(C) in subparagraph (C), by inserting ''or Native Hawaiian communities'' after ''tribal communities''; and

(D) in subparagraph (D)—

(i) by inserting ''or Native Hawaiian communities'' after ''Indian tribes''; and

(ii) by inserting ''or Native Hawaiian'' after ''against Indian'';

(2) in paragraph (2)—

(A) in subparagraph (A)(iii), by inserting ''or Native Hawaiian communities'' after ''Indian tribes''; and

(B) in subparagraph (B), by inserting ''or Native Hawaiian communities'' after ''Indian tribes''; and

(3) by adding at the end the following:

''(6) NATIVE HAWAIIAN DEFINED.—In this subsection, the term 'Native Hawaiian' has the meaning given that term in section 801 of the Native American Housing Assistance and Self-Determination Act of 1996 (25 U.S.C. 4221).''.

(b) TECHNICAL AND CONFORMING AMENDMENT.—Section 40002(a)(42) of the Violence Against Women Act of 1994 (34 U.S.C. 12291(a)(42)) is amended—

(1) in subparagraph (A)—

(A) by inserting ''or the Native Hawaiian community'' after ''Indian service providers''; and

(B) by inserting ''or Native Hawaiian'' after ''designed to assist Indian''; and

(2) in subparagraph (B), in clause (ii), by inserting ''or Native Hawaiian communities'' after ''tribal communities''.

SA 6312. Ms. SMITH submitted an amendment intended to be proposed to amendment SA 5499 submitted by Mr. REED (for himself and Mr. INHOFE) and intended to be proposed to the bill H.R. 7900, to authorize appropriations for fiscal year 2023 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. ___. CDFI BOND GUARANTEE PROGRAM.

(a) SHORT TITLE.—This section may be cited as the ''CDFI Bond Guarantee Program Improvement Act of 2022'',

(b) SENSE OF CONGRESS.—It is the sense of Congress that the authority to guarantee bonds under section 114A of the Community Development Banking and Financial Institutions Act of 1994 (12 U.S.C. 4713a) (in this section referred to as the ''CDFI Bond Guarantee Program'') provides community development financial institutions with a sustainable source of long-term capital and furthers the mission of the Community Development Financial Institutions Fund (established under section 104(a) of such Act (12 U.S.C. 4703(a)) to increase economic opportunity and promote community development investments for underserved populations and distressed communities in the United States.

(c) GUARANTEES FOR BONDS AND NOTES ISSUED FOR COMMUNITY OR ECONOMIC DEVELOPMENT PURPOSES.—Section 114A of the Community Development Banking and Financial Institutions Act of 1994 (12 U.S.C. 4713a) is amended—

(1) in subsection (c)(2), by striking '', multiplied by an amount equal to the outstanding principal balance of issued notes or bonds'';

(2) in subsection (e)(2)(B), by striking ''$100,000,000'' and inserting ''$25,000,000''; and

(3) in subsection (k), by striking ''September 30, 2014'' and inserting ''the date that is 4 years after the date of enactment of the CDFI Bond Guarantee Program Improvement Act of 2022''.

(d) REPORT ON THE CDFI BOND GUARANTEE PROGRAM.—Not later than 1 year after the date of enactment of this Act, and not later than 3 years after such date of enactment, the Secretary of the Treasury shall issue a report to the Committee on Banking, Housing, and Urban Affairs of the Senate and the Committee on Financial Services of the House of Representatives on the effectiveness of the CDFI Bond Guarantee Program.

SA 6313. Mr. MENENDEZ submitted an amendment intended to be proposed to amendment SA 5499 submitted by Mr. REED (for himself and Mr. INHOFE) and intended to be proposed to the bill H.R. 7900, to authorize appropriations for fiscal year 2023 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the end of title XII, add the following:

Subtitle G—Strengthening International Cybersecurity Engagement

SEC. 1281. FINDINGS.

