

House Engrossed

critical infrastructure; foreign adversary; prohibition

State of Arizona
House of Representatives
Fifty-seventh Legislature
First Regular Session
2025

HOUSE BILL 2696

AN ACT

AMENDING TITLE 18, CHAPTER 1, ARTICLE 1, ARIZONA REVISED STATUTES, BY
ADDING SECTION 18-105; AMENDING TITLE 44, ARIZONA REVISED STATUTES, BY
ADDING CHAPTER 42; RELATING TO CRITICAL INFRASTRUCTURE.

(TEXT OF BILL BEGINS ON NEXT PAGE)

1 Be it enacted by the Legislature of the State of Arizona:

2 Section 1. Title 18, chapter 1, article 1, Arizona Revised
3 Statutes, is amended by adding section 18-105, to read:

4 18-105. Software; critical infrastructure; critical
5 communications infrastructure; annual list;
6 definitions

7 A. ANY SOFTWARE THAT IS USED FOR CRITICAL INFRASTRUCTURE IN THIS
8 STATE MAY NOT BE PRODUCED BY A COMPANY THAT IS HEADQUARTERED IN THE
9 PEOPLE'S REPUBLIC OF CHINA OR THAT IS UNDER THE CONTROL OF THE PEOPLE'S
10 REPUBLIC OF CHINA.

11 B. ANY CRITICAL COMMUNICATIONS INFRASTRUCTURE WITHIN THIS STATE MAY
12 NOT INCLUDE ANY EQUIPMENT THAT IS MANUFACTURED BY A CORPORATION DOMICILED
13 IN THE PEOPLE'S REPUBLIC OF CHINA.

14 C. ANY EQUIPMENT OF CRITICAL COMMUNICATIONS INFRASTRUCTURE IN THIS
15 STATE THAT IS CURRENTLY MANUFACTURED BY A CORPORATION DOMICILED IN THE
16 PEOPLE'S REPUBLIC OF CHINA SHALL BE REPLACED WITH EQUIPMENT THAT IS NOT
17 MANUFACTURED BY A CORPORATION DOMICILED IN THE PEOPLE'S REPUBLIC OF CHINA.

18 D. ON OR BEFORE JANUARY 1 OF EACH YEAR, IF A CRITICAL
19 COMMUNICATIONS INFRASTRUCTURE PROVIDER IS A PARTICIPANT IN THE SECURE AND
20 TRUSTED COMMUNICATIONS NETWORKS REIMBURSEMENT PROGRAM PURSUANT TO 47
21 UNITED STATES CODE SECTION 1601 (P.L. 116-124, 134 STAT. 158), THE
22 CRITICAL COMMUNICATIONS INFRASTRUCTURE PROVIDER SHALL CERTIFY TO THE
23 CORPORATION COMMISSION ANY INSTANCES OF PROHIBITED CRITICAL COMMUNICATIONS
24 EQUIPMENT USE PURSUANT TO SUBSECTION B OF THIS SECTION, ALONG WITH THE
25 GEOGRAPHIC COORDINATES OF THE AREAS SERVED BY THE PROHIBITED EQUIPMENT.
26 IF THE CRITICAL COMMUNICATIONS INFRASTRUCTURE PROVIDER IS CERTIFIED BY THE
27 CORPORATION COMMISSION, THE CRITICAL COMMUNICATIONS INFRASTRUCTURE
28 PROVIDER SHALL SUBMIT A STATUS REPORT TO THE CORPORATION COMMISSION EVERY
29 QUARTER DETAILING COMPLIANCE WITH THE SECURE AND TRUSTED COMMUNICATIONS
30 NETWORKS REIMBURSEMENT PROGRAM PURSUANT TO THIS SUBSECTION. EACH QUARTER,
31 THE CORPORATION COMMISSION SHALL PRODUCE A MAP OF THIS STATE DETAILING THE
32 AREAS THAT ARE SERVICED BY CRITICAL COMMUNICATIONS INFRASTRUCTURE THAT
33 INCLUDES EQUIPMENT THAT IS MANUFACTURED BY A CORPORATION DOMICILED IN THE
34 PEOPLE'S REPUBLIC OF CHINA.

35 E. ANY COMMUNICATIONS PROVIDER THAT REMOVES, DISCONTINUES OR
36 REPLACES ANY COMMUNICATIONS EQUIPMENT THAT IS PROHIBITED BY THIS SECTION
37 IS NOT REQUIRED TO OBTAIN AN ADDITIONAL PERMIT FROM ANY STATE AGENCY OR
38 POLITICAL SUBDIVISION OF THIS STATE FOR THE REMOVAL, DISCONTINUANCE OR
39 REPLACEMENT OF THE PROHIBITED EQUIPMENT.

