

116TH CONGRESS  
2D SESSION

# H. R. 8310

To amend the Homeland Security Act of 2002 to provide for enhanced visa security, and for other purposes.

---

## IN THE HOUSE OF REPRESENTATIVES

SEPTEMBER 17, 2020

Mr. ROGERS of Alabama (for himself, Mrs. HARTZLER, Mr. RESCHENTHALER, Mr. HIGGINS of Louisiana, and Mr. JOYCE of Pennsylvania) introduced the following bill; which was referred to the Committee on the Judiciary, and in addition to the Committees on Homeland Security, and Foreign Affairs, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

---

## A BILL

To amend the Homeland Security Act of 2002 to provide for enhanced visa security, and for other purposes.

1       *Be it enacted by the Senate and House of Representa-*  
2       *tives of the United States of America in Congress assembled,*

3       **SECTION 1. SHORT TITLE.**

4       This Act may be cited as the “Countering China’s  
5       Theft of American Research and Innovation Act” or the  
6       “CCTARI Act”.

1 **SEC. 2. VISA SECURITY.**

2 (a) ESTABLISHMENT.—Not later than 90 days after  
3 the date of the enactment of this Act, the interagency  
4 working group established under section 1746(a) of the  
5 National Defense Authorization Act for Fiscal Year 2020  
6 (Public Law 116–92) shall commence a review of the cur-  
7 rent policies and procedures of the Department of Home-  
8 land Security and Department of State for the purpose  
9 of identifying, investigating, and preventing the illicit  
10 transfer of sensitive technologies and research from  
11 United States institutions of higher education and re-  
12 search institutions through more effective visa security op-  
13 erations and improved protections for such sensitive tech-  
14 nologies.

15 (b) OBJECTIVES.—

16 (1) ANALYSIS OF CURRENT VISA ISSUANCE AND  
17 ADMISSION PROCEDURES.—The interagency working  
18 group referred to in subsection (a) shall—

19 (A) analyze the current visa application  
20 process, and the role of the Department of  
21 Homeland Security and the Department of  
22 State in such process, including the screening  
23 of visa applicants against appropriate criminal,  
24 intelligence, national security, terrorism, and  
25 other databases and information maintained by  
26 the Federal Government, and make rec-

ommendations to the Secretaries of such Departments to better screen, identify, and refuse entry to individuals who seek to enter the United States to engage in the illicit transfer of sensitive technologies from United States institutions of higher educations or research institutions;

(B) evaluate current policies for refusing visas on grounds that an individual is likely to enter the United States to engage in the illicit transfer of sensitive technologies and recommend updates to the Foreign Affairs Manual and other agency guidance to clarify when and how visas can be refused on such grounds; and

(C) analyze current screening procedures at United States ports of entry and make recommendations to the Secretaries of such Departments to better identify individuals who seek to enter the United States to engage in such illicit transfer of sensitive technologies.

(2) NATIONAL SECURITY REVIEW OF CERTAIN NONIMMIGRANT STUDENTS.—The interagency working group shall recommend procedures and standards for the Department of Homeland Security, in

1 cooperation with other appropriate Federal agencies,  
2 to conduct national security reviews of aliens who—

3 (A) are present in the United States—

4 (i) in a nonimmigrant classification  
5 described in subparagraphs (F), (J), or  
6 (M) of section 101(a)(15) of the Immigra-  
7 tion and Nationality Act (8 U.S.C.  
8 1101(a)(15)) and change from a program  
9 of study not related to sensitive tech-  
10 nologies to a program of study or signifi-  
11 cant coursework, research, or laboratory  
12 access related to sensitive technologies; or

13 (ii) as a nonimmigrant and seek to  
14 change status, pursuant to section 248 of  
15 the Immigration and Nationality Act (8  
16 U.S.C. 1258)), to that of a nonimmigrant  
17 described in subparagraph (F), (J), or (M)  
18 of section 101(a)(15) of such Act (8  
19 U.S.C. 1101(a)(15)), for purposes of en-  
20 gaging in a program of study related to  
21 sensitive technologies; and

22 (B) as a result of engaging in a program  
23 of study related to sensitive technologies, will  
24 have access to information related to operating,  
25 installing, maintaining, repairing, overhauling,

1 or refurbishing sensitive technologies or devel-  
2 opment activities related to sensitive tech-  
3 nologies.

