(2) the Committee on Foreign Affairs, the Committee on Armed Services, and the Committee on Appropriations of the House of Representatives.

(Pub. L. 117–263, div. E, title LV, § 5577, Dec. 23, 2022, 136 Stat. 3370.)

SUBCHAPTER IV—EFFORTS AGAINST HUMAN RIGHTS ABUSES

§ 10251. Authorization to provide technical assistance for efforts against human rights abuses

(a) In general

The Secretary of State is authorized to provide assistance to support appropriate civilian or international entities that—

(1) identify suspected perpetrators of war crimes, crimes against humanity, and genocide in Burma;

(2) collect, document, and protect evidence of crimes in Burma and preserving the chain of custody for such evidence;

(3) conduct criminal investigations of such crimes; and

(4) support investigations related to Burma conducted by other countries, and by entities mandated by the United Nations, such as the Independent Investigative Mechanism for Myanmar.

(b) Authorization for transitional justice mechanisms

The Secretary of State, taking into account any relevant findings in the report submitted under section 5941,[1] is authorized to provide support for the establishment and operation of transitional justice mechanisms, including a hybrid tribunal, to prosecute individuals suspected of committing war crimes, crimes against humanity, or genocide in Burma.

(Pub. L. 117–263, div. E, title LV, § 5578, Dec. 23, 2022, 136 Stat. 3370.)

Editorial Notes

REFERENCES IN TEXT

Section 5941, referred to in subsec. (b), is unidentifiable in the original. Although Pub. L. 117–263 does contain a section 5941, that section is outside the BURMA Act of 2022, which comprises this chapter, and relates to the submission of a report by the Secretary of Agriculture on wholesale produce markets. Prior versions of the Act included a section requiring a report containing a study of the feasibility and desirability of a transitional justice mechanism for Burma, but that section did not appear in the version of the Act enacted by Pub. L. 117–263.

SUBCHAPTER V—SANCTIONS EXCEPTION RELATING TO IMPORTATION OF GOODS

§ 10261. Sanctions exception relating to importation of goods

(a) In general

The authorities and requirements to impose sanctions under this chapter shall not include the authority or requirement to impose sanctions on the importation of goods.

(b) Good defined

In this section, the term ''good'' means any article, natural or man-made substance, material, supply, or manufactured product, including inspection and test equipment, and excluding technical data.

(Pub. L. 117–263, div. E, title LV, § 5579, Dec. 23, 2022, 136 Stat. 3370.)

CHAPTER 110—INFORMATION SECURITY AND CYBER DIPLOMACY

Sec.

§ 10301. United States international cyberspace policy

(a) In general

It is the policy of the United States—

(1) to work internationally to promote an open, interoperable, reliable, and secure internet governed by the multi-stakeholder model, which—

(A) promotes democracy, the rule of law, and human rights, including freedom of expression;

(B) supports the ability to innovate, communicate, and promote economic prosperity; and

(C) is designed to protect privacy and guard against deception, malign influence, incitement to violence, harassment and abuse, fraud, and theft;

(2) to encourage and aid United States allies and partners in improving their own technological capabilities and resiliency to pursue, defend, and protect shared interests and values, free from coercion and external pressure; and

(3) in furtherance of the efforts described in paragraphs (1) and (2)—

(A) to provide incentives to the private sector to accelerate the development of the technologies referred to in such paragraphs;

(B) to modernize and harmonize with allies and partners export controls and investment screening regimes and associated policies and regulations; and

(C) to enhance United States leadership in technical standards-setting bodies and avenues for developing norms regarding the use of digital tools.

(b) Implementation

In implementing the policy described in subsection (a), the President, in consultation with outside actors, as appropriate, including private sector companies, nongovernmental organizations, security researchers, and other relevant stakeholders, in the conduct of bilateral and multilateral relations, shall strive—

[1] See References in Text note below.

(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;