''(iv) A description of technologies currently available to reduce the susceptibility and vulnerability of civilian aircraft to man-portable air-defense systems, including an assessment of the feasibility of using aircraft-based anti-missile systems to protect United States passenger jets.

''(v) Recommendations for the most effective policy measures that can be taken to reduce and mitigate the threat posed to United States citizens and citizens of allies of the United States from man-portable air-defense systems that were in Libya as of March 19, 2011.

''(vi) Such recommendations for legislative or administrative action as the President considers appropriate to implement the strategy required by paragraph (1).

''(C) FORM.—The report required by this paragraph shall be submitted in unclassified form, but may include a classified annex.

''(d) APPROPRIATE COMMITTEES OF CONGRESS DEFINED.—In this section, the term 'appropriate committees of Congress' means—

''(1) the Committee on Armed Services, the Committee on Foreign Relations, and the Select Committee on Intelligence of the Senate; and

''(2) the Committee on Armed Services, the Committee on Foreign Affairs, and the Permanent Select Committee on Intelligence of the House of Representatives.''

[Memorandum of President of the United States, Apr. 20, 2012, 77 F.R. 28757, delegated the reporting functions conferred upon the President by section 1235(c) of Pub. L. 112–81, set out above, to the Secretary of State.]

PART X—CYBERSPACE, DIGITAL CONNECTIVITY, AND RELATED TECHNOLOGIES (CDT) FUND

§ 2349cc. Findings

Congress makes the following findings:

(1) Increasingly digitized and interconnected social, political, and economic systems have introduced new vulnerabilities for malicious actors to exploit, which threatens economic and national security.

(2) The rapid development, deployment, and integration of information and communication technologies into all aspects of modern life bring mounting risks of accidents and malicious activity involving such technologies, and their potential consequences.

(3) Because information and communication technologies are globally manufactured, traded, and networked, the economic and national security of the United State[1] depends greatly on cybersecurity practices of other actors, including other countries.

(4) United States assistance to countries and international organizations to bolster civilian capacity to address national cybersecurity and deterrence in cyberspace can help—

(A) reduce vulnerability in the information and communication technologies ecosystem; and

(B) advance national and economic security objectives.

(Pub. L. 87–195, pt. II, § 591, as added Pub. L. 118–31, div. F, title LXIII, § 6307, Dec. 22, 2023, 137 Stat. 990.)

[1] So in original. Probably should be ''States''.

§ 2349cc–1. Authorization of assistance and funding for cyberspace, digital connectivity, and related technologies (CDT) capacity building activities

(a) Authorization

The Secretary of State is authorized to provide assistance to foreign governments and organizations, including national, regional, and international institutions, on such terms and conditions as the Secretary may determine, in order to—

(1) advance a secure and stable cyberspace;

(2) protect and expand trusted digital ecosystems and connectivity;

(3) build the cybersecurity capacity of partner countries and organizations; and

(4) ensure that the development of standards and the deployment and use of technology supports and reinforces human rights and democratic values, including through the Digital Connectivity and Cybersecurity Partnership.

(b) Scope of uses

Assistance under this section may include programs to—

(1) advance the adoption and deployment of secure and trustworthy information and communications technology (ICT) infrastructure and services, including efforts to grow global markets for secure ICT goods and services and promote a more diverse and resilient ICT supply chain;

(2) provide technical and capacity building assistance to—

(A) promote policy and regulatory frameworks that create an enabling environment for digital connectivity and a vibrant digital economy;

(B) ensure technologies, including related new and emerging technologies, are developed, deployed, and used in ways that support and reinforce democratic values and human rights;

(C) promote innovation and competition; and

(D) support digital governance with the development of rights-respecting international norms and standards;

(3) help countries prepare for, defend against, and respond to malicious cyber activities, including through—

(A) the adoption of cybersecurity best practices;

(B) the development of national strategies to enhance cybersecurity;

(C) the deployment of cybersecurity tools and services to increase the security, strength, and resilience of networks and infrastructure;

(D) support for the development of cybersecurity watch, warning, response, and recovery capabilities, including through the development of cybersecurity incident response teams;

(E) support for collaboration with the Cybersecurity and Infrastructure Security Agency (CISA) and other relevant Federal agencies to enhance cybersecurity;

(F) programs to strengthen allied and partner governments' capacity to detect, investigate, deter, and prosecute cybercrimes;