

**ORAL ARGUMENT SCHEDULED FOR SEPTEMBER 16, 2024**

**Nos. 24-1113, 24-1130, 24-1183**

---

---

**IN THE UNITED STATES COURT OF APPEALS  
FOR THE DISTRICT OF COLUMBIA CIRCUIT**

TIKTOK INC. and BYTEDANCE LTD.,

Petitioners,

v.

MERRICK B. GARLAND, in his official capacity as Attorney General of the  
United States,

Respondent.

consolidated with

*caption continued on inside cover*

---

On Petitions for Review of the Protecting Americans from Foreign Adversary  
Controlled Applications Act

---

**PUBLIC REDACTED GOVERNMENT APPENDIX**

---

TRICIA WELLMAN  
*Acting General Counsel*

JAMES R. POWERS  
*Chief, Litigation*

JENNIFER M. PIKE  
*Associate General Counsel  
Office of the Director of National  
Intelligence*

DIANE KELLEHER  
BONNIE E. DEVANY  
SIMON G. JEROME  
*Attorneys, Federal Programs Branch  
Civil Division  
U.S. Department of Justice*

(additional counsel on inside cover)

BRIAN M. BOYNTON  
*Principal Deputy Assistant Attorney  
General*

BRIAN D. NETTER  
*Deputy Assistant Attorney General*

MARK R. FREEMAN  
SHARON SWINGLE  
DANIEL TENNY  
CASEN B. ROSS

SEAN R. JANDA  
BRIAN J. SPRINGER  
*Attorneys, Appellate Staff  
Civil Division, Room 7260  
U.S. Department of Justice  
950 Pennsylvania Avenue NW  
Washington, DC 20530  
(202) 514-3388*

---

---

BRIAN FIREBAUGH, CHLOE JOY SEXTON, TALIA CADET, TIMOTHY MARTIN, KIERA SPANN, PAUL TRAN, CHRISTOPHER TOWNSEND, and STEVEN KING,

Petitioners,

v.

MERRICK B. GARLAND, in his official capacity as Attorney General of the United States,

Respondent.

---

BASED Politics Inc.

Petitioner,

v.

MERRICK B. GARLAND, in his official capacity as Attorney General of the United States,

Respondent.

---

MATTHEW G. OLSEN  
*Assistant Attorney General for National Security*

DEVIN A. DEBACKER  
*Chief, Foreign Investment Review Section*

ERIC S. JOHNSON  
*Principal Deputy Chief, Foreign Investment Review Section*

TYLER J. WOOD  
*Deputy Chief, Foreign Investment Review Section*

EVAN SILLS  
*Attorney-Advisor, Foreign Investment Review Section  
National Security Division  
U.S. Department of Justice*

BRADLEY BOOKER  
*General Counsel*

KELLY SMITH  
*Section Chief*

NADIN LINTHORST  
*Assistant General Counsel*

TUCKER MCNULTY  
*Assistant General Counsel*

ANN OAKES  
*Assistant General Counsel  
Federal Bureau of Investigation*

## TABLE OF CONTENTS

	<b><u>Page</u></b>
Declaration of Casey Blackburn, Assistant Director of National Intelligence, Office of the Director of National Intelligence .....	Gov't App. 1
Declaration of Kevin Vorndran, Assistant Director, Counterintelligence Division, Federal Bureau of Investigation.....	Gov't App. 31
Declaration of David Newman, Principal Deputy Assistant Attorney General, National Security Division, Department of Justice ....	Gov't App. 44



UNITED STATES COURT OF APPEALS  
FOR THE DISTRICT OF COLUMBIA CIRCUIT

TIKTOK INC., *et al.*,  
*Petitioners*,  
  
v.  
  
MERRICK B. GARLAND, in his official capacity  
as Attorney General of the United States,  
*Respondent*.

Case No. 24-1113, 24-1130, 24-1183

**FILED IN CAMERA, EX PARTE,  
AND UNDER SEAL**

**(U) IN CAMERA, EX PARTE CLASSIFIED DECLARATION OF CASEY BLACKBURN,  
ASSISTANT DIRECTOR OF NATIONAL INTELLIGENCE**

(U) I, Casey Blackburn, declare as follows:

1. (U) I am an Assistant Director of National Intelligence and the Director of the Office of Economic Security and Emerging Technologies (“OESET”) at the Office of the Director of National Intelligence (“ODNI”). I have held these positions since October 2023.

2. (U//~~FOUO~~) As the Director of OESET, I seek to integrate the Intelligence Community, non-Intelligence Community government partners, and industry to enable consolidated understanding of the trends and comparative advantages in emerging technologies to better inform U.S. policymakers. I also oversee OESET’s Investment Security Group, which



[REDACTED]

has played a leading role in the Intelligence Community’s efforts to assess the national security risks posed by ByteDance Ltd. (“ByteDance”) and TikTok Inc. (“TikTok US”).<sup>1</sup>

3. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

4. (U) In the course of my official duties at ODNI, I have been advised of these lawsuits and the allegations at issue in the above-captioned Petitions for Review. The statements made in this declaration are based on my personal knowledge, as well as on information provided to me in my official capacity, and on my personal evaluation of that information.

5. (U) Two intelligence officers assigned to OESET’s Investment Security Group, in concert with representatives from the Department of Justice and the FBI, provided several briefings to Congress, including numerous members of the Senate and House of Representatives and their staffs, in January, February, and March 2024, regarding the national security threat

---

<sup>1</sup> (U) In general, I use the term “TikTok” in this declaration to broadly refer to the worldwide TikTok entities and TikTok application. Where relevant, I use the more specific term “TikTok US” to refer to the U.S.-based entity that operates the TikTok application within the United States. And I use the term “TikTok Global” to refer to TikTok Limited and the constellation of other entities that own, operate, or otherwise control the TikTok application outside of the United States. Finally, I use the term “ByteDance” to refer to that entity in its capacity both as TikTok’s parent and as the operator of Douyin, the Chinese version of the TikTok application.

[REDACTED]

[REDACTED]

posed by ByteDance and TikTok. These included a House Energy and Commerce full committee markup hearing on March 7, 2024; an all-member classified briefing of the House of Representatives on March 12, 2024, that included more than 100 Members; and a classified briefing for members of the Senate Select Committee on Intelligence and the Senate Commerce, Science, and Technology Committee on March 20, 2024.

6. [REDACTED]

[REDACTED]

7. (U) My declaration complements declarations provided by other agencies in support of the government's defense in this matter. This includes the Declaration of David Newman, Principal Deputy Assistant Attorney General, Department of Justice, National Security Division, and the Declaration of Kevin Vorndran, Assistant Director, FBI. I make this declaration in support of the U.S. government's responses to the Petitions.

8. (U) This declaration contains classified national security information under Executive Order 13526, *Classified National Security Information*, 75 Fed. Reg. 707 (Dec. 29, 2009), and applicable regulations. Consistent with those authorities, the unauthorized disclosure

[REDACTED]

[REDACTED]

of the information discussed herein could cause serious, or in some cases exceptionally grave, damage to U.S. national security, as well as damage to intelligence sources and methods. As a result, I am submitting this declaration solely for the Court's *in camera, ex parte* review.

**(U) Summary Of National Security Risks Associated with TikTok**

9. (U) The U.S. Intelligence Community assesses that ByteDance and TikTok pose a potential threat to U.S. national security because they could be used by the PRC against the United States in two principal ways: malign foreign influence targeting U.S. persons, and collection of sensitive data of U.S. persons.<sup>2</sup> First, while we have no information that the PRC has done so with respect to the platform operated by TikTok in the United States, there is a risk that the PRC may coerce ByteDance or TikTok to covertly manipulate the information received by the millions of Americans that use the TikTok application every day, through censorship or manipulation of TikTok's algorithm, in ways that benefit the PRC and harm the United States. Second, there is a risk that the PRC may coerce ByteDance or TikTok to provide the PRC access to sensitive and personally identifying U.S. user data collected by the TikTok application, so that the PRC can use that data in ways that are harmful to U.S. national security. I elaborate on these risks below.

10. [REDACTED]

[REDACTED]

[REDACTED]

---

<sup>2</sup> [REDACTED]

[REDACTED]

[REDACTED]

11. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

12. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

13. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

---

<sup>3</sup> (U) Douyin is the version of the TikTok application that operates within China.

[REDACTED]



[REDACTED]

14. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

**(U) Background**

***(U) Threats And Challenges to The United States Posed by The People’s Republic of China***

15. (U) The PRC engages in competitive behavior that directly threatens U.S. interests, including in national security, military, economic, social, cyber, and technological domains.

16. (U) The Chinese Communist Party, through the PRC (which it controls), seeks to make the PRC the preeminent power in East Asia and a major power on the world stage. In pursuit of that goal, the PRC seeks to undercut U.S. influence, drive wedges between the United States and its partners, surpass the United States in comprehensive national power, and foster norms that favor the PRC’s authoritarian system.

17. (U) The PRC combines its economic heft with its growing military power and its diplomatic and technological dominance for a coordinated approach to strengthen Chinese Communist Party rule, secure what it views as its sovereign territory and regional preeminence, and pursue global power.

18. (U) The PRC has attempted to expand its influence through projects like the Belt and Road Initiative, Global Development Initiative, and Global Security Initiative, to promote a

[REDACTED]

PRC-led alternative to U.S.- and Western-led international development and security frameworks.

19. (U) The PRC seeks to undercut U.S. military superiority, particularly in East Asia. Taiwan, in particular, is a significant potential flashpoint for confrontation between the PRC and the United States as the PRC claims that the United States is using Taiwan to undermine China's rise. The PRC will continue to apply military and economic pressure as well as public messaging and influence activities in pursuit of forced unification with Taiwan.

20. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

21. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

22. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

23. (U) The PRC has undertaken, undertakes, and will undertake overt and covert actions to undermine U.S. interests, public and private. The PRC uses whole-of-government tools to compel other countries to acquiesce to its preferences, including its assertions of sovereignty over Taiwan.