Congress finds the following:

(1) The stated goal of the United States International Strategy for Cyberspace, launched on May 16, 2011, is to ''work internationally to promote an open, interoperable, secure, and reliable information and communications infrastructure that supports international trade and commerce, strengthens international security, and fosters free expression and innovation in which norms of responsible behavior guide states' actions, sustain partnerships, and support the rule of law in cyberspace.''.

(2) On April 11, 2017, the 2017 Group of 7 Declaration on Responsible State Behavior in Cyberspace—

(A) recognized ''the urgent necessity of increased international cooperation to promote security and stability in cyberspace'';

(B) expressed commitment to ''promoting a strategic framework for conflict prevention, cooperation and stability in cyberspace, consisting of the recognition of the applicability of existing international law to State behavior in cyberspace, the promotion of voluntary, non-binding norms of responsible State behavior during peacetime, and the development and the implementation of practical cyber confidence building measures (CBMs) between States''; and

(C) reaffirmed that ''the same rights that people have offline must also be protected online''.

(3) The 2018 National Cyber Strategy states that ''[t]he United States will strive to improve international cooperation in investigating malicious cyber activity, including developing solutions to potential barriers to gathering and sharing evidence'' and ''will promote a framework of responsible state behavior in cyberspace built upon international law, adherence to voluntary nonbinding norms of responsible state behavior that apply during peacetime, and the consideration of practical confidence building measures to reduce the risk of conflict stemming from malicious cyber activity''.

(4) In its May 28, 2021 consensus report, the United Nations Group of Governmental Experts on Advancing Responsible State Behavior in Cyberspace wrote that countries ''should cooperate in developing and applying measures to increase stability and security in the use of ICTs'' and ''respect and protect human rights and fundamental freedoms, both online and offline in accordance with their respective obligations''.

(5) Emerging technologies, such as artificial intelligence, biotechnology, and quantum computing—

(A) have profound implications for global cybersecurity;

(B) are deeply integrated with, and often dependent on, information and communication technologies;

(C) are exposed to cyber threats and may have cyber vulnerabilities that could cause significant harm, if exploited; and

(D) can be used both offensively and defensively in cyberspace.

SEC. 1282. SENSE OF CONGRESS.

It is the sense of Congress that—

(1) the United States and its allies and partners must cooperate to ensure the security and safety of information and communication technologies to ensure global peace and prosperity and protect democratic institutions, norms, and values;

(2) the United States should engage with adversary nations, as appropriate—

(A) to define responsible norms of behavior in cyberspace;

(B) to address nonstate cybersecurity threats; and

(C) to establish confidence-building measures that reduce the risk of unintended cyber conflict and escalation;

(3) effective international engagement across cyber issues and stakeholders requires strategic planning, focused leadership, dedicated resources and personnel, and continuous monitoring and evaluation;

(4) Federal agencies involved in international cybersecurity engagement—

(A) must ensure that the preconditions described in paragraph (3) are in place; and

(B) must work with each other to ensure that efforts are consistent, coordinated, and nonduplicative; and

(5) United States international cybersecurity engagement—

(A) must draw on the active involvement, expertise, and resources of the private sector and civil society; and

(B) United States international cybersecurity engagement must account for the cybersecurity implications of novel and emerging technologies.

SEC. 1283. STATEMENT OF POLICY.

It shall be the policy of the United States—

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

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

(B) respects individual privacy; and

(C) guards against deception, fraud, and theft;

(2) to take an active role in international and multi-stakeholder fora to strengthen existing norms of responsible behavior of cyberspace, including those set forth in the 2015 and 2021 consensus reports of the United Nations Group of Governmental Experts on Advancing Responsible State Behavior in Cyberspace;

(3) to incorporate, as appropriate, the interests, expertise, and resources of the private sector and civil society into international cybersecurity efforts;

(4) to help allies and partners boost their own cyber capabilities and resiliency in order to pursue, defend, and protect shared interests and values;

(5) to support, in collaboration with allies and partners, the innovation, development, and adoption of technologies and technical standards that—

(A) improve cybersecurity; and

(B) sustain a free, open, and secure internet; and

(6) to coordinate international cybersecurity engagement across the Federal Government to ensure that such efforts are consistent and nonduplicative.