4 (3) IDENTIFYING INDIVIDUALS REQUIRING NA-  
5 TIONAL SECURITY REVIEW.—For purposes of facili-  
6 tating the identification of individuals described in  
7 paragraph (2)(B), the interagency working group  
8 shall—

9 (A) develop a nonpublic list of six-digit  
10 Classification of Instructional Programs (CIP)  
11 codes for programs of study related to sensitive  
12 technologies to be used in reporting required by  
13 section 641 of the Immigration and Nationality  
14 Act (8 U.S.C. 1372(d)) and related regulations;

15 (B) recommend to the Secretary of Home-  
16 land Security changes, as appropriate, to the  
17 Student and Exchange Visitor Information Sys-  
18 tem, or other system designated for such pur-  
19 pose by the Secretary of Homeland Security, to  
20 ensure that individuals who seek to engage in  
21 programs of study but who will not have access  
22 to information related to operating, installing,  
23 maintaining, repairing, overhauling, or refur-  
24 bishing sensitive technologies or development  
25 activities related to sensitive technologies are

1 not unnecessarily subjected to national security  
2 reviews;

3 (C) recommend to the Secretary of Home-  
4 land Security changes to relevant regulations to  
5 ensure that entities certified by the Student and  
6 Exchange Visitor Program routinely and accu-  
7 rately report the program of study and other  
8 necessary information in the Student and Ex-  
9 change Visitor Information System, or other  
10 system designated for such purpose by the Sec-  
11 retary of Homeland Security, for each non-  
12 immigrant described in subparagraph (F), (J),  
13 or (M) of section 101(a)(15) of the Immigra-  
14 tion and Nationality Act (8 U.S.C.  
15 1101(a)(15)) who is enrolled in such entity; and

16 (D) identify mechanisms for the Depart-  
17 ment of Homeland Security, in cooperation with  
18 other appropriate Federal agencies, to order the  
19 removal of and make ineligible for future non-  
20 immigrant classification described in subpara-  
21 graphs (F), (J), or (M) of section 101(a)(15) of  
22 the Immigration and Nationality Act (8 U.S.C.  
23 1101(a)(15)) individuals who may be identified  
24 following pursuant to national security reviews  
25 conducted in accordance with paragraph (2).

1           (4) IDENTIFYING GAPS IN AUTHORITY TO AD-  
2       DRESS NATIONAL SECURITY THREATS.—Not later  
3       than one year after the date of the enactment of this  
4       Act, the interagency working group shall identify de-  
5       ficiencies in existing legal authorities determined to  
6       be an impediment in achieving the recommendations  
7       described in subparagraphs (B) and (C) of para-  
8       graph (3), and recommend to the appropriate con-  
9       gressional committees legislative solutions to address  
10      such deficiencies.

11      (c) COMPOSITION.—In addition to the members spec-  
12     ified in section 1746(a)(2) of the National Defense Au-  
13     thorization Act for Fiscal Year 2020 (Public Law 116–  
14     92), for purposes of carrying out the review required  
15     under subsection (a), the interagency working group con-  
16     sult with the following:

17           (1) U.S. Customs and Border Protection, Office  
18       of Field Operations.

19           (2) U.S. Immigration and Customs Enforce-  
20       ment, Student and Exchange Visitor Program.

21           (3) U.S. Immigration and Customs Enforce-  
22       ment, Counterterrorism and Criminal Exploitation  
23       Unit.

24           (4) U.S. Immigration and Customs Enforce-  
25       ment, Visa Security Program.

1           (5) The Department of Homeland Security, Of-  
2       fice of Intelligence and Analysis.

3           (6) The Federal Bureau of Investigation.

4           (7) At least two representatives from the De-  
5       partment of State, Bureau of Consular Affairs.

6           (8) Private sector and higher education per-  
7       sonnel, as appropriate and to a degree that would  
8       not detrimentally impact any ongoing law enforce-  
9       ment investigation or intelligence operation, as de-  
10      termined by the Secretary of Homeland Security.

11       (d) CONSULTATION.—In carrying out the objectives  
12      described in subsection (b), the interagency working group  
13      shall coordinate and consult regularly with the National  
14      Science, Technology, and Security Roundtable established  
15      under section 1746(b) of the National Defense Authoriza-  
16      tion Act for Fiscal Year 2020 (Public Law 116–92).