24. (U) The threat from the PRC manifests in many ways, including the following categories:

25. (U) *Technology*. The PRC targets key sectors and proprietary commercial and military technology from U.S. and allied companies and institutions. The PRC has shown a willingness to use various methods, including economic espionage and cyber theft, to give its firms a competitive advantage against the United States and its companies. China seeks to become a world science and technology superpower and to use this technological superiority for economic, political, and military gain.

26. (U) *Cyber*. The PRC is the most active and persistent cyber espionage threat to U.S. government, private-sector, and critical infrastructure networks. The PRC's cyber espionage pursuits and its industry's export of surveillance, information, and communications technologies increase the threats of aggressive cyber operations against the United States and the suppression of the free flow of information in cyberspace. The PRC's cyber espionage includes not just traditional targeting of the U.S. government but extensive and broad-ranging economic espionage aimed at stealing U.S. technology, commercial information, and trade secrets from many different sectors to benefit the PRC and Chinese companies. The PRC has stolen

technology and information worth billions of dollars from the United States through cyber and other means. Moreover, PRC-sponsored hackers have pre-positioned for potential cyber-attacks against U.S. critical infrastructure by building out offensive weapons within that infrastructure, poised to attack whenever the PRC decides the time is right. The United States has found persistent PRC access in U.S. critical telecommunications, energy, water, and other infrastructure. PRC hackers known as “Volt Typhoon” hide within our networks, lying in wait to use their access to harm U.S. civilians. China’s hacking program, which spans the globe and thus affects U.S. partners as well, is larger than that of every other major nation, combined.

27. (U) *Censorship and transnational repression.* The PRC leads the world in applying surveillance and censorship to monitor its population and suppress dissent. In addition, the PRC conducts cyber intrusions targeted to affect U.S. and non-U.S. citizens beyond its borders—including journalists, dissidents, and individuals it views as threats—to counter and suppress views it considers critical of Chinese Communist Party narratives, policies, and actions.

28. (U) For example, in 2023, the United States indicted dozens of PRC officials for a campaign of harassment against pro-democracy dissidents in the United States. The officials created and maintained thousands of fake social media accounts to spread PRC propaganda in the United States and to identify and harass dissidents who objected to the propaganda. PRC officials also conspired with an employee at a videoconferencing company to disrupt meetings by U.S.-based dissidents commemorating the 1989 Tiananmen Square massacre. And a PRC official attempted to derail the candidacy of a person seeking elected office in the United States, who was critical of the PRC government, by attempting to find and release compromising information on the candidate

29. (U) *Malign influence operations.* The PRC is expanding its global covert influence posture to better support the Chinese Communist Party's goals. The PRC aims to sow doubts about U.S. leadership, undermine democracy, and extend the PRC's influence abroad. Through its online influence operations, the PRC seeks to promote pro-PRC narratives, refute U.S.-promoted narratives, and counter other countries' policies that threaten the PRC's interests. In particular, the PRC is intensifying its efforts to mold U.S. public discourse or magnify U.S. societal divisions in ways favorable to the PRC.

30. (U) *Intelligence operations.* The PRC seeks to expand its global intelligence posture to advance the Chinese Communist Party's ambitions, challenge U.S. national security and global influence, and steal trade secrets and intellectual property to bolster the PRC's domestic industry. PRC intelligence officials will try to expand their use of digital monitoring, data collection, and advanced analytic capabilities against political security targets beyond the PRC's borders. The PRC is rapidly expanding and improving its artificial intelligence and big data analytics capabilities for intelligence operations.

31. (U) *Data Collection on U.S. Persons.* The PRC has engaged in extensive and years-long efforts to accumulate structured datasets, in particular on U.S. persons, to support its intelligence and counterintelligence operations.

32. (U) The PRC uses a number of methods to obtain data. For example, cyber actors associated with the PRC obtained reams of data on U.S. government personnel from the Office of Personnel Management's systems and PRC intelligence services stole financial data on over 147 million Americans from a U.S. credit-reporting agency and were almost certainly responsible for the theft of health data on nearly 80 million Americans from a U.S. health insurance provider.

[REDACTED]

33. (U) The PRC also tries to leverage access through its relationships with Chinese companies, strategic investments in foreign companies, and by purchasing large data sets. For example:

a. (U) The PRC, and Chinese companies, have sought to acquire sensitive health and genomic data on U.S. persons through, for example, investment in U.S. firms that handle such data or by partnering with healthcare or research organizations in the United States to provide genomic sequencing services.

b. [REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

34. [REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

35. [REDACTED]  
[REDACTED]

a. [REDACTED]  
[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

b.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

c.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

d.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

e.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

36. (U) As set forth at greater length below, ByteDance and TikTok present powerful platforms by which the PRC could take actions falling in many of the foregoing categories.

**(U) TikTok Background**

37. (U) TikTok is a social media application (with corresponding mobile and web applications) on which users can create, share, and watch short videos.

38. (U) An estimated 170 million Americans use TikTok monthly.

39. (U) ByteDance Limited is a holding company founded in 2012 and incorporated in the Cayman Islands, primarily operating out of offices in the PRC. ByteDance owns or controls several subsidiary and affiliated entities that, collectively, play various roles in operating Douyin, the version of the TikTok application that exists within China.

40. (U) ByteDance also owns TikTok Limited, an entity also registered in the Cayman Islands and primarily operating out of offices in the PRC. TikTok Limited owns or controls various subsidiary and affiliated entities that collectively operate the TikTok application throughout the world outside China.

41. (U) Among the TikTok subsidiaries and affiliates owned or controlled by TikTok Limited is TikTok LLC, a Delaware limited liability company based in California.

42. (U) TikTok Inc. operates the TikTok application in the United States. TikTok Inc. is a wholly owned subsidiary of TikTok LLC.



[REDACTED]

43. (U) The predominant manner by which users view content on TikTok is through the “For You Page.” This feed presents users with a practically endless stream of videos that are selected for users by ByteDance and TikTok’s proprietary content recommendation algorithm.

44. (U) When presented with a video on the For You Page, users may watch the video for as little or as long as they want. At any time, the user may scroll up to view the next video selected for them by the application’s algorithm. The user may also engage with the video by liking it, sharing it, commenting on it, or subscribing to its creator. TikTok offers users an option of viewing a feed composed of only videos from creators to which the user is subscribed.

45. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

46. (U) TikTok’s algorithm constantly updates its users’ preference profiles with more data collected through the application.

**(U) Risks Of PRC-Directed Censorship and Algorithmic Manipulation**

47. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

48. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

49. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

50. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

51. (U) Nonetheless, the Intelligence Community’s concern is grounded in the actions ByteDance and TikTok have already taken overseas, and in the PRC’s malign activities in the United States that, while not reliant on ByteDance and TikTok to date, demonstrate its capability and intent to engage in malign foreign influence and theft of sensitive data.

***(U) ByteDance and TikTok’s History of Censorship and Content Manipulation at PRC Direction***

52. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

a. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

b. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

c. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

53.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

a.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

b.

[REDACTED]

[REDACTED]

[REDACTED]

54. (U) Intelligence reporting further demonstrates that ByteDance and TikTok

Global have taken action in response to PRC demands to censor content *outside* of China.

a.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

b. [REDACTED]

[REDACTED]

55. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

56. [REDACTED]

[REDACTED]

[REDACTED]

a. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[Redacted]

b. [Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

57. [Redacted]

[Redacted]

[Redacted]

a. [Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

b. [Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[REDACTED]

c. [REDACTED]

[REDACTED]

[REDACTED]

58. (U) In sum, ByteDance and TikTok Global have a demonstrated history of manipulating the content on their platforms, including at the direction of the PRC.

[REDACTED]

59. [REDACTED]

[REDACTED]

60. [REDACTED]

[REDACTED]

[REDACTED]

a. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

b. [REDACTED]

[REDACTED]

61. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

62. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

63. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

64. (U) A recent December 2023 academic study using TikTok’s own data underscores the concern. *See A Tik-Tok-ing Timebomb: How TikTok’s Global Platform Anomalies Align with the Chinese Communist Party’s Geostrategic Objectives*, Network Contagion Research Institute (Dec. 2023). This study examined the volume of posts on TikTok containing certain hashtags and compared that to the number of posts with the same hashtags on Instagram. Based on the platform’s respective user base sizes, one would expect approximately

[REDACTED]



[REDACTED]

1.5 to 2 times more posts on Instagram with each hashtag, something that largely held true on average as to certain pop culture hashtags. But the study detected sizable anomalies in the prevalence of both pro- and anti-Chinese Communist Party narratives when compared to Instagram, with topics in line with Chinese Communist Party priorities having outsized prevalence on TikTok and posts on sensitive topics being far less prevalent than expected. For example, various Uyghur-related and Tibet-related hashtags appeared approximately 11 times and 37 times more on Instagram, respectively, than TikTok.

65.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

66. (U) Notably, the study writers report that TikTok eliminated the research mechanism underlying this study shortly after it was published. Specifically, the writers indicate the elimination of certain search capabilities to analyze hashtag trends on TikTok, including the elimination of trend data on all China-sensitive hashtags that the researchers relied on. The company did not publicize this action.

67.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

***(U) If the PRC Directed ByteDance or TikTok US to Censor Content or Manipulate Its Algorithm, The Firms Would Likely Comply***

68. (U) As discussed above, the PRC has a strong interest in manipulating the American information space and a demonstrated history of successfully tasking ByteDance and TikTok Global to censor discourse on their platforms outside of the United States.

69. (U) We believe ByteDance and TikTok similarly would try to comply if the PRC asked for specific actions to be taken to manipulate content for censorship, propaganda, or other malign purposes on TikTok US. As currently structured, ByteDance could accomplish the PRC's goals either by acting unilaterally to manipulate the platform or by compelling the cooperation of TikTok US.