SEC. 1284. REPORT ON UNITED STATES INTERNATIONAL CYBERSECURITY EFFORTS.

(a) DEFINED TERM.—In this section, the term ''national security strategy'' means the national security strategy of the United States required to be transmitted to Congress annually under section 108 of the National Security Act of 1947 (50 U.S.C. 3043).

(b) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, and every 3 years thereafter, the Secretary of State, in coordination with the National Cyber Director, the Secretary of Defense, the Director of the National Security Agency, the Secretary of Commerce, the Attorney General, the Secretary of Homeland Security, the Director of the Cybersecurity and Infrastructure Security Agency, and the heads of such other relevant Federal agencies as the Secretary of State considers appropriate, and in consultation with such nongovernmental partners as the Secretary of State considers appropriate, shall—

(1) review United States strategy, programs, and resources pertaining to international engagement on cybersecurity issues, including relevant diplomatic, foreign assistance, and joint law enforcement initiatives; and

(2) submit a report to the appropriate congressional committees that contains the findings of the review conducted pursuant to paragraph (1).

(c) REPORT ELEMENTS.—Each report submitted pursuant to subsection (b)(2) shall indicate—

(1) whether and to what extent previous and ongoing United States international engagements on cybersecurity-related issues have—

(A) reduced the frequency and severity of cyberattacks on United States individuals, businesses, governmental agencies, and other organizations;

(B) reduced cybersecurity risks to United States and allied critical infrastructure;

(C) deterred and disrupted international cybercrime, including ransomware attacks;

(D) induced other countries to endorse and uphold international laws, norms, standards, and principles supporting a free, open, and secure internet, including relevant treaties and international agreements;

(E) improved allies' and partners' cybersecurity capabilities;

(F) fostered 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;

(G) disrupted the laundering of cybercrime proceeds and other illicit financial activities related to cybercrime, including activities involving cryptocurrency and related services and exchanges;

(H) recovered the proceeds of cybercrime; and

(I) supported the innovation and development of new methods and tools for improving cybersecurity;

(2) the key ongoing challenges to achieving the objectives described in paragraph (1);

(3) whether the budgetary resources, technical expertise, legal authorities, and personnel available to the Department of State and other relevant Federal agencies are adequate to achieve the objectives described in paragraph (1);

(4) whether United States international engagements on cybersecurity-related issues adequately mobilize the private sector and civil society;

(5) whether the Department of State is properly organized and coordinated with other Federal agencies to achieve the objectives described in paragraphs (1), (3), and (4);

(6) country-specific strategies for United States international engagement with respect to malign activity in cyberspace by China, Russia, Iran, North Korea, and each country determined to be a state sponsor of international cybercrime; and

(7) any other matters that the Secretary of State considers relevant.

(d) CLASSIFICATION AND PUBLICATION.—Each report required under subsection (b)(2)—

(1) shall be unclassified, but may include a classified annex; and

(2) shall be published (without its classified annex, if any) on the public website of the Department of State.

(e) INTERAGENCY COOPERATION.—Upon a request from the Secretary of State, the head of a Federal agency, subject to any applicable restrictions under other provisions of law, shall provide full support and cooperation to the Secretary in carrying out this section, including by providing information necessary to prepare the report and strategy required under subsection (b)(2).

SEC. 1285. ESTABLISHMENT OF CYBERSECURITY ASSISTANCE FUND.

Part II of the Foreign Assistance Act of 1961 (22 U.S.C. 2301 et seq.) is amended by adding at the end the following:

''CHAPTER 10—CYBERSECURITY ASSISTANCE FUND

''SEC. 591. FINDINGS.