40 F. A GOVERNMENTAL ENTITY OR CRITICAL INFRASTRUCTURE SERVICE
41 PROVIDER IN THIS STATE MAY NOT ENTER INTO OR RENEW A CONTRACT WITH A
42 VENDOR OF WI-FI ROUTERS, MODEM SYSTEMS, LIDAR TECHNOLOGY, CAMERA-BASED
43 SCHOOL BUS INFRACTION DETECTION SYSTEMS, SPEED DETECTION SYSTEMS, TRAFFIC
44 INFRACTION DETECTOR SYSTEMS OR ANY OTHER CAMERA SYSTEMS, BATTERY
45 TECHNOLOGY OR SMART METER TECHNOLOGY OR A VENDOR OF ANY OTHER TECHNOLOGY
46 IF ANY OF THE FOLLOWING APPLIES:

1 1. THE VENDOR IS OWNED BY THE GOVERNMENT OF THE PEOPLE'S REPUBLIC
2 OF CHINA.

3 2. THE GOVERNMENT OF THE PEOPLE'S REPUBLIC OF CHINA HAS A
4 CONTROLLING INTEREST IN THE VENDOR.

5 3. THE VENDOR IS SELLING A PRODUCT THAT IS PRODUCED BY THE
6 GOVERNMENT OF THE PEOPLE'S REPUBLIC OF CHINA OR A COMPANY DOMICILED IN
7 THE PEOPLE'S REPUBLIC OF CHINA.

8 4. THE VENDOR'S PRODUCT INCLUDES CELLULAR INTERNET-OF-THINGS
9 MODULES FROM THE PEOPLE'S REPUBLIC OF CHINA.

10 5. THE VENDOR'S PRODUCT INCLUDES A PRODUCT PRODUCED BY A CHINESE
11 MILITARY COMPANY OPERATING IN THE UNITED STATES AS IDENTIFIED BY SECTION
12 1260H OF THE WILLIAM M. THORNBERRY NATIONAL DEFENSE AUTHORIZATION ACT FOR
13 FISCAL YEAR 2021 (P.L. 116-283; 134 STAT. 3388).

14 G. ON OR BEFORE MARCH 31, 2026 AND EACH YEAR THEREAFTER, EACH
15 GOVERNMENTAL ENTITY AND CRITICAL INFRASTRUCTURE SERVICE PROVIDER IN THIS
16 STATE SHALL CERTIFY TO THE CORPORATION COMMISSION THAT THE PROVIDER DOES
17 NOT USE ANY TECHNOLOGY THAT INCLUDES CELLULAR INTERNET-OF-THINGS MODULES
18 OR ANY WI-FI ROUTER OR MODEM SYSTEM, LIDAR TECHNOLOGY, CAMERA-BASED SCHOOL
19 BUS INFRACTION DETECTION SYSTEM, SPEED DETECTION SYSTEM, TRAFFIC
20 INFRACTION DETECTOR SYSTEM OR ANY OTHER CAMERA SYSTEM, BATTERY TECHNOLOGY
21 OR SMART METER TECHNOLOGY THAT IS PRODUCED BY ANY OF THE FOLLOWING:

22 1. A COMPANY THAT IS OWNED BY THE GOVERNMENT OF THE PEOPLE'S
23 REPUBLIC OF CHINA.

24 2. A COMPANY IN WHICH THE PEOPLE'S REPUBLIC OF CHINA HAS A
25 CONTROLLING INTEREST.

26 3. THE GOVERNMENT OF THE PEOPLE'S REPUBLIC OF CHINA OR A COMPANY
27 DOMICILED IN THE PEOPLE'S REPUBLIC OF CHINA.

28 H. ON OR BEFORE DECEMBER 31, 2025 AND EACH YEAR THEREAFTER, THE
29 CORPORATION COMMISSION SHALL PUBLISH A LIST OF ALL TECHNOLOGIES THAT ARE
30 PROHIBITED PURSUANT TO THIS SECTION AND SHALL POST THE LIST ON THE
31 CORPORATION COMMISSION'S WEBSITE.