70. [REDACTED]

[REDACTED]

[REDACTED]

71. (U) ByteDance is subject to the National Security Law of the PRC, which imposes broad obligations on citizens and corporations to assist and cooperate with the Chinese government in protecting what it broadly defines as national security. Among other things, the law requires Chinese citizens and organizations to comply with relevant PRC departments to assist national security efforts. Furthermore, the law prohibits those who comply with the PRC's requests from disclosing such cooperation publicly.

72. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

73. (U) The PRC can also leverage the Chinese Communist Party committee embedded in ByteDance to exert its will on the company. ByteDance has a Communist Party committee that, as of 2022, was headed by the company’s chief editor and comprised at least 138 employees at its Beijing office, including senior company managers. Party Committees—which are legally required for domestic firms and many foreign firms operating in China—are grassroots units of the party responsible for advancing party priorities and ideology, but the committees also have become involved in business decisions. Since 2020, some Party Committees in private firms, including multinational firms, have pushed to put party members on their boards and have influenced hiring decisions, despite Chinese government officials’ claims that the cells serve a primarily social function.

74. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

75.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

76. (U) To begin, the content recommendation algorithm at the core of the TikTok application—and thus TikTok’s success—resides within China and is largely maintained and controlled by ByteDance. This fact alone provides ByteDance with extremely powerful leverage over TikTok US.

77.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

78. (U) Altogether, TikTok US is heavily reliant on its corporate parent in numerous ways—operational and technological. Despite TikTok’s efforts to publicly distance itself from the PRC, the PRC is well-positioned to maintain some degree of access or influence over TikTok in the future. As a prominent example, Chinese law prohibits the export of the TikTok application’s source code, including to the United States, without government authorization (which is unlikely).

[REDACTED]

[REDACTED]

79.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

80. (U) In conclusion, TikTok poses a potential risk of serving as a powerful tool of information operations that could be used by an adversary, China, with a demonstrated commitment to shaping the information landscape in this country and around the world.

[REDACTED]

81.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

82.

[REDACTED]

[REDACTED]

[REDACTED]

83.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

84. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

85. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

86. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

4

87.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

88.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

---

[REDACTED]

4

[REDACTED]

[REDACTED]

89.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

a.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

b. (U) In 2024, former TikTok employees told Western media outlets that TikTok Global employees share U.S. user data on PRC-based internal communication systems that China-based ByteDance employees can access, and that TikTok US also approved sending U.S. data to China several times.

c.

[REDACTED]

[REDACTED]

d.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]



[REDACTED]

90.

[REDACTED]

[REDACTED]

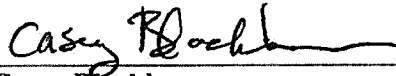
91.

[REDACTED]

[REDACTED]

Pursuant to 28 U.S.C. § 1746, I declare under penalty of perjury that the foregoing is true and correct.

Executed on July 26, 2024



Casey Blackburn  
Director  
Office of Economic Security and Emerging Technologies  
Assistant Director of National Intelligence  
Office of the Director of National Intelligence

[REDACTED]

**UNITED STATES COURT OF APPEALS  
FOR THE DISTRICT OF COLUMBIA CIRCUIT**

TIKTOK INC., *et al.*,  
*Petitioners,*

v.

MERRICK B. GARLAND, in his official capacity  
as Attorney General of the United States,  
*Respondent.*

Case No. 24-1113, 24-1130, 24-1183

**FILED IN CAMERA, EX PARTE,  
AND UNDER SEAL**

**(U) IN CAMERA, EX PARTE DECLARATION OF  
KEVIN VORNDRAN, ASSISTANT DIRECTOR,  
COUNTERINTELLIGENCE DIVISION,  
FEDERAL BUREAU OF INVESTIGATION**

(U) I, Kevin Vorndran, hereby declare the following:

1. (U) I am the Assistant Director, Counterintelligence Division, Federal Bureau of Investigation (FBI), United States Department of Justice (DOJ), a component of an Executive Department of the United States Government. I am responsible for, among other things, directing the conduct of the FBI's counterintelligence investigations. As Assistant Director, I have official supervision and control over the files and records of the Counterintelligence Division, FBI, Washington, D.C.

2. (U) In the course of my official duties at the FBI, I have been advised of these lawsuits and the allegations at issue in the above-captioned Petitions for Review. I understand that TikTok Inc. (TikTok US),<sup>1</sup> ByteDance Ltd. (ByteDance), and several TikTok application users filed

<sup>1</sup> In general, I use the term "TikTok" in this declaration to broadly refer to the worldwide TikTok entities and TikTok application. Where relevant, I use the more specific term "TikTok US" to

Petitions for Review of Constitutionality of the Protecting Americans from Foreign Adversary Controlled Applications Act. The matters stated herein are based on my personal knowledge, my review and consideration of documents and information made available to me in my official capacity, and on information furnished to me by Special Agents, Intelligence Analysts, and other employees of the FBI and the DOJ. My conclusions have been reached in accordance therewith.

3. (U) My declaration complements declarations provided by other agencies in support of the government's defense in this matter. This includes the Declaration of David Newman (Department of Justice, National Security Division) and the Declaration of Casey Blackburn (Office of the Director of National Intelligence). I make this declaration in support of the U.S. government's responses to the Petitions.

4. (U) This Declaration specifically addresses Hybrid Commercial Threats; risks posed by TikTok; limitations in the FBI's ability to monitor and investigate TikTok and its operations; and the FBI's role in the Committee on Foreign Investment in the United States mitigation monitoring.

5. (U) This declaration contains classified national security information under Executive Order 13526, *Classified National Security Information*, 75 Fed. Reg. 707 (Dec. 29, 2009), and applicable regulations. Consistent with those authorities, the unauthorized disclosure of the information discussed herein could cause serious, or in some cases exceptionally grave, damage to U.S. national security, as well as damage to intelligence sources and methods. As a result, I am submitting this declaration solely for the Court's *in camera*, *ex parte* review.

---

refer to the U.S.-based entity that operates the TikTok application within the United States. And I use the term "TikTok Global" to refer to TikTok Limited and the constellation of other entities that own, operate, or otherwise control the TikTok application outside of the United States. Finally, I use the term "ByteDance" to refer to that entity in its capacity both as TikTok's parent and as the operator of Douyin, the Chinese version of the TikTok application.

**(U) Hybrid Commercial Threats**

6. (U) Hybrid Commercial Threats are businesses whose legitimate commercial activity can facilitate foreign government access to U.S. data, critical infrastructure, and emerging technologies that enable adversaries to conduct espionage, technology transfer, data collection, and other disruptive activities under the guise of an otherwise legitimate commercial activity. Hybrid Commercial Threats are a global phenomenon that allow foreign governments—and the PRC in particular—to take advantage of legitimate business operations and leverage commercial access to pursue strategic national goals.



10. (U) The PRC's ability to exploit Hybrid Commercial Threats stems from a fundamental asymmetry between the relationships such U.S.-based subsidiaries have with the PRC and the U.S. government, respectively. U.S. subsidiaries of Chinese parent corporations remain subject to PRC jurisdiction and laws, which are outlined in paragraphs 16-25 of the Declaration of David Newman

(Newman Decl.). In exerting control over Chinese parent companies through formal legal means and, more frequently, the informal business culture that surrounds the PRC's legal framework, the PRC can access information from and about U.S. subsidiaries and compel their cooperation with PRC directives. In contrast, in the United States, U.S. subsidiaries are generally treated as U.S. persons and afforded robust legal and constitutional protections.

12. (U) Because Chinese laws enable the PRC to exert control over Chinese companies' U.S. subsidiaries, *see* Newman Decl. ¶¶ 16-25, the PRC has and can benefit from those companies' commercial successes as the Chinese government can leverage its legal regime and other tools to co-opt those companies for geopolitical gain. The use of prepositioning is a part of the PRC's broader geopolitical and long-term strategy to undermine U.S. national security. The PRC's prepositioning tactics can occur over the span of several years of planning and implementation. For example, the PRC, via its investment in Hybrid Commercial Threats in the emerging technology sector, has assumed leadership roles and active participation in international standards organizations.

14. (U) I am also aware of public reporting that Chinese hackers have considered exploiting U.S. legal protections for their own gain. In March 2021, a Microsoft executive noted in a U.S. press interview that the Chinese actors behind the 2021 Microsoft Exchange breach "apparently spent the

time to research the legal authorities and recognized that if they could operate from inside the United States, it takes some of the government's best threat-hunters off the field."

**(U) Risks Posed by TikTok**

15. (U) I am aware that ByteDance is a limited liability company based in Beijing, China, and that ByteDance is the parent company of TikTok Global and its U.S. subsidiary, TikTok US.

17. (U) While many of the TikTok application's functions and data collection practices are used for legitimate commercial purposes, those same functions and practices can also be used at the PRC's direction in ways that threaten U.S. national security.

18. (U) The FBI assesses ByteDance and TikTok could facilitate the PRC's access to U.S. users' data, which could enable PRC espionage, technology transfer, data collection, and influence activities.

19. (U) The following three examples illustrate how otherwise legitimate commercial activities can be used to harm the United States' national security.

20. (U) First, I am aware that TikTok US requests access to its millions of American user's contact list upon installation of the application (app) on the user's phone. I am aware that TikTok uses contact list information for legitimate business purposes, such as suggesting contacts to follow on the app.

21. (U) However, the FBI assesses this information can also be used for illegitimate and malign purposes.

22. (U) Once a user approves, the TikTok app has access to any data stored in the user's contact list, from names and contact information to job titles, contact photos, and notes. TikTok also periodically syncs contact lists, obtaining any updated and new information in user's contact lists.

[REDACTED]

This gives TikTok access to extensive information about users and non-users, including U.S. Government and U.S. intelligence community employees, U.S. political dissidents, and other individuals of interest to the PRC.

[REDACTED]

24. (U) Modern software applications can parse, centralize, and aggregate even disparate data that can facilitate targeting and operational activities.

[REDACTED]

27. (U) Second, TikTok US can access its users' physical locations through geolocation data.