''Congress finds the following:

''(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 depends greatly on cybersecurity developments and practices in other countries.

''(4) United States assistance to countries and international organizations to bolster civilian cybersecurity capacity can help—

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

''(B) advance national and economic security objectives.

''SEC. 592. AUTHORIZATION OF ASSISTANCE FOR CYBERSECURITY CAPACITY BUILDING.

''(a) AUTHORIZATION.—The Secretary of State is authorized to provide assistance to foreign governments and organizations, including national and regional institutions, on such terms and conditions as the Secretary may determine, in order to build the cybersecurity capacity of partner countries and organizations.

''(b) SCOPE OF ASSISTANCE.—Assistance under this section may include—

''(1) support for the development of national strategies to enhance cybersecurity;

''(2) programs to enhance government-industry collaboration to manage cybersecurity risks and share cybersecurity knowledge;

''(3) expertise on the revision and enactment of criminal laws, policies, and procedures related to cybersecurity threats;

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

''(5) programs to strengthen the government's capacity to detect, investigate, deter, and prosecute cybercrimes;

''(6) programs to build a culture of cybersecurity, increasing awareness of citizenry and industry of their critical role in cybersecurity;

''(7) programs to enhance cybersecurity workforce development;

''(8) support for the development and use of globally relevant information and communication technologies security standards endorsed by bodies that are transparent and invite multi-stakeholder engagement;

''(9) programs to provide information and resources to diplomats engaging in discussions and negotiations around international law, norms, and capacity building measures related to cybersecurity;

''(10) support for multilateral, intergovernmental, and nongovernmental efforts to coordinate cybersecurity capacity building efforts internationally;

''(11) programs that enhance the ability of relevant stakeholders to act collectively against shared cybersecurity threats;

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

''(13) programs addressing emerging issues relevant to cybersecurity, including security, safety, and resilience concerns related to artificial intelligence, biotechnology, autonomous systems, and other emerging technological domains; and

''(14) such other functions in furtherance of this chapter, as determined by the Secretary of State.

''(c) RESPONSIBILITY FOR POLICY DECISIONS AND JUSTIFICATION.—The Secretary of State, or a designated Senate-confirmed official of the Department of State, shall be responsible for policy decisions and justifications for cybersecurity capacity support programs under this chapter, including determinations of—

''(1) whether there will be a cybersecurity support program for a country or organization; and

''(2) the amount of funds for each country or organization.

''(d) DETAILED JUSTIFICATION FOR USES AND PURPOSES OF FUNDS.—As part of the presentation materials for foreign assistance submitted annually to Congress, the Secretary of State or the Secretary's designee shall provide a detailed justification for the uses and purposes of the amounts provided under this chapter, including information concerning—

''(1) the amounts and kinds of cash grant transfers;

''(2) the amounts and kinds of budgetary and balance-of-payments support provided; and

''(3) the amounts and kinds of project assistance provided with such amounts.

''(e) ASSISTANCE UNDER OTHER AUTHORITIES.—The authority granted under this section to provide assistance for cybersecurity capacity building in countries and organizations does not preclude the use of other authorities also available for such purpose.

''(f) AVAILABILITY OF FUNDS.—Amounts appropriated to carry out this chapter shall be available for—

''(1) civilian cybersecurity programs; and

''(2) supporting military organizations if—

''(A) such organizations are responsible for civilian cybersecurity in their respective countries; and

''(B) such amounts are directed only toward the civilian cybersecurity activities of such organizations.

''(g) NOTIFICATION REQUIREMENTS.—Funds may not be obligated for assistance under this section unless the Committee on Foreign Relations of the Senate and the Committee on Foreign Affairs of the House of Representatives are each notified in writing of the amount and nature of the proposed assistance not later than 15 days before making such funds available for assistance.