32 I. EXCEPT AS PROVIDED IN SUBSECTION J OF THIS SECTION, EACH
33 GOVERNMENTAL ENTITY AND CRITICAL INFRASTRUCTURE SERVICE PROVIDER IN THIS
34 STATE SHALL REMOVE ANY TECHNOLOGY THAT IS INCLUDED BY THE CORPORATION
35 COMMISSION ON THE PROHIBITED TECHNOLOGIES LIST PURSUANT TO SUBSECTION H OF
36 THIS SECTION WITHIN NINETY DAYS AFTER THE CORPORATION COMMISSION PUBLISHES
37 THE LIST.

38 J. A GOVERNMENT ENTITY OR CRITICAL INFRASTRUCTURE PROVIDER MAY
39 CONTINUE TO PURCHASE AND USE ANY PROHIBITED TECHNOLOGY PURSUANT TO THIS
40 SECTION IF ALL OF THE FOLLOWING APPLY:

41 1. THERE ARE NO OTHER REASONABLE PROVIDERS OF THE PROHIBITED
42 TECHNOLOGY.

43 2. THE PURCHASE OR USE OF THE PROHIBITED TECHNOLOGY IS PREAPPROVED
44 BY THE CORPORATION COMMISSION.

1 3. NOT PURCHASING OR USING THE PROHIBITED TECHNOLOGY WOULD POSE A
2 GREATER THREAT TO THIS STATE THAN THE THREAT ASSOCIATED WITH THE
3 PROHIBITED TECHNOLOGY.

4 K. FOR THE PURPOSES OF THIS SECTION:

5 1. "CELLULAR INTERNET-OF-THINGS MODULE" MEANS A HARDWARE COMPONENT
6 THAT INCLUDES A CELLULAR RADIO TRANSCEIVER AND THAT IS DESIGNED TO PROVIDE
7 CELLULAR NETWORK CONNECTIVITY TO AN INTERNET-OF-THINGS DEVICE.

8 2. "COMPANY" MEANS:

9 (a) A SOLE PROPRIETORSHIP, ORGANIZATION, ASSOCIATION, CORPORATION,
10 PARTNERSHIP, JOINT VENTURE, LIMITED PARTNERSHIP, LIMITED LIABILITY
11 PARTNERSHIP OR LIMITED LIABILITY COMPANY, INCLUDING A WHOLLY OWNED
12 SUBSIDIARY, MAJORITY-OWNED SUBSIDIARY, PARENT COMPANY OR AFFILIATE OF
13 THOSE ENTITIES OR BUSINESS ASSOCIATIONS, THAT EXISTS TO MAKE A PROFIT.

14 (b) A NONPROFIT ORGANIZATION.

15 3. "CRITICAL COMMUNICATIONS INFRASTRUCTURE" MEANS ALL PHYSICAL
16 BROADBAND INFRASTRUCTURE AND EQUIPMENT THAT SUPPORTS THE TRANSMISSION OF
17 INFORMATION AND THAT ALLOWS THE USER TO ENGAGE IN COMMUNICATIONS,
18 INCLUDING SERVICE PROVIDED DIRECTLY TO THE PUBLIC.

19 4. "CRITICAL INFRASTRUCTURE" MEANS INFRASTRUCTURE THAT IS OWNED OR
20 OPERATED BY THIS STATE, A POLITICAL SUBDIVISION OF THIS STATE OR A
21 PUBLICLY REGULATED UTILITY AND THAT IS ANY OF THE FOLLOWING:

22 (a) GAS AND OIL PRODUCTION, STORAGE OR DELIVERY SYSTEMS.

23 (b) WATER SUPPLY REFINEMENT, STORAGE OR DELIVERY SYSTEMS.

24 (c) ELECTRICAL POWER DELIVERY SYSTEMS.

25 (d) TELECOMMUNICATIONS NETWORKS.

26 (e) TRANSPORTATION SYSTEMS AND SERVICES.

27 (f) PERSONAL DATA STORAGE SYSTEMS, INCLUDING CYBERSECURITY.

28 (g) EMERGENCY SERVICES.

29 5. "DOMICILED" MEANS LOCATED IN A COUNTRY WHERE EITHER THE COMPANY
30 IS REGISTERED, THE COMPANY'S AFFAIRS ARE PRIMARILY COMPLETED OR THE
31 MAJORITY OF THE COMPANY'S OWNERSHIP SHARES ARE HELD.