I am aware that TikTok US can use users' geolocations for legitimate commercial purposes, such as targeting advertisements or content to TikTok US users.

28. (U) However, the PRC could also require ByteDance to share this data, which the PRC can use to locate, track, or monitor targeted persons.

29. (U) I am aware of reporting that ByteDance has improperly used TikTok US's geolocation data as a surveillance tactic in the past. I am aware that in October 2020, Forbes reported that ByteDance employees used IP address locations to track multiple journalists covering the company.

30. (U) Third, I am aware that TikTok's recommendation algorithm is used for legitimate business purposes to promote and demote certain content, such as showing users videos consistent with their interests or promoting advertising content.

31. (U) However, the FBI assesses TikTok's algorithm can also be used for illegitimate and malign purposes, posing risks to U.S. national security.

32. (U) For example, the PRC's artificial intelligence capabilities are greatly enhanced by the collection of U.S. person data, which could include users' data collected by TikTok. The FBI assesses that the PRC could use its AI capabilities to augment its influence campaigns, such as amplifying preexisting social divisions, and targeting U.S. audiences through TikTok's algorithm by promoting and suppressing particular videos. The FBI assesses that this would occur covertly, with little, if any, outward sign of PRC control.

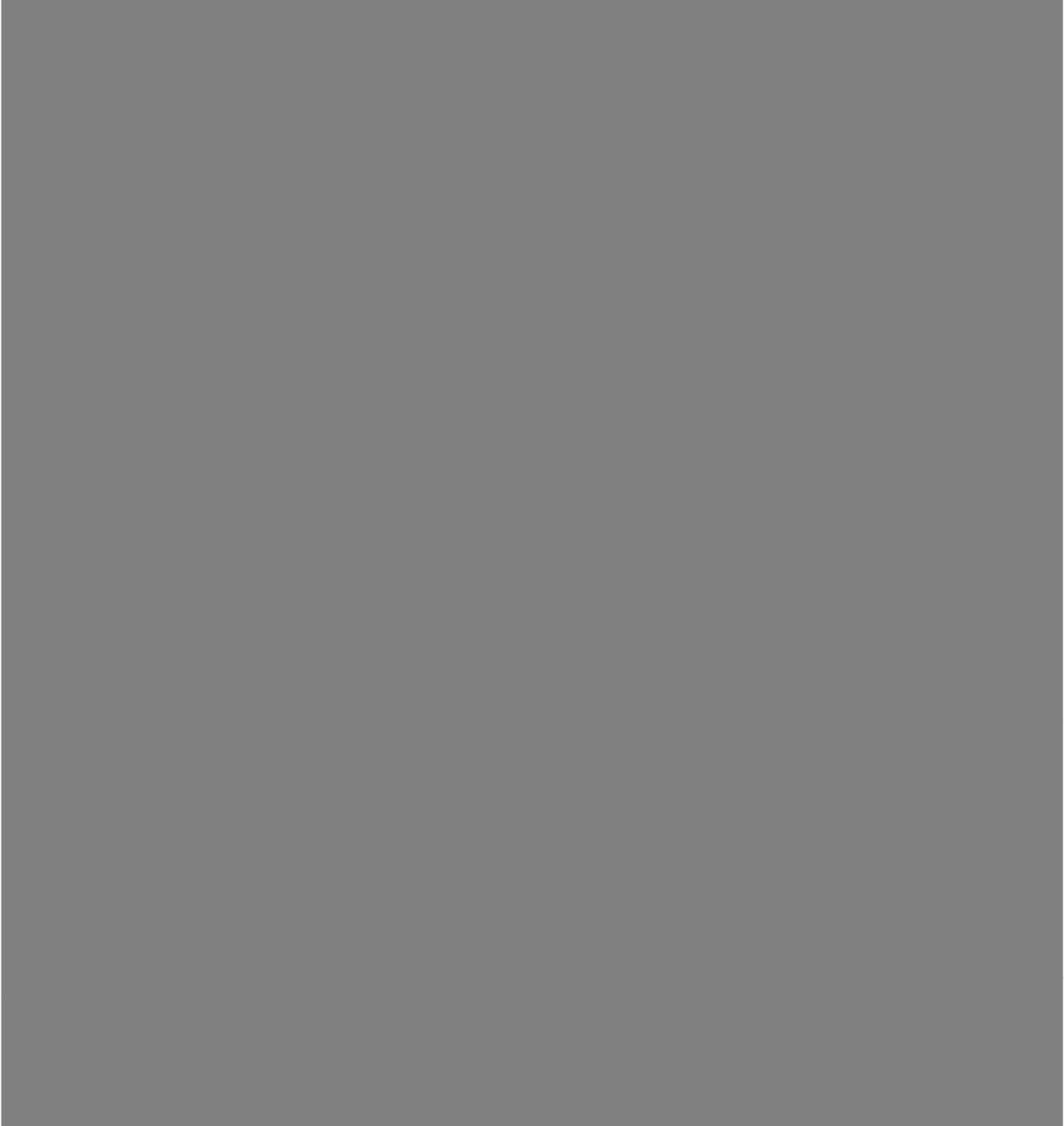


33. (U) Similarly, the PRC has exerted control over the content shown on other ByteDance-managed apps and has reprimanded ByteDance when its apps showed content inconsistent with PRC socialist values. For example, in April 2018, China's State Administration of Radio and Television publicly chastised ByteDance for hosting vulgar and insensitive content on two of its social media apps, Neihan Duanzi and Toutiao, and temporarily ordered their removal from app stores in China. In response, ByteDance discontinued Neihan Duanzi altogether and ByteDance's Founder and then-CEO, Zhang Yiming, issued a public apology for failing to acknowledge that "technology must be led by the socialist core value system." Zhang further pledged to "deepen cooperation with authoritative media" and "elevate distribution of authoritative media content." ByteDance announced plans to educate its employees about socialist core values and committed to hiring 4,000 additional employees to monitor and censor content, also calling upon PRC government representatives to supervise ByteDance's platforms.

**(U) Limitations to FBI's Ability to Monitor and Investigate TikTok**

34. (U) There are several challenges that the FBI faces in monitoring and investigating TikTok. One challenge is if a seemingly legitimate commercial activity is being used for illegitimate national security purposes, this would be difficult—if not impossible—to detect, both by TikTok users and by law enforcement personnel. The Chinese government can, in secret, compel or coerce ByteDance to share TikTok's data or utilize the TikTok application to harm the national security interests of the United States.

36. (U) It is difficult for the FBI to assess whether the algorithmic outputs, which display videos to users, are the result of a legitimate commercial algorithmic input or the result of covert malicious algorithmic input at the direction of the PRC.



**(U) FBI's Role in the Committee on Foreign Investment in the United States Mitigation Monitoring**

41. (U) In addition to providing timely intelligence and analysis to the Committee on Foreign Investment in the United States (CFIUS), the FBI's Foreign Investment Unit provides mitigation monitoring support to CFIUS Monitoring Agencies in three key areas.

42. (U/ ) First, in support of a CFIUS derived National Security Agreement (NSA) or Letter of Assurance, a CFIUS Monitoring Agency may request a vendor or person name check (name check) related to the parties of the CFIUS transaction. In this case, the FBI typically conducts an (1) open source review, (2) criminal background check, (3) internal FBI file review and in transactions that are co-lead by DOJ (4) other government databases. The FBI provides their findings back to the CFIUS Monitoring Agency for their assessment and suitability determination.

43. (U/ ) Second, at the request of the CFIUS Monitoring Agencies, the FBI may provide operational and/or intelligence support to CFIUS Monitoring Agency led site visits of parties under an existing NSA or Letter of Assurance. Typically, FBI support to a site visit may include (1) conducting a threat briefing on a certain topic (e.g., threats from foreign cyber actors), (2) providing subject matter expertise opinions, or (3) acting in a liaison capacity with the parties. Additionally, FBI's Foreign Investment Unit may leverage its U.S. based field offices and/or international based offices to provide support to a site visit within their area of responsibility.

44. (U/ [REDACTED]) Third, in limited situations, a CFIUS transaction may touch upon law enforcement equities, to include DOJ and/or the FBI. In these situations, the FBI may provide subject matter expertise to the CFIUS Monitoring Agencies in order to draft an NSA and/or Letter of Assurance that attempts to protect the identified equities.

45. (U) If the CFIUS Monitoring Agencies identify a violation of an NSA, the FBI could review any information or materials required by the NSA. Depending on the extent of the violation, the FBI could also seek to further investigate using legally appropriate law enforcement authorities.

46. (U) The FBI does not independently monitor compliance with CFIUS NSAs. It does not have agents or analysts devoted to monitoring these agreements and instead would only get involved when one of the co-lead agencies seeks FBI review.

47. (U) Any previous, current, or future investigations of TikTok on national security or criminal matters would be unrelated to monitoring of a potential NSA. The FBI would require sufficient information regarding potential violations of an NSA by monitoring agencies to determine whether it would have the predication to open an investigation on the matter.

#### Conclusion





Pursuant to 28 U.S.C. § 1746, I declare under penalty of perjury that the foregoing is true and correct.

Executed on July 25, 2024



---

**Kevin Vorndran**  
Assistant Director  
Counterintelligence Division  
Federal Bureau of Investigation

UNITED STATES COURT OF APPEALS  
FOR THE DISTRICT OF COLUMBIA CIRCUIT

TIKTOK INC., *et al.*,  
*Petitioners,*

v.

MERRICK B. GARLAND, in his official capacity  
as Attorney General of the United States,  
*Respondent.*

Case No. 24-1113, 24-1130, 24-1183

**FILED *IN CAMERA*, *EX PARTE*,  
AND UNDER SEAL**

**(U) *IN CAMERA*, *EX PARTE* CLASSIFIED DECLARATION OF DAVID NEWMAN,  
PRINCIPAL DEPUTY ASSISTANT ATTORNEY GENERAL, NATIONAL SECURITY  
DIVISION, DEPARTMENT OF JUSTICE**

(U) I, David Newman, declare as follows:

1. (U) I am the Principal Deputy Assistant Attorney General of the National Security Division (“NSD”) of the Department of Justice (“DOJ”). I have held this position since October 2022 after previously serving as Associate Deputy Attorney General (for National Security Affairs) between January 2021 and October 2022. Earlier in my career, I served in various roles on the National Security Council staff, as Special Assistant to the President and Associate White House Counsel in the Office of the White House Counsel, and as a career attorney in the DOJ’s National Security Division.