''SEC. 593. REVIEW OF EMERGENCY ASSISTANCE CAPACITY.

''(a) IN GENERAL.—The Secretary of State, in consultation with other relevant Federal departments and agencies, including the Department of Defense, the Department of Justice, the Department of Homeland Security, the Department of Commerce, and the Department of Treasury, shall conduct a review that—

''(1) analyzes the Department of State's capacity to promptly and effectively deliver emergency support to countries experiencing major cybersecurity incidents;

''(2) identifies relevant legal, institutional, and resource constraints preventing the support referred to in paragraph (1); and

''(3) develops a plan for resolve such constraints.

''(b) REPORT.—Not later than 1 year after the date of the enactment of the International Cybercrime Response Act of 2022, the Secretary of State shall submit a report to the Committee on Foreign Relations of the Senate, the Committee on Appropriations of the Senate, the Committee on Foreign Affairs of the House of Representatives, and the Committee on Appropriations of the House of Representatives that contains the results of the review conducted pursuant to subsection (a).

''SEC. 594. AUTHORIZATION OF APPROPRIATIONS.

''There is authorized to be appropriated $150,000,000, during the 5-year period beginning on October 1, 2022, to carry out the purposes of this chapter.''.

SEC. 1286. ASSESSMENT, MONITORING, AND EVALUATION OF CYBERSECURITY CAPACITY BUILDING ASSISTANCE.

(a) IN GENERAL.—Not later than 18 months after the date of the enactment of this Act, the Secretary of State shall—

(1) develop an assessment, monitoring, and evaluation program for cybersecurity capacity building assistance provided by the Department of State to countries and organizations, including assistance provided pursuant to chapter 10 of part II of the Foreign Assistance Act of 1961, as added by section 1285; and

(2) provide a briefing to the Committee on Foreign Relations of the Senate and the Committee on Foreign Affairs of the House of Representatives regarding the program developed pursuant to paragraph (1).

(b) ELEMENTS.—The program developed pursuant to subsection (a)(1) shall include—

(1) maintaining a complete list of every cybersecurity capacity building assistance project of the Department of State that has a total budget in excess of $100,000;

(2) regularly evaluating the efficacy and efficiency of cybersecurity capacity building assistance, including—

(A) assessing the overall efficacy and efficiency of the Department of State's cybersecurity capacity building assistance efforts, including whether such efforts are—

(i) appropriately prioritized across different geographies, recipient organizations, and cybersecurity activities;

(ii) aligned with other Department of State and United States cybersecurity initiatives;

(iii) adequately informed by, and integrated with, relevant cybersecurity efforts in the private sector and civil society;

(iv) coordinated with other Federal agencies engaged in international cybersecurity activities, including the Department of Defense, the Department of Homeland Security, the Cybersecurity and Infrastructure Security Agency, and the Department of Commerce; and

(v) duplicative of other public or private sector initiatives;

(B) defining measurable project-level evaluation criteria;

(C) individually assessing every project referred to in paragraph (1) against the criteria defined pursuant to subparagraph (B), as applicable; and

(D) identifying relevant human rights and civil liberties concerns pertaining to each project referred to in paragraph (1), and assessing whether and how such concerns have been addressed; and

(3) identifying the lessons learned in carrying out cybersecurity capacity building assistance and recommendations for improving future assistance.

(c) OVERSIGHT.—The Secretary of State shall designate a senior official of the Department of State to lead, in coordination with relevant regional and functional bureaus, the ongoing implementation of the program developed pursuant to subsection (a)(1).

(d) GAO REPORT.—Not later than 18 months after the date of the enactment of this Act, the Comptroller General of the United States Government Accountability Office shall—

(1) evaluate the capacity of Department of State cybersecurity capacity building assistance to achieve desired outcomes in accordance with the framework described in subsection (b); and

(2) publish a report containing the results of the evaluation conducted pursuant to paragraph (1).