17       (e) REPORT.—Not later than one year after the com-  
18      mencement of the review required under subsection (a),  
19      the interagency working group shall submit to the appro-  
20      priate congressional committees a report—

21           (1) detailing the results of such review and the  
22           analyses and evaluation required under subsection  
23           (b)(1); and

24           (2) identifying any legislative solutions nec-  
25           essary to improve the ability of the Department of



1 Homeland Security, the Department of State, or  
2 both, to identify, investigate, and prevent the illicit  
3 transfer of sensitive technologies from United States  
4 institutions of higher education and research institu-  
5 tions as a result of programs of study related to sen-  
6 sitive technologies undertaken by aliens described in  
7 subparagraph (F), (J), or (M) of section 101(a)(15)  
8 of the Immigration and Nationality Act (8 U.S.C.  
9 1101(a)(15)).

10 (f) DEFINITIONS.—In this section:

11 (1) APPROPRIATE CONGRESSIONAL COMMIT-  
12 TEES.—The term “appropriate congressional com-  
13 mittees” means the Committee on Homeland Secu-  
14 rity, the Committee on the Judiciary, the Committee  
15 on Armed Services, and the Committee on Foreign  
16 Affairs of the House of Representatives and the  
17 Committee on Homeland Security and Governmental  
18 Affairs, the Committee on the Judiciary, the Com-  
19 mittee on Armed Services, and the Committee on  
20 Foreign Relations of the Senate.

21 (2) INSTITUTION OF HIGHER EDUCATION.—The  
22 term “institution of higher education” has the  
23 meaning given such term in section 101 of the High-  
24 er Education Act of 1965 (20 U.S.C. 1001).

1           (3) PROGRAM OF STUDY.—The term “program  
2       of study” means any degree program, field of study,  
3       significant coursework, research, or laboratory ac-  
4       cess related to sensitive technologies, or other aca-  
5       demic activity required to be reported pursuant to  
6       section 641(a) of the Omnibus Consolidated Appro-  
7       priations Act, 1997 (Public Law 104–208 (8 U.S.C.  
8       1372(a))).

9           (4) SENSITIVE TECHNOLOGIES.—The term  
10      “sensitive technologies” has the meaning given such  
11      term in paragraph (8) of section 428(e) of the  
12      Homeland Security Act of 2002 (6 U.S.C. 236(e)),  
13      as added by section 3.

14   **SEC. 3. VISA SECURITY.**

15      (a) PROGRAM SCOPE.—Paragraph (1) of section  
16      428(e) of the Homeland Security Act of 2002 (6 U.S.C.  
17      236(e)) is amended—

18           (1) by striking “The Secretary” and inserting  
19      the following:

20                   “(A) AUTHORIZATION.—The Secretary”;  
21                   and

22           (2) by adding at the end the following new sub-  
23      paragraph:

24                   “(B) RISK-BASED ASSIGNMENTS.—

1 “(i) IN GENERAL.—Assignments  
2 under subparagraph (A) shall be made—

3 “(I) in a risk-based manner;

4 “(II) considering the criteria de-  
5 scribed in clause (ii); and

6 “(III) in accordance with Na-  
7 tional Security Decision Directive 38  
8 of June 2, 1982, or any superseding  
9 presidential directive concerning staff-  
10 ing at diplomatic and consular posts.

11 “(ii) CRITERIA DESCRIBED.—The cri-  
12 teria described in this clause are the fol-  
13 lowing:

14 “(I) The number of nationals of  
15 the subject country who were identi-  
16 fied in United States Government  
17 databases related to the identities of  
18 known or suspected terrorists during  
19 the previous two years.

20 “(II) Information on the coopera-  
21 tion of such country with the counter-  
22 terrorism efforts of the United States.

23 “(III) Information analyzing the  
24 presence, activity, or movement of ter-  
25 rorist organizations (as such term is

1 defined in section 212(a)(3)(B)(vi) of  
2 the Immigration and Nationality Act  
3 (8 U.S.C. 1182(a)(3)(B)(vi))) within  
4 or through such country.

5 “(IV) The number of formal ob-  
6 jections and denials based on deroga-  
7 tory information issued through the  
8 interagency Security Advisory Opinion  
9 process.

10 “(V) Countries identified as a  
11 strategic competitor in the ‘Summary  
12 of the 2018 National Defense Strat-  
13 egy of the United States of America:  
14 Sharpening the American Military’s  
15 Competitive Edge’ issued by the De-  
16 partment of Defense pursuant to sec-  
17 tion 113(g)(1)(A) of title 10, United  
18 States Code, or any successor docu-  
19 ment.