2. (U) In my current role as the second-highest ranking official in the DOJ’s National Security Division, I regularly lead and supervise all aspects of the National Security Division’s work, including overseeing investigations and prosecutions involving espionage,

1

Classified By: Newman David NSD USA GOV

terrorism, national security cyber threats, sanctions and export control violations, and foreign malign influence. In addition, I supervise and am regularly engaged in the work of the National Security Division's Foreign Investment Review Section ("FIRS"). I also regularly serve as DOJ's lead representative at the Assistant Secretary-level meetings of the Committee on Foreign Investment in the United States.

3. (U) In the course of my official duties in NSD, I am familiar with the petitions filed in the D.C. Circuit challenging the Protecting Americans from Foreign Adversary Controlled Applications Act, Pub. L. No. 118-50, Div. H (April 24, 2024) ("Act") and of the allegations at issue in those cases. The statements made in this declaration are based on my personal knowledge, as well as on information provided to me in my official capacity (including about time periods predating my current tenure at DOJ), and on my personal evaluation of that information.

4. (U) My declaration complements declarations provided by other federal agencies in support of the government's position in these cases. Those declarations include the Declaration of Casey Blackburn, Office of the Director of National Intelligence ("ODNI"); and the Declaration of Kevin Vorndran, Federal Bureau of Investigation ("FBI"). I make this declaration in support of the government's responses to the Petitions.

5. (U) My declaration describes the following topics: (1) background on TikTok and ByteDance; (2) the formal legal regime and informal practices applicable to private enterprise in the People's Republic of China ("PRC"); (3) a review, investigation, and presidential referral by the Committee on Foreign Investment in the United States ("CFIUS" or "Committee") of ByteDance Ltd.'s ("ByteDance") 2017 acquisition of the social media application Musical.ly; (4) subsequent Presidential orders against TikTok under the Defense



Production Act (“DPA”) and International Emergency Economic Powers Act (“IEEPA”) and litigation stemming therefrom; (5) the subsequent negotiations between the Executive Branch<sup>1</sup> and ByteDance<sup>2</sup>; (6) ByteDance’s final proposal<sup>3</sup> to mitigate the national security risk posed by the continued operation of the TikTok platform in the United States; (7) the fundamental inadequacies of that proposal in addressing national security risks; (8) further discussions between the Executive Branch and ByteDance; (9) additional information about TikTok & ByteDance practices; and (10) the parallel legislative efforts by Congress (including briefings in which I participated) to address similar risks to national security posed by TikTok.

6. (U) In brief, over the course of my tenure at the Department, I have observed and been personally involved in the Executive Branch’s good faith negotiations with ByteDance to reach an agreement to address the national security risks posed by TikTok’s operation in the United States under Chinese ownership. Notwithstanding such extensive negotiations, the Executive Branch was ultimately unable to reach a national security agreement with ByteDance because senior Executive Branch officials concluded that the terms of ByteDance’s final proposal would not sufficiently ameliorate those risks. Specifically, Byte Dance was unwilling

---

<sup>1</sup> (U) My references in this declaration to the “Executive Branch” denote the officials charged with negotiating with ByteDance to address the national security risks posed by the TikTok platform’s operation in the United States, as described in detail below.

<sup>2</sup> (U) For simplicity, I refer to ByteDance and TikTok US collectively as “ByteDance” in the context of the Executive Branch’s negotiations with both companies.

<sup>3</sup> (U) In its Petition, TikTok refers to portions of this proposal as “Project Texas.” Because “Project Texas” was ByteDance’s public label for a voluntary effort of ByteDance’s own making and does not appear to capture the full set of risk mitigation measures that ByteDance proposed to the Executive Branch and that was carefully evaluated by the Executive Branch, I will not use the term “Project Texas” in this declaration to avoid any confusion.

to agree to a proposal that would adequately mitigate the risks of (1) PRC access to sensitive U.S. user data and (2) the PRC's ability to drive state-sponsored malign narratives without public visibility into their role in promoting such narratives. In its Petition, ByteDance claims that the agreement it had put forward during the negotiations would have been sufficient because it would have made a "Trusted Technology Partner," Oracle, the guarantor of ByteDance's compliance. As described below, however, the proposed role for Oracle under ByteDance's proposal would not have resolved the Executive Branch's national security concerns because, among other things, the proposed agreement contemplated extensive data flows of U.S. users back to ByteDance and thus to China and because the agreement sought to maintain extensive engagement between TikTok's U.S. operations and the leadership at ByteDance.

7. (U) Furthermore, the Executive Branch review found that the only feasible way to resolve these national security concerns was for ByteDance to divest TikTok's operations in the United States in favor of a more trusted owner, severing the link between Beijing and the U.S. platform.

8. (U) This declaration contains classified national security information under Executive Order 13526, *Classified National Security Information*, 75 Fed. Reg. 707 (Dec. 29, 2009), and applicable regulations. Consistent with those authorities, the unauthorized disclosure of the information discussed herein could cause serious, or in some cases exceptionally grave, damage to U.S. national security, as well as damage to intelligence sources and methods. As a result, I am submitting this declaration solely for the Court's *in camera*, *ex parte* review.

**(U) Background: TikTok and ByteDance**

9. (U) ByteDance Ltd. is a privately-owned Cayman Islands company founded by PRC nationals with headquarters in Beijing, China, founded in 2012 by PRC national Yiming

Zhang. ByteDance develops machine learning-driven mobile applications, and offers a variety of mobile applications through both in-house development and acquisitions that broadly fall into two categories: (1) news aggregation platforms and (2) entertainment video sharing platforms.

10. (U) In September 2016, ByteDance launched Douyin—an entertainment video-sharing app—in China; in May 2017, the company launched the TikTok platform, a counterpart to Douyin for the global, non-Chinese market.

11. (U) Upon its launch, in May 2017, the TikTok platform operated under one of ByteDance’s Chinese subsidiaries, Beijing Shaking Youth Technology Co., Ltd., but around October 2017 ByteDance moved the principal offices of the TikTok platform—and the related User Data—from China to Singapore, and ByteDance subsidiary TikTok Pte. Ltd. then served as the TikTok platform’s operator.

12. (U) ByteDance controls the wholly owned subsidiary TikTok Ltd., which is responsible for operating the TikTok platform globally. Through TikTok Ltd., ByteDance also controls TikTok, Inc., a company with operations in Singapore and the United States and which operates the TikTok platform.<sup>4</sup>

13. (U) TikTok United States Data Security (“TTUSDS”) is a Delaware corporation, formed in May 2022, and is a wholly owned subsidiary of TikTok, Inc.

14. (U) Musical.ly was a social media application on which users could create, share, and watch short-form videos.

---

<sup>4</sup> (U) In general, I use the term “TikTok” in this declaration to broadly refer to the worldwide TikTok entities and the TikTok application. Where relevant, I use the more specific term “TikTok US” to refer to the U.S.-based entity that operates the TikTok application within the United States. I use the term “TikTok platform” to refer to the application (on iOS, Android, and computer operating systems) and that application’s underlying software.

15. (U) The TikTok platform is predominantly a mobile application (also accessible via a computer internet browser, through which its users access it) that permits users to create, view, and share videos. TikTok's success rests in large part on its proprietary algorithm, owned by ByteDance and engineered and stored in the PRC, which drives the platform's Recommendation Engine. The Recommendation Engine, and beneath it the algorithm, rely on TikTok's Source Code to function. ByteDance frequently updates the Source Code.

***(U) The Formal Legal Regime and Informal Norms Applicable to Private Enterprise in the PRC***

16. (U) China has enacted the world's most comprehensive set of laws, regulations, and national plans to broadly define its national and public security interests in data and to govern data collection, sales, sharing, and storage. This regime provides the PRC with broad control of large datasets hosted in China—controlled by both Chinese and non-Chinese companies—allowing it to restrict and suppress data that it deems could harm its national security or benefit international competitors.

17. (U) Because of the authoritarian structures and laws of the PRC regime, Chinese companies lack meaningful independence from the PRC's agenda and objectives. As a result, even putatively "private" companies based in China do not operate with independence from the government and cannot be analogized to private companies in the United States.

18. (U) I am aware that the PRC's legal code contains several laws that, in concert, allow the Chinese government to access sensitive personal data possessed by Chinese companies. These laws include the National Security Law, the Cybersecurity Law, the Anti-Terrorism Law, the National Intelligence Law, and the Counter-Espionage Law.

19. (U) *The National Security Law of the People's Republic of China* (promulgated by the Standing Committee of the National People's Congress, July 1, 2015, effective July 1,

2015) (attached hereto as Exhibit A) imposes broad obligations on corporations as well as citizens to assist and cooperate with the Chinese government in protecting what it defines as national security. China's National Security Law broadly defines national security as "the state where the country's political power, sovereignty, unity and territorial integrity, people's well-being, sustainable economic and social development, and other major national interests are relatively free from danger and internal and external threats" and "the ability to maintain a continuous state of security." *Id.* art. 2. Under the law, tasks to preserve national security include "maintain[ing] the socialist system with Chinese characteristics," "strengthen[ing] mechanisms for restricting and supervising the exercise of power," "control[ing] the ideological field," and "enhanc[ing] overall cultural strength and competitiveness." *Id.* arts. 15, 23. The law also imposes duties on citizens and Chinese organizations, including obligations to promptly report any clues and provide evidence of any activities endangering national security and to assist military agencies and relevant departments with national security efforts. *Id.* arts. 54, 77; *see also id.* art. 11.

