(1) to clarify the applicability of international laws and norms to the use of information and communications technology (referred to in this subsection as ''ICT'');

(2) to reduce and limit the risk of escalation and retaliation in cyberspace, damage to critical infrastructure, and other malicious cyber activity that impairs the use and operation of critical infrastructure that provides services to the public;

(3) to cooperate with like-minded countries that share common values and cyberspace policies with the United States, including respect for human rights, democracy, and the rule of law, to advance such values and policies internationally;

(4) to encourage the responsible development of new, innovative technologies and ICT products that strengthen a secure internet architecture that is accessible to all;

(5) to secure and implement commitments on responsible country behavior in cyberspace, including commitments by countries—

(A) not to conduct, or knowingly support, cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors;

(B) to take all appropriate and reasonable efforts to keep their territories clear of intentionally wrongful acts using ICT in violation of international commitments;

(C) not to conduct or knowingly support ICT activity that intentionally damages or otherwise impairs the use and operation of critical infrastructure providing services to the public, in violation of international law;

(D) to take appropriate measures to protect the country's critical infrastructure from ICT threats;

(E) not to conduct or knowingly support malicious international activity that harms the information systems of authorized international emergency response teams (also known as ''computer emergency response teams'' or ''cybersecurity incident response teams'') of another country or authorize emergency response teams to engage in malicious international activity, in violation of international law;

(F) to respond to appropriate requests for assistance to mitigate malicious ICT activity emanating from their territory and aimed at the critical infrastructure of another country;

(G) not to restrict cross-border data flows or require local storage or processing of data; and

(H) to protect the exercise of human rights and fundamental freedoms on the internet, while recognizing that the human rights that people have offline also need to be protected online; and

(6) to advance, encourage, and support the development and adoption of internationally recognized technical standards and best practices.

(Pub. L. 117–263, div. I, title XCV, § 9501, Dec. 23, 2022, 136 Stat. 3897.)

Statutory Notes and Related Subsidiaries

SUPPORT OF POLICY IN UNITED NATIONS

Pub. L. 117–263, div. I, title XCV, § 9502(c), Dec. 23, 2022, 136 Stat. 3902, provided that: ''The Permanent Representative of the United States to the United Nations should use the voice, vote, and influence of the United States to oppose any measure that is inconsistent with the policy described in section 9501(a) [22 U.S.C. 10301(a)].''

§ 10302. International cyberspace and digital policy strategy

(a) Strategy required

Not later than 1 year after December 23, 2022, the President, acting through the Secretary, and in coordination with the heads of other relevant Federal departments and agencies, shall develop an international cyberspace and digital policy strategy.

(b) Elements

The strategy required under subsection (a) shall include—

(1) a review of actions and activities undertaken to support the policy described in section 10301(a) of this title;

(2) a plan of action to guide the diplomacy of the Department with regard to foreign countries, including—

(A) conducting bilateral and multilateral activities—

(i) to develop and support the implementation of norms of responsible country behavior in cyberspace consistent with the commitments listed in section 10301(b)(5) of this title;

(ii) to reduce the frequency and severity of cyberattacks on United States individuals, businesses, governmental agencies, and other organizations;

(iii) to reduce cybersecurity risks to United States and allied critical infrastructure;

(iv) to improve allies' and partners' collaboration with the United States on cybersecurity issues, including information sharing, regulatory coordination and improvement, and joint investigatory and law enforcement operations related to cybercrime; and

(v) to share best practices and advance proposals to strengthen civilian and private sector resiliency to threats and access to opportunities in cyberspace; and

(B) reviewing the status of existing efforts in relevant multilateral fora, as appropriate, to obtain commitments on international norms regarding cyberspace;

(3) a review of alternative concepts for international norms regarding cyberspace offered by foreign countries;

(4) a detailed description, in consultation with the Office of the National Cyber Director and relevant Federal agencies, of new and evolving threats regarding cyberspace from foreign adversaries, state-sponsored actors, and non-state actors to—

(A) United States national security;

(B) the Federal and private sector cyberspace infrastructure of the United States;

