

(D) produce public-facing reports of the findings from such testing for a general audience;

(E) develop policies and procedures accounting for the legal and social implications of activities under this paragraph when working with a foreign entity of concern (as such term is defined in section 19221 of this title);

(F) establish procedures to prioritize testing of biometrics identification technologies developed by entities headquartered in the United States; and

(G) conduct such other activities as determined necessary by the Director.

(c) GAO report to Congress

Not later than 18 months after August 9, 2022, the Comptroller General of the United States shall submit a detailed report to Congress on the impact of biometric identification technologies on historically marginalized communities, including low-income communities and minority religious, racial, and ethnic groups. Such report should be made publicly available on an internet website.

(Pub. L. 117–167, div. B, title II, § 10226, Aug. 9, 2022, 136 Stat. 1479.)

§ 18935. Dissemination of resources for research institutions

(a) Dissemination of resources for research institutions

(1) In general

Not later than one year after August 9, 2022, the Director shall, using the authorities of the Director under subsections (c)(15) and (e)(1)(A)(ix) of section 272 of title 15, disseminate and make publicly available tailored resources to help qualifying institutions identify, assess, manage, and reduce their cybersecurity risk related to conducting research.

(2) Requirements

The Director shall ensure that the resources disseminated pursuant to paragraph (1)—

(A) are generally applicable and usable by a wide range of qualifying institutions;

(B) vary with the nature and size of the qualifying institutions, and the nature and sensitivity of the data collected or stored on the information systems or devices of the qualifying institutions;

(C) include elements that promote awareness of simple, basic controls, a workplace cybersecurity culture, and third-party stakeholder relationships, to assist qualifying institutions in mitigating common cybersecurity risks;

(D) include case studies, examples, and scenarios of practical application;

(E) are outcomes-based and can be implemented using a variety of technologies that are commercial and off-the-shelf; and

(F) to the extent practicable, are based on international technical standards.

(3) National cybersecurity awareness and education program

The Director shall ensure that the resources disseminated under paragraph (1) are consistent with the efforts of the Director under section 7443 of title 15.

(4) Updates

The Director shall review periodically and update the resources under paragraph (1) as the Director determines appropriate.

(5) Voluntary resources

The use of the resources disseminated under paragraph (1) shall be considered voluntary.

(b) Other Federal cybersecurity requirements

Nothing in this section may be construed to supersede, alter, or otherwise affect any cybersecurity requirements applicable to Federal agencies.

(c) Definitions

In this section:

(1) Qualifying institutions

The term ''qualifying institutions'' means institutions of higher education that are awarded in excess of $50,000,000 per year in total Federal research funding.

(2) Resources

The term ''resources'' means guidelines, tools, best practices, technical standards, methodologies, and other ways of providing information.

(Pub. L. 117–167, div. B, title II, § 10229, Aug. 9, 2022, 136 Stat. 1481.)

§ 18936. Neutron scattering

(a) Strategic plan for the Institute neutron reactor

The Director shall develop a strategic plan for the future of the NIST Center for Neutron Research after the current neutron reactor is decommissioned, including—

(1) a succession plan for the reactor, including a roadmap with timeline and milestones;

(2) conceptual design of a new reactor and accompanying facilities, as appropriate; and

(3) a plan to minimize disruptions to the user community during the transition.

(b) Coordination with the Department of Energy

The Secretary, acting through the Director, shall coordinate with the Secretary of Energy on issues related to Federal support for neutron science, including estimation of long-term needs for research using neutron sources, and planning efforts for future facilities to meet such needs.

(c) Report to Congress

Not later than 30 months after August 9, 2022, the Director shall submit to Congress the plan required under subsection (a), and shall notify Congress of any substantial updates to such plan in subsequent years.

(Pub. L. 117–167, div. B, title II, § 10231, Aug. 9, 2022, 136 Stat. 1483.)

§ 18937. Artificial intelligence

The Director shall continue to support the development of artificial intelligence and data science, and carry out the activities of the National Artificial Intelligence Initiative Act of 2020 authorized in division E of the National De-