20. (U) *The Cybersecurity Law of the People's Republic of China* (promulgated by the Standing Committee of the National People's Congress, Nov. 7, 2016, effective June 1, 2017) (attached hereto as Exhibit B) requires Chinese companies<sup>5</sup> to store their data within China, *id.* art. 37, to cooperate with crime and security investigations, *id.* arts. 28, 49, and to allow full access to data to Chinese authorities, *id.* arts. 9, 28, 49. The law was developed, in part, to "promote the healthy development of economic and social informatization." *Id.* art. 1.

---

<sup>5</sup> (U) The Law applies to "the construction, operation, maintenance, and use of networks, as well as the supervision and management of cybersecurity within" China. *Cybersecurity Law of the People's Republic of China, supra* ¶ 20, art 2.

The law requires network operators to, among other things, “respect social morals” and “accept supervision from the government.” *Id.* art. 9.

21. (U) *The Anti-Terrorism Law of the People’s Republic of China* (promulgated by the Standing Committee of the National People’s Congress, Dec. 27, 2015, effective January 1, 2016, amended Apr. 27, 2018) (attached hereto as Exhibit C) authorizes the government to conduct “terrorism” investigations and requires individuals and organizations to comply, in secret, with such investigations. The law defines “terrorism” as “propositions and actions that . . . create social panic, endanger public safety, infringe on personal and property rights, or coerce state organs or international organization to achieve their political, ideological, and other objectives.” *Id.* art. 3. The law authorizes “electronic monitoring” and “irregular inspections.” *Id.* art. 53. All organizations and individual have “the obligation to assist and cooperate with relevant departments in anti-terrorism work.” *Id.* art. 9.

22. (U) *The National Intelligence Law of the People’s Republic of China* (promulgated by the Standing Committee of the National People’s Congress, June 27, 2017, effective June 28, 2017, amended Apr. 27, 2018) (attached hereto as Exhibit D) also required companies to share information with the PRC. *Id.* art. 7. The law also authorizes “national intelligence work agencies” to use any “necessary methods, means, and channels” to carry out “intelligence work both domestically and abroad,” *id.* art. 10, including by establishing “cooperative relationships with relevant individuals and organizations” and “entrust[ing] them with related tasks, *id.* art. 12.

23. (U) *The Counter-Espionage Law of the People’s Republic of China* (promulgated by the Standing Committee of the National People’s Congress, Nov. 1, 2014, amended Apr. 26, 2023, effective July 1, 2023) (attached hereto as Exhibit E) authorizes “national security agency

staff” to “enter restricted areas, locations, and units,” *id.* art. 43 and to “inspect the electronic devices, facilities, and relevant procedures and tools of concerned individuals and organizations,” *id.* art. 25. The Law requires “citizens and organizations” to “support and assist” such efforts. *Id.* art. 8.

24. (U) Significantly, these laws contain provisions that prohibit individuals and organizations from revealing when and if the Chinese government has requested any assistance or information from them. *See* National Security Law of the People’s Republic of China, *supra* ¶ 19, art. 77; Cybersecurity Law of the People’s Republic of China, *supra* ¶ 20, art. 47; Anti-Terrorism Law of the People’s Republic of China, *supra* ¶ 21, art. 48; National Intelligence Law of the People’s Republic of China, *supra* ¶ 22, art. 7; Counter-Espionage Law of the People’s Republic of China, *supra* ¶ 23, art. 8.

25. (U) Through these comprehensive laws, the PRC effectively blurs the line between the private and public sector, in a way that is very different from the way private companies in the United States operate.

**(U) CFIUS Review, Investigation, & Presidential Referral of ByteDance’s Acquisition of Musical.ly**

26. (U) As detailed below, I have been advised and am aware that prior to my current tenure at DOJ, the Committee on Foreign Investment in the United States (“CFIUS” or “Committee”) reviewed, investigated, and ultimately referred to the then-President the 2017 acquisition by ByteDance of the social media platform Musical.ly.

***(U) ByteDance’s Acquisition of Musical.ly***

27. (U) On November 23, 2017, a subsidiary of ByteDance acquired Musical.ly (the “Transaction”).

28. (U) In August 2018, ByteDance re-launched the TikTok platform in the United States, converting most of the Musical.ly users into TikTok users.

**(U) CFIUS Review**

29. (U) On October 15, 2019, CFIUS sent an extensive questionnaire to ByteDance in furtherance of evaluating whether CFIUS had national security concerns relating to the Transaction and potential authority to review it.

30. (U) On November 12, 2019 and March 27, 2020, CFIUS and ByteDance held two meetings to discuss CFIUS's concerns regarding the Transaction.

31. (U) On May 27, 2020, at CFIUS's request, ByteDance filed a Joint Voluntary Notice regarding the Transaction with CFIUS, pursuant to 31 C.F.R. § 800.501.

32. (U) On June 16, 2020, CFIUS began a 45-day formal review of ByteDance's acquisition of Musical.ly pursuant to 31 C.F.R. § 800.503(b). As part of the ensuing consultative process between CFIUS and ByteDance, the company submitted two mitigation proposals on July 15, 2020 and July 29, 2020.

33. (U) During this time, CFIUS agencies had extensive internal discussions about the size, scope, and potential mitigation of the national security risk identified by the Committee.

**(U) CFIUS Investigation**

34. (U) On July 30, 2020, at the close of its formal review, CFIUS sent a letter informing ByteDance that the Committee would initiate a 45-day investigation of the Transaction pursuant to 31 C.F.R. § 800.505. CFIUS explained that ByteDance's two mitigation proposals were insufficient to address the national security risk CFIUS had identified. The letter also informed ByteDance that the Committee anticipated referring the Transaction to the



President for decision, but invited ByteDance to submit additional information for CFIUS's consideration.

**(U) Presidential Referral**

35. (U) At the conclusion of its investigation, CFIUS's view remained that ByteDance's mitigation proposals were insufficient to address the national security threat posed by the TikTok platform's operation in the United States. Accordingly, CFIUS referred the Transaction to the President for action on August 1, 2020. CFIUS's referral to the President marked the conclusion of the CFIUS's action vis-à-vis the Transaction. *See* 50 U.S.C. § 4565(l)(2). This referral to the President "complete[d] the action of [CFIUS]," *see id.*, with respect to the ByteDance-Musical.ly transaction, meaning that future interactions between the Executive Branch and ByteDance were not subject to CFIUS's statutory procedures (including, for example, the confidentiality protections at 50 U.S.C. § 4565(c)).

**(U) CFIUS Divestment Order and Prohibitions Under the International Emergency Economic Powers Act; Subsequent Litigation**

36. (U) On August 14, 2020, the President took action under 50 U.S.C. § 4565(d) by issuing an order requiring ByteDance to divest all interests and rights in property used to enable or support its operation of TikTok in the United States, and to divest all interests and rights in any data obtained or derived from users of the TikTok platform or Musical.ly in the United States ("Divestment Order"). *Regarding the Acquisition of Musical.ly by ByteDance Ltd.*, 85 Fed. Reg. 51,297 (Aug. 14, 2020).

37. (U) The CFIUS Divestment Order was issued soon after the publication of an August 6, 2020 Presidential order under IEEPA (50 U.S.C. §§ 1701 et seq.) ("IEEPA Order") prohibiting certain transactions in the United States involving ByteDance and TikTok, and

authorizing the Department of Commerce to promulgate rules and regulations to implement the order.

38. (U) ByteDance and other parties sought to enjoin the IEEPA Order in several federal district courts. Three of those courts enjoined the Department of Commerce from implementing the IEEPA Order, holding that the Order exceeded the President's authority under IEEPA.

39. (U) ByteDance also filed a petition for review of the Divestment Order in the United States Court of Appeals for the District of Columbia Circuit on November 10, 2020.

40. (U) The parties jointly moved to place the D.C. Circuit litigation in abeyance while they engaged in the negotiations described below. The government did not enforce the order pending those negotiations. On February 19, 2021, the D.C. Circuit placed the case in abeyance. Since that date, the parties have filed joint status reports every 60 days, and the matter remains administratively stayed.

**(U) Negotiations to Address National Security Risk**

41. (U) After the Divestment Order, ByteDance and TikTok offered further mitigation proposals in an effort to address the Executive Branch's national security concerns and had multiple discussions with Executive Branch agencies. ByteDance and TikTok submitted to Executive Branch agencies a "National Security Agreement/Term Sheet" on November 6, 2020, which for the first time identified a potential restructuring to create a new potential entity under ByteDance and TikTok responsible for trust and safety in the United States.

42. (U) TikTok sent an updated mitigation proposal to the Executive Branch on January 4, 2021, thus renewing negotiations to potentially resolve identified national security risks.

43. (U) Following a Presidential transition in January 2021, the leadership at DOJ and at other Executive Branch Departments and Agencies undertook their own intensive evaluation of the risk presented by TikTok's operation in the United States, as well as of the adequacy of potential mitigation and remedial options available.

44. (U) Notwithstanding demands associated with a global pandemic and Presidential transition, Executive Branch personnel in 2021 and 2022 reviewed dozens of proposed draft mitigation terms and held a series of meetings on this topic with both the parties and within the Executive Branch. These discussions frequently included extensive discussions driven by subject matter experts in data storage, source code and software review, content review, lawful process, content moderation, and trust and safety.

45. (U) Over a two-year period from 2020 to 2022, in conjunction with their negotiations with ByteDance, Executive Branch negotiators engaged in extensive, in-depth discussions with Oracle, the proposed Trusted Technology Provider, whose responsibility under the proposed mitigation structure included storing data in the United States, performing source code review, and ensuring safety of the operation of the TikTok platform in the United States.

46. (U) The length of these negotiations reflected both the complexity of the task and the iterative nature of the negotiation process. The Executive Branch's discussions with ByteDance and TikTok personnel and counsel, as well its discussions with the proposed Trusted Technology Provider, would sometimes result in new or revised proposed mitigation measures that, in turn, required additional Executive Branch review and discussion, often involving personnel with highly technical backgrounds and expertise.