32 6. "SCHOOL BUS INFRACTION DETECTION SYSTEM" MEANS AN AUTOMATED
33 SYSTEM INSTALLED ON A SCHOOL BUS CONSISTING OF CAMERAS, SENSORS AND
34 SOFTWARE DESIGNED TO DETECT, RECORD AND DOCUMENT TRAFFIC VIOLATIONS, SUCH
35 AS ILLEGALLY PASSING THE BUS WHEN ITS STOP ARM IS EXTENDED AND WARNING
36 LIGHTS ARE ACTIVATED, TO ENHANCE STUDENT SAFETY AND ENFORCE COMPLIANCE
37 WITH TRAFFIC LAWS.

38 Sec. 2. Title 44, Arizona Revised Statutes, is amended by adding
39 chapter 42, to read:

40 CHAPTER 42

41 CRITICAL INFRASTRUCTURE

42 ARTICLE 1. PROHIBITED AGREEMENTS

43 44-8051. Definition of critical infrastructure

44 IN THIS ARTICLE, UNLESS THE CONTEXT OTHERWISE REQUIRES, "CRITICAL
45 INFRASTRUCTURE" MEANS INFRASTRUCTURE THAT IS OWNED OR OPERATED BY THIS

1 STATE, A POLITICAL SUBDIVISION OF THIS STATE OR A PUBLICLY REGULATED
2 UTILITY AND THAT IS ANY OF THE FOLLOWING:

- 3 1. GAS AND OIL PRODUCTION, STORAGE OR DELIVERY SYSTEMS.
- 4 2. WATER SUPPLY REFINEMENT, STORAGE OR DELIVERY SYSTEMS.
- 5 3. ELECTRICAL POWER DELIVERY SYSTEMS.
- 6 4. TELECOMMUNICATIONS NETWORKS.
- 7 5. TRANSPORTATION SYSTEMS AND SERVICES.
- 8 6. PERSONAL DATA STORAGE SYSTEMS, INCLUDING CYBERSECURITY.
- 9 7. EMERGENCY SERVICES.

10 44-8052. Critical infrastructure: prohibited agreements and
11 contracts; exceptions

12 A. EXCEPT AS PROVIDED IN SUBSECTION B OF THIS SECTION, A
13 GOVERNMENTAL ENTITY OR A PUBLICLY REGULATED UTILITY IN THIS STATE MAY NOT
14 ENTER INTO AN AGREEMENT OR CONTRACT INVOLVING CRITICAL INFRASTRUCTURE IN
15 THIS STATE WITH THE PEOPLE'S REPUBLIC OF CHINA IF UNDER THE AGREEMENT OR
16 CONTRACT THE PEOPLE'S REPUBLIC OF CHINA, DIRECTLY OR REMOTELY, WOULD BE
17 ABLE TO ACCESS OR CONTROL CRITICAL INFRASTRUCTURE IN THIS STATE.

18 B. A GOVERNMENTAL ENTITY OR A PUBLICLY REGULATED UTILITY IN THIS
19 STATE MAY ENTER INTO AN AGREEMENT OR CONTRACT INVOLVING CRITICAL
20 INFRASTRUCTURE IN THIS STATE WITH THE PEOPLE'S REPUBLIC OF CHINA IF ANY OF
21 THE FOLLOWING APPLIES:

22 1. NO OTHER REASONABLE OPTION EXISTS FOR ADDRESSING A NEED THAT IS
23 RELEVANT TO CRITICAL INFRASTRUCTURE IN THIS STATE.

24 2. THE AGREEMENT OR CONTRACT IS PREAPPROVED BY THE CORPORATION
25 COMMISSION.

26 3. NOT ENTERING INTO THE AGREEMENT WOULD POSE A GREATER THREAT TO
27 THIS STATE THAN THE THREAT ASSOCIATED WITH ENTERING INTO THE AGREEMENT OR
28 CONTRACT.

29 C. THE CORPORATION COMMISSION SHALL ESTABLISH A SECURE AND
30 DEDICATED COMMUNICATIONS CHANNEL FOR CRITICAL INFRASTRUCTURE PROVIDERS AND
31 MILITARY INSTALLATIONS ACROSS THIS STATE TO CONNECT WITH THE CORPORATION
32 COMMISSION AND OFFICE OF THE GOVERNOR IN THE EVENT OF AN EMERGENCY THAT
33 DAMAGES CRITICAL COMMUNICATIONS INFRASTRUCTURE. FOR THE PURPOSES OF THIS
34 PARAGRAPH, "CRITICAL COMMUNICATIONS INFRASTRUCTURE" HAS THE SAME MEANING
35 PRESCRIBED IN SECTION 18-105.

36 Sec. 3. Short title

37 This act may be cited as the "Arizona Critical Infrastructure
38 Protection Act".