20 “(VI) The number of cases in-  
21 volving counterintelligence, illicit tech-  
22 nology transfer, and counterprolifera-  
23 tion related to the identities of nation-  
24 als of such country.

1 “(VII) Information on the co-  
2 operation of such country with the  
3 counterintelligence, countering non-  
4 traditional collection, illicit technology  
5 transfer, and counterproliferation ef-  
6 forts of the United States, including  
7 information on foreign government-  
8 owned infrastructure and organiza-  
9 tions dedicated to such matters.

10 “(VIII) The adequacy of the bor-  
11 der and immigration control of such  
12 country.

13 “(IX) Any other criteria the Sec-  
14 retary determines appropriate.

15 “(iii) PRIORITIZATION.—The Sec-  
16 retary shall, until December 31, 2024,  
17 prioritize the establishment of new over-  
18 seas assignments made under this sub-  
19 section to diplomatic and consular posts in  
20 countries that are strategic competitors  
21 with the goal of countering the exploitation  
22 or illicit transfer of sensitive technologies  
23 by aliens described in subparagraph (F),  
24 (J), or (M) of section 101(a)(15) of such  
25 Act (8 U.S.C. 1101(a)(15)).”.

1       (b) SCREENING.—Paragraph (2) of section 428(e) of  
2 the Homeland Security Act of 2002 (6 U.S.C. 236(e)) is  
3 amended—

4           (1) by redesignating subparagraph (C) as sub-  
5 paragraph (D); and

6           (2) by inserting after subparagraph (B) the fol-  
7 lowing new subparagraph:

8           “(C) Review visa applications of aliens  
9 against appropriate criminal, national security,  
10 and terrorism databases or other relevant infor-  
11 mation maintained by the Federal Government  
12 to improve the detection and examination of  
13 aliens whose entry into the United States would  
14 pose a substantial risk of the illicit transfer of  
15 sensitive technologies.”.

16       (c) DEFINITION.—Subsection (e) of section 428 of  
17 the Homeland Security Act of 2002 (6 U.S.C. 236(e)) is  
18 amended by inserting at the end the following new para-  
19 graph:

20           “(8) DEFINITION.—In this subsection, the term  
21 ‘sensitive technologies’ means—

22           “(A) areas of research or technology that  
23 require additional protection, as established by  
24 the interagency working group in accordance  
25 with section 1746(a)(3)(E)(i)(III) of the Na-

1           tional Defense Authorization Act for Fiscal  
2           Year 2020 (Public Law 116–92);

3           “(B) emerging and foundational tech-  
4           nologies identified through the interagency  
5           process established under section 1758 of the  
6           John S. McCain National Defense Authoriza-  
7           tion Act for Fiscal Year 2019 (Public Law  
8           115–232);

9           “(C) sciences, technologies, and associated  
10          programs of study at an institution of higher  
11          education, related to energy, nuclear science,  
12          nuclear engineering, or a related field for which  
13          an alien who is a citizen of Iran would be de-  
14          nied a visa to participate in coursework pursu-  
15          ant to section 501 of the Iran Threat Reduction  
16          and Syria Human Rights Act of 2012 (22  
17          U.S.C. 8771); and

18          “(D) technologies and items included on  
19          the Commerce Control List, the United States  
20          Munitions List, the Nuclear Regulatory Com-  
21          mission Controls, or the Technology Alert  
22          List.”.

23          (d) MEMORANDUM OF UNDERSTANDING.—Not later  
24          than 18 months days after the date of the enactment of  
25          this Act, the Secretary of Homeland Security and the Sec-

1   retary of State shall jointly develop and submit to the ap-  
2   propriate congressional committees a memorandum of un-  
3   derstanding detailing the responsibilities of and proce-  
4   dures used by Department of Homeland Security per-  
5   sonnel assigned to diplomatic and consular posts under  
6   section 428 of the Homeland Security Act of 2002, as  
7   amended by this section, including visa security vetting  
8   and screening activities, the collection and distribution of  
9   relevant fees, and the sharing of information on visa refus-  
10   als based on derogatory information issued through the  
11   interagency Security Advisory Opinion process.