47. (U) In total, Executive Branch negotiators conducted dozens of meetings and video conferences and exchanged scores of drafts of proposed mitigation terms. Throughout

these negotiations, the Executive Branch continued meeting internally to evaluate the national security risk, analyze the parties' proposals to address the risk, and determine whether the proposals would be effective and monitorable.

48. (U) Executive Branch negotiators conducted the negotiations with TikTok and ByteDance in good faith, expending significant time and attention to achieve a mutually acceptable national security agreement that would resolve the U.S. government's national security concerns without the need for contested litigation or the enactment of new legislation. ByteDance's willingness to make certain concessions over the lifetime of those negotiations supplied a basis for the Executive Branch to continue to believe that the negotiations could ultimately succeed. As a senior DOJ official, I received repeated briefings on the status and progress of these negotiations as did other senior officials across the Executive Branch. It was well understood by those involved in the negotiations that any agreement would require review and approval at very senior levels of the Executive Branch before it could take effect.

**(U) ByteDance's Proposal**

49. (U) On August 23, 2022, TikTok submitted to the Executive Branch what the company portrayed as final proposed national security agreement ("Final Proposed NSA"), which represented the culmination of years of negotiations and discussions, following significant analysis by TikTok, presumptively ByteDance (or entities representing ByteDance's interests), and the Executive Branch. The Executive Branch extensively reviewed the Final Proposed NSA to determine whether the terms would sufficiently address the identified national security risks.

50. (U) As elaborated in greater detail below, the Final Proposed NSA would have made several organizational and technical changes affecting the operation of the TikTok platform in the United States<sup>6</sup>:

**(U) Proposed Measures to Achieve Operational Independence for TikTok USDS**

51. (U) The Final Proposed NSA purported to introduce operational independence from the decisional influence of TikTok US. and ByteDance for personnel managing operation of the TikTok platform<sup>7</sup> in the United States, under the auspices of the newly created TTUSDS.

52. (U) Article III of the Final Proposed NSA specified that TTUSDS's Board would consist of three directors, none with ByteDance or TikTok US. affiliations, to be approved by the Executive Branch, with ostensibly no duty to report to TikTok US. or to ByteDance.

53. (U) Article V of the Final Proposed NSA specified that key management personnel at TTUSDS would be subject to Executive Branch approval, and that all personnel could only be hired subject to Executive Branch approval that ensured new employees had no prior relationship with ByteDance.

54. (U) TTUSDS would have been responsible for the following functions, among others:

- a. (U) Overall compliance with the Final Proposed NSA;
- b. (U) Oversight over the storage and protection of Protected Data, including all data that TTUSDS maintained on U.S. persons; and

---

<sup>6</sup> (U) ByteDance has voluntarily implemented some components of the Final Proposed NSA, although the agreement was never signed.

<sup>7</sup> (U) Petitioners refer to relevant operations of the TikTok platform as "CFIUS functions." *See, e.g.,* Simkins Decl. ¶ 53.

c. (U) Day-to-day operations of the TikTok platform in the United States.

55. (U) The composition of the TikTok US. board of directors would change. Under the Final Proposed NSA, the board of TikTok US would have five members—two from ByteDance, two outside directors (citizens of the United States, Australia, Canada, New Zealand, or the United Kingdom), and the chair of TTUSDS.

**(U) Proposed Data Protection Measures**

56. (U) The Final Proposed NSA purported to offer certain protections for U.S. users' data.

57. (U) Article XI of the Final Proposed NSA would have established three tiers of data: Protected Data, Excepted Data, and Public Data.

58. (U) "Protected Data" would have included "any data collected from a TikTok U.S. user," but excluded data whose sharing was authorized by users of the TikTok platform who affirmatively chose to share more data with TTUSDS.

59. (U) Protected Data would be stored in the United States in a "cloud" storage facility operated by Oracle Corporation.

60. (U) Protected Data stored overseas would be deleted.

61. (U) Protected Data would be deleted no later than 18 months after creation.

62. (U) ByteDance's access to Protected Data would purportedly be limited to certain scenarios that would have been identified in advance, such as sharing IP addresses to mitigate a global cybersecurity incident.

**(U) Proposed Third-Party Oversight Mechanisms**

63. (U) The Final Proposed NSA purported to introduce trusted third-party oversight of operation of the TikTok platform in the United States.

64. (U) Under Articles XIII and IX of the Final Proposed NSA, a “Trusted Technology Partner” (also referred to as a “TTP”) would be appointed, with the consent of the U.S. government, to support TTUSDS in the performance of its functions and purportedly to verify its compliance with its obligations under the Final Proposed NSA. TikTok indicated they continued to contemplate Oracle Corporation would serve as the TTP, at least at the outset.

- a. (U) Personnel hired by the TTP would be subject to the same limitations applicable to TTUSDS staff.
- b. (U) The TTP would manage the storage of Protected Data.
- c. (U) The TTP would be responsible for initially inspecting, and monitoring changes to, Source Code developed by ByteDance.
- d. (U) The TTP would regularly report to the U.S. government on TTUSDS’s compliance with the Final Proposed NSA.

65. (U) Additional third-party monitoring would have taken place, facilitated by the TTP, through a Third-Party Monitor, a Third-Party Auditor, and a Cybersecurity Auditor.

***(U) Proposed Source Code Inspection and Verification Measures***

66. (U) The Final Proposed NSA purported to guarantee the safety of the TikTok platform’s Source Code.

67. (U) Article IX of the Final Proposed NSA would have permitted the TTP, as well as a Source Code Inspector, to inspect the TikTok platform’s Source Code.

68. (U) All Source Code for the TikTok platform in the United States would be stored in TTP servers in the United States.

69. (U) Updates and changes to the Source Code from ByteDance would be pushed to Dedicated Transparency Centers operated by the TTP, where they would not be synched with the TikTok platform in the United States until the TTP had reviewed the changes.

**(U) *Proposed Additional Compliance Measures***

70. (U) The Final Proposed NSA contemplated various compliance measures.

71. (U) In particular, under Article XXI of the Final Proposed NSA, the U.S. government would have had the authority under the Final Proposed NSA to instruct the TTP to stop permitting downloads of, and updates to, the TikTok platform in the United States. TikTok has referred to this as the “kill switch.”

72. (U) The Final Proposed NSA would have allowed the U.S. government to impose monetary penalties for noncompliance.

**(U) Insufficiencies of TikTok’s Proposal**

73. (U) Between August 2022 and February 2023, the Executive Branch scrutinized, evaluated, and discussed the Final Proposed NSA, including through a robust interagency process with substantial, personal involvement at senior levels of the Executive Branch.

a. (U) During the Executive Branch’s internal deliberations concerning the Final Proposed NSA, the Executive did not stop engaging with ByteDance.

b. (U) To the contrary, the period between August 2022 and February 2023 saw numerous communications between the two sides, including multiple requests by the Executive Branch for additional written updates and answers to follow-up questions.



[REDACTED]

74. (U) Though the Executive Branch and ByteDance made progress in their negotiations, culminating in the Final Proposed NSA, the resulting proposal did not mitigate the risks posed to U.S. national security interests to a degree acceptable to the Executive Branch.

75. (U) Most fundamentally, the Final Proposed NSA still permitted certain data of U.S. users to flow to China, still permitted ByteDance executives to exert leadership control and direction over TikTok's US operations, and still contemplated extensive contacts between the executives responsible for the TikTok U.S. platform and ByteDance leadership overseas. Moreover, the Final Proposed NSA would ultimately have relied on the Executive Branch trusting ByteDance to make day-to-day business decisions that enforce the mitigation measures even as the Executive Branch lacked the resources and capabilities to fully monitor and verify ByteDance's compliance with the Final Proposed NSA. For the reasons described below, this model was deemed to pose an unacceptable risk of national security harm.

**(U) *Lack of Visibility into PRC Activity or Influence***

76. (U) Certain inherent features of the PRC, ByteDance and the TikTok platform would have greatly inhibited the U.S. government's ability to detect violations of the Final Proposed NSA.

77. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

78. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- a. (U) *Data*. The flow of U.S. user data into TTUSDS's servers, and from there to other locations, would not be subject to direct U.S. government monitoring under the Final Proposed NSA. Moreover, PRC-based companies like ByteDance are compelled to cooperate with PRC law enforcement requests and are prohibited from disclosing that cooperation. *See* Blackburn Decl. ¶ 71. Even absent a formal request from the PRC, it is inherent in the nature of a commercial hybrid threat that ByteDance would cooperate with PRC efforts to obtain U.S. user data, with the U.S. government none the wiser.
- b. (U) *Limitations of Source Code Analysis*. Even assuming every line of Source Code could be monitored and verified by the TTP, the PRC could exert malign influence through the very same features that have made the TikTok platform globally successful. For example, the TikTok platform includes a feature known as "heating," by which employees may manually boost certain content for viewing on users' For You Pages. Users cannot see that a video has been "heated" when they view it. Heating is useful from a commercial perspective, as it enables TikTok to curate popular content and disseminate that content widely on the platform, potentially increasing user engagement and increasing the value

[REDACTED]

of advertising it sells. But it may also be used to drive views of content of the PRC's choosing. A review of the Source Code, in other words, would not and could not satisfy that the platform's features would be used for benign commercial ends, not malicious ones, thus inhibiting the government from detecting noncompliance with the Final Proposed NSA.

c. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- d. (U) *Content: Outputs.* The outputs of a Recommendation Engine influenced by the PRC are superficially indistinguishable from what would appear on the TikTok platform in the absence of malign influence. For example, in the event of a global conflict involving a foreign adversary that invades an ally of the United States, videos criticizing the United States' relationship with the ally might appear to users because they are organically popular among Americans, because they are deemed newsworthy by TikTok's content curators, or because the PRC directed TTUSDS (through ByteDance) to make those videos appear more frequently. The Executive Branch thus would have limited means of observing and verifying with certainty such manipulation by the PRC.