(C) intellectual property in the United States; and

(D) the privacy and security of citizens of the United States;

(5) a review of the policy tools available to the President to deter and de-escalate tensions with foreign countries, state-sponsored actors, and private actors regarding—

(A) threats in cyberspace;

(B) the degree to which such tools have been used; and

(C) whether such tools have been effective deterrents;

(6) a review of resources required to conduct activities to build responsible norms of international cyber behavior;

(7) a review, in coordination with the Office of the National Cyber Director and the Office of Management and Budget, to determine whether the budgetary resources, technical expertise, legal authorities, and personnel available to the Department are adequate to achieve the actions and activities undertaken by the Department to support the policy described in section 10301(a) of this title;

(8) a review to determine whether the Department is properly organized and coordinated with other Federal agencies to achieve the objectives described in section 10301(b) of this title; and

(9) a plan of action, developed in coordination with the Department of Defense and in consultation with other relevant Federal departments and agencies as the President may direct, with respect to the inclusion of cyber issues in mutual defense agreements.

(c) Form of strategy

(1) Public availability

The strategy required under subsection (a) shall be available to the public in unclassified form, including through publication in the Federal Register.

(2) Classified annex

The strategy required under subsection (a) may include a classified annex.

(d) Briefing

Not later than 30 days after the completion of the strategy required under subsection (a), the Secretary shall brief the Committee on Foreign Relations of the Senate, the Select Committee on Intelligence of the Senate, the Committee on Armed Services of the Senate, the Committee on Foreign Affairs of the House of Representatives, the Permanent Select Committee on Intelligence of the House of Representatives, and the Committee on Armed Services of the House of Representatives regarding the strategy, including any material contained in a classified annex.

(e) Updates

The strategy required under subsection (a) shall be updated—

(1) not later than 90 days after any material change to United States policy described in such strategy; and

(2) not later than 1 year after the inauguration of each new President.

(Pub. L. 117–263, div. I, title XCV, § 9503, Dec. 23, 2022, 136 Stat. 3902.)

Statutory Notes and Related Subsidiaries

DEFINITIONS

''Secretary'' and ''Department'' as used in this section mean the Secretary and Department of State, unless otherwise specified, see section 9002 of Pub. L. 117–263, set out as a note under section 2651 of this title.

§ 10303. Cybersecurity recruitment and retention

(a) Sense of Congress

It is the sense of Congress that improving computer programming language proficiency will improve—

(1) the cybersecurity effectiveness of the Department; and

(2) the ability of foreign service officers to engage with foreign audiences on cybersecurity matters.

(b) Technology talent acquisition

(1) Establishment

The Secretary shall establish positions within the Bureau of Global Talent Management that are solely dedicated to the recruitment and retention of Department personnel with backgrounds in cybersecurity, engineering, data science, application development, artificial intelligence, critical and emerging technology, and technology and digital policy.

(2) Goals

The goals of the positions described in paragraph (1) shall be—

(A) to fulfill the critical need of the Department to recruit and retain employees for cybersecurity, digital, and technology positions;

(B) to actively recruit relevant candidates from academic institutions, the private sector, and related industries;

(C) to work with the Office of Personnel Management and the United States Digital Service to develop and implement best strategies for recruiting and retaining technology talent; and

(D) to inform and train supervisors at the Department on the use of the authorities listed in subsection (c)(1).

(3) Implementation plan

Not later than 180 days after December 23, 2022, the Secretary shall submit a plan to the appropriate congressional committees that describes how the objectives and goals set forth in paragraphs (1) and (2) will be implemented.

(4) Authorization of appropriations

There is authorized to be appropriated $750,000 for each of the fiscal years 2023 through 2027 to carry out this subsection.

(c) Annual report on hiring authorities

Not later than 1 year after December 23, 2022, and annually thereafter for the following 5 years, the Secretary shall submit a report to the appropriate congressional committees that includes—

(1) a list of the hiring authorities available to the Department to recruit and retain personnel with backgrounds in cybersecurity, engineering, data science, application development, artificial intelligence, critical and