12       (e) MACHINE READABLE TECHNOLOGY PILOT PRO-  
13   GRAM.—

14           (1) IN GENERAL.—Not later than one year  
15   after the date of the enactment of this Act, the Sec-  
16   retary of Homeland Security and the Secretary of  
17   State shall jointly commence a pilot program at a  
18   United States diplomatic or consular post in a coun-  
19   try with a high volume of individuals who are known  
20   to have engaged in government sponsored technology  
21   transfer campaigns. The pilot program shall—

22           (A) be conducted for not fewer than 365  
23   days; and

24           (B) assess opportunities to enhance secu-  
25   rity vetting, including the use of machine-read-



1           able technology and applicant interviews, to bet-  
2           ter defend research or sensitive technologies in  
3           the United States from foreign government  
4           sponsored technology transfer campaigns.

5           (2) MACHINE READABLE TECHNOLOGY.—The  
6           Secretary of Homeland Security and the Secretary  
7           of State shall jointly, as part of the pilot program  
8           under paragraph (1)—

9                   (A) deploy and test equipment and tech-  
10                  nology to ensure that all documents collected in  
11                  connection with visa applications are stored in  
12                  a machine-readable and content-searchable for-  
13                  mat compatible and shareable between the De-  
14                  partment of Homeland Security and the De-  
15                  partment of State, and as appropriate, other  
16                  interagency partners;

17                  (B) collect supplemental documents from  
18                  visa applicants in accordance with the require-  
19                  ments under subparagraph (A), as appropriate,  
20                  and ensure appropriate personnel from the De-  
21                  partment of Homeland Security and the De-  
22                  partment of State have access to such docu-  
23                  ments for visa security vetting purposes; and

1 (C) evaluate the use of such technology  
2 and supplemental documents in improving the  
3 efficacy and efficiency of visa security vetting.

4 (3) APPLICANT INTERVIEWS.—The Secretary of  
5 Homeland Security, in coordination with the Sec-  
6 retary of State, shall determine whether additional  
7 questions or further documentation requests may be  
8 appropriate during visa applicant in-person inter-  
9 views to improve visa security vetting to address  
10 evolving threats to the United States.

11 (4) REPORT.—Not later than 420 days after  
12 the initiation of the pilot program under paragraph  
13 (1), the Secretary of Homeland Security and the  
14 Secretary of State shall jointly submit to the appro-  
15 priate congressional committees and other appro-  
16 priate Federal partners a report on the following:

17 (A) The results of the pilot program.

18 (B) Recommendations for machine-read-  
19 able and content searchable equipment and  
20 technology and supplemental documents under  
21 paragraph (2).

22 (C) Recommendations for additional inter-  
23 view questions and further documentation re-  
24 quests under paragraph (3).

1 (D) A determination as to whether and  
2 where to expand the use of technologies evalu-  
3 ated during the pilot program.

4 (f) DEFINITIONS.—In this section:

5 (1) APPROPRIATE CONGRESSIONAL COMMIT-  
6 TEES.—The term “appropriate congressional com-  
7 mittees” means—

8 (A) the Committee on Homeland Security,  
9 the Committee on the Judiciary, and the Com-  
10 mittee on Foreign Affairs of the House of Rep-  
11 resentatives; and

12 (B) the Committee on Homeland Security  
13 and Governmental Affairs, the Committee on  
14 the Judiciary, and the Committee on Foreign  
15 Relations of the Senate.

16 (2) SCREENING.—The term “screening” means  
17 the review of public, private, or governmental infor-  
18 mation to assess the accuracy and authenticity of  
19 claims made on a visa application, including infor-  
20 mation contained in Federal Government records to  
21 include derogatory information.

22 (3) SENSITIVE TECHNOLOGIES.—The term  
23 “sensitive technologies” has the meaning given such  
24 term in paragraph (8) of section 428(e) of the

1 Homeland Security Act of 2002 (6 U.S.C. 236(e)),  
2 as added by subsection (c)

3 (4) STRATEGIC COMPETITOR.—The term “stra-  
4 tegic competitor” means a country identified as a  
5 strategic competitor to the United States in the  
6 “Summary of the 2018 National Defense Strategy  
7 of the United States of America: Sharpening the  
8 American Military’s Competitive Edge” issued by  
9 the Department of Defense pursuant to section  
10 113(g)(1)(A) of title 10, United States Code, or any  
11 successor document.

12 (5) VETTING.—The term “vetting” with respect  
13 to a visa applicant means the review and use of in-  
14 formation collected during screening, any additional  
15 information obtained through interviews, consulta-  
16 tion with other Federal Government officials, derog-  
17 atory information, and information drawn from  
18 other sources to reach a determination regarding a  
19 national security concern related to the visa appli-  
20 cant.

○