SA 6314. Mrs. SHAHEEN (for herself, Mr. ROMNEY, Mr. WICKER, Mr. BLUMENTHAL, Mr. CORNYN, Mr. TILLIS, Mr. DURBIN, Mr. KING, Mr. CARDIN, Mr. PORTMAN, and Mr. COONS) submitted an amendment intended to be proposed to amendment SA 5499 submitted by Mr. REED (for himself and Mr. INHOFE) and intended to be proposed to the bill H.R. 7900, to authorize appropriations for fiscal year 2023 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the end of title XII, add the following:

Subtitle G—Black Sea Security

SEC. 1281. SHORT TITLE.

This subtitle may be cited as the ''Black Sea Security Act of 2022''.

SEC. 1282. SENSE OF CONGRESS ON BLACK SEA SECURITY.

(a) SENSE OF CONGRESS.—It is the sense of Congress that—

(1) it is in the interest of the United States to prevent the spread of further armed conflict in Europe by recognizing the Black Sea region as an arena of Russian aggression;

(2) littoral states of the Black Sea are critical in countering aggression by the Government of the Russian Federation and contributing to the collective security of NATO;

(3) the repeated, illegal, unprovoked, and violent attempts of the Russian Federation to expand its territory and control access to the Mediterranean through the Black Sea constitutes a threat to the national security of the United States and NATO;

(4) the United States condemns attempts by the Russian Federation to change or alter boundaries in the Black Sea region by force or any means contrary to international law and to impose a sphere of influence across the region;

(5) the United States and its allies should robustly counter Russia's purported territorial claims on the Crimean Peninsula, along Ukraine's territorial waters in the Black Sea and the Sea of Azov, in the Black Sea's international waters, and in the territories it is illegally occupying in Ukraine;

(6) the United States should continue to work within NATO and with NATO Allies to develop a long-term strategy to enhance security, establish a permanent, sustainable presence in the eastern flank, and bolster the democratic resilience of its allies and partners in the region;

(7) the United States should also work with the European Union in coordinating a strategy to support democratic initiatives and economic prosperity in the region, which includes two European Union members and four European Union aspirant nations;

(8) the United States should explore efforts to rebuild trust and bilateral relations with Turkey, a key NATO Ally in the Black Sea region and a bulwark against Iran;

(9) it is in the interest of the United States that NATO adopt a robust strategy toward the Black Sea, including by working with interested partner countries in the region to advance common security objectives;

(10) the United States should work to foster dialogue among countries within the Black Sea region to improve communication and intelligence sharing and increase cyber defense capabilities;

(11) countries with historic and economic ties to Russia are looking to the United States and Europe to provide a positive economic presence in the broader region as a counterbalance to the Russian Federation's malign influence in the region;

(12) it is in the interest of the United States to support and bolster the economic ties between the United States and Black Sea partners;

(13) the United States should support the initiative undertaken by central and eastern European states to advance the Three Seas Initiative Fund to strengthen transport, energy, and digital infrastructure connectivity in the region between the Adriatic Sea, Baltic Sea, and Black Sea;

(14) there are mutually beneficial opportunities for increased investment and economic expansion, particularly on energy, climate, and transport infrastructure initiatives, between the United States and Black Sea states and the broader region;

(15) improved economic ties between the United States and the Black Sea states and the broader region can lead to a strengthened strategic partnership;

(16) the United States must seek to address the food security challenges arising from closure of Ukraine's Black Sea ports, as this global challenge will have critical national security implications for the United States, our partners, and allies;

(17) Russia has a brutal history of using hunger as a weapon and must be stopped; and

(18) countering the PRC's coercive economic pursuits remains an important policy imperative in order to further integrate the Black Sea countries into western economies and improve regional stability.

SEC. 1283. UNITED STATES POLICY.

It is the policy of the United States to—

(1) actively deter the threat of Russia's further escalation in the Black Sea region