**(U) *Additional Challenges for Monitoring Compliance***

79. (U) Because of the size and technical complexity of the TikTok platform and its underlying software, attempting to ensure ByteDance's, TikTok US.'s, and TTUSDS's

compliance with the Final Proposed NSA would require resources far beyond what the U.S. government and Oracle possess.

80. (U) *Source Code Review Limitations.* Though varying over time, ByteDance's representations as to the size of the TikTok platform's Source Code leave no doubt that a complete review of each line would be a monumental undertaking. Most recently, ByteDance represented to the Executive Branch in 2022 that the Source Code contained 2 billion lines of code. For comparison, the Zoom application contains 10 million lines of code, and Windows Operating System contains approximately 50 million. Even if static, Oracle estimated it would require three years to review this body of code. But the Source Code is not static; ByteDance regularly updates it to add and modify TikTok's features. Even with Oracle's considerable resources, perfect review would be an impossibility.

81. (U) *Data Limitations.* While the Final Proposed NSA theoretically envisioned robust protections for Protected Data, it also specified that Protected Data could and would be transmitted to the PRC at regular intervals to update the Source Code. This included data from content creators operating on the TikTok platform, data necessary for business metrics, engineering data, interoperability data, E-Commerce data, and data to identify whether a user should be protected as a U.S. user. Oracle's role as TTP was insufficient to prevent this harm because it would rely on precision in source code review and access controls that were by definition incomplete, with significant volumes of excepted information able to travel to the PRC for engineering and commercial reasons.

82. (U) As a result, NSD assessed that even under the Final Proposed NSA, such transmissions would expose U.S. users' data to malign purposes.

[REDACTED]

*(U) Inability of Executive Branch or Third Parties to Verify Compliance*

83.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

84.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

8

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

85. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- a. (U) First, the Trusted Technology Provider would be faced with the challenge of the massive scale of data that could be transported back to Beijing for ostensibly legitimate purposes. The TTP would be required to sift through such data, using both untested and experimental tools to try to ascertain whether information was routed for legitimate commercial reasons or nefarious reasons at the request of PRC actors.
- b. (U) Second, the TTP and others faced a challenge with the scope of data, as the Final Proposed NSA was designed so that ByteDance and its engineers would continue to have access to data for some purposes and would continue to be involved in engineering, source code and algorithm development, code testing, and user testing. The TTP and other independent monitors and auditors would

[REDACTED]

have theoretically been able to see that data left the U.S. storage regime to go back to ByteDance, but those independent monitors and auditors would have no way (that the Executive Branch is aware of) to be able to distinguish legitimate transfers of U.S. person data from nefarious transfers of U.S. person data.

- c. (U) Third, these private parties also lack insight into ByteDance's communications with PRC officials, ByteDance's use of U.S. user data, and ByteDance's other TikTok-related activities. The Executive Branch thus determined that the Final Proposed NSA presented too great a risk because the TTP and other monitors faced massive scope and scale hurdles that could not be overcome.

**(U) *Lack of Trust***

86. (U) In the absence of sufficient visibility and resources to monitor the agreement, the government's confidence in the agreement's efficacy would necessarily require a significant level of trust that ByteDance and TTUSDS would comply in good faith with the agreement. In the Executive Branch's assessment, the requisite trust did not exist. As a result, the entire framework of the Final Proposed NSA presented an unacceptable challenge to the Executive Branch: a potential agreement with a party that it did not trust, and a lack of confidence that it had either the resources or capability to catch violations.

87. (U) To be effective, verifiable, and enforceable in the real world, an agreement to mitigate national-security risks involving the private sector requires a baseline level of trust between the U.S. Government and the parties. The sensitive technologies, data, and other assets that are vulnerable to exploitation by foreign adversaries (and that form the basis of any risk) are in the private sector outside of the U.S. Government's direct control and oversight. On a day-to-

[REDACTED]

day basis, the U.S. Government must rely on the mitigation parties to be the gatekeepers of those assets and must trust that they will make business decisions that enforce, rather than undermine, the measures that mitigate the national-security risks. Without that baseline level of trust, the U.S. Government lacks the confidence that the oversight mechanisms to monitor compliance would be adequate to detect efforts to violate mitigation measures, either through the parties' intentional actions or through their failure to report actions by state-sponsored actors with whom the companies have relevant ties.

88.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

89. (U) Similarly, in the context of mitigation agreements under the Foreign Ownership, Control, or Influence ("FOCI") regulations of the Department of Defense's Defense Counterintelligence and Security Agency ("DCSA"), the Department of Defense enters into mitigation agreements only with companies it assesses are motivated to comply solely by

[REDACTED]



[REDACTED]

business incentives: retaining their U.S. Government contracts in order to maximize profits. For these businesses, maximizing profit is their primary motivation, and failure to comply with a FOCI mitigation agreement exposes them to losing significant profits from classified contracts. On the other hand, for companies that are controlled by a hostile foreign power seeking to penetrate the United States, national objectives may outweigh business incentives. This is true even for otherwise legitimate companies.

90. (U) Likewise, the Department of Justice, Department of Homeland Security, Department of Defense, and other agencies, in their roles as members of CFIUS, enter mitigation agreements only where there is a baseline level of trust that enables the mitigation agreements to be monitorable, verifiable, and enforcement.

91. (U) The Executive Branch concluded that ByteDance lacked the baseline trust required of parties to mitigation agreements.

92. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

93. (U) In my recent experience, these concerns have been particularly difficult to overcome in cases where the company is part of a rapidly evolving industry where the risks are multi-vector (as opposed to limited-vector risks like those involving physical access to a tangible item or facility), and the mitigation measures would have to exist in perpetuity (meaning, they would not ultimately result in the divestment of the equity or the cessation of the mitigation regime). Those risk factors are further heightened risk where, as here, the PRC and companies like ByteDance and TikTok can exercise influence through soft power, frequently in person, that is inherently difficult to monitor.

94. (U) In addition, while mitigation measures could keep ByteDance at least one step removed from the TTUSDS Board, ByteDance would still be an essential member for any quorum of the TikTok US Board, have rights to be a member of all committees designated by the TikTok US Board, and have to vote in the affirmative for TikTok to take certain actions. Only a divestment can wholly eliminate ByteDance and TikTok's presence and capability to wield influence on the U.S. companies' boards of directors.

95. (U) The vignettes outlined below illustrate why the Executive Branch felt it could not trust ByteDance.

- a. (U) Public reporting by Forbes Magazine indicates that ByteDance employees abused U.S. user data, even after the establishment of TTUSDS. Moreover, the audio recordings of ByteDance meetings obtained by Forbes indicate that ByteDance retained considerable control and influence over TTUSDS operations.

- [REDACTED]
- b. (U) As made public in a June 18, 2024 statement, the Federal Trade Commission (“FTC”) referred a complaint against TikTok and ByteDance to the Department of Justice for violations of the Children’s Online Privacy Protection Act (“COPPA”), despite a 2019 settlement between FTC and ByteDance. ByteDance’s failure to adhere to that settlement cast doubt on its future compliance with the Final Proposed NSA.
  - c. (U) As described in paragraphs 16-18 above, Chinese law would obligate ByteDance to cooperate with PRC efforts to obtain personal data or drive propaganda narratives. ByteDance’s susceptibility to the influence of that legal system caused the Executive Branch to doubt that, if forced to choose between compliance with PRC law and with the Final Proposed NSA, it would be faithful to its obligations under the Final Proposed NSA. Moreover, as noted, the Executive Branch would have limited visibility into such cooperation.
  - d. (U) Also, even under the Final Proposed NSA, ByteDance would have retained significant presence and representation on the ByteDance board, and the TikTok US board, rendering those individuals susceptible to the influence described above.
  - e. (U) On April 18, 2018, in response to PRC concerns about violating PRC content guidelines, the founder of TikTok publicly pledged to increase the number of censors from 6,000 to 10,000, while creating a blacklist of banned users and developing better technology to boost censorship. As part of the pledge, Zhang stated “[w]e didn’t realize that technology has to be guided by the core values of

socialism so it can be used to spread positive energy, meet the requirements of the times and respect public order and good customs.”

**(U) *Insufficient Operational Independence***

96. (U) TTUSDS would have remained a wholly owned subsidiary of TikTok US ByteDance communicated to the Executive Branch that they envisioned frequent meetings between TTUSDS and TikTok US to ensure TTUSDS’s continued alignment with the global TikTok platform.

97. (U) Despite the Final Proposed NSA’s contemplation of U.S. Government approval for TTUSDS’s choices of vendors, negotiators for ByteDance expressed ByteDance’s intention that employees of TTUSDS would continue to use certain ByteDance products, such as Lark (a ByteDance proprietary platform for in-office communications), which collected and stored large amounts of personal data.

98. (U) The 2022 incident involving ByteDance’s tracking of journalists, as reported by Forbes Magazine in December 2022, only heightened the Executive Branch’s longstanding concerns surrounding a continuing role for ByteDance in TTUSDS’s operations, despite the latter’s nominal independence. TTUSDS was formed in May 2022. Later that same year, according to Forbes, four internal auditors at ByteDance were fired for improperly tracking journalists’ IP addresses. Aside from the concerns raised by the behavior of those employees vis-à-vis journalists, the episode highlights that ByteDance’s own staff continued to have significant levels of access, and participated to a large degree, in TTUSDS’s operations. Even today, I understand that audits of TTUSDS are conducted in the PRC, not the United States.

99. (U) Although the Final Proposed NSA had not been signed, and therefore ByteDance was under no obligation to the U.S. government to guarantee TTUSDS’s operational

[REDACTED]

independence, this vignette gave the Executive Branch additional reason to doubt the true independence TTUSDS would possess under the Final Proposed NSA, if enacted.

a. (U) First, the same data flow and access to and from the PRC seemed to exist both pre-execution and contemplated post-execution.

b. [REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

c. (U) Third, the structure would nevertheless still rely on ByteDance engineers in the PRC developing and deploying the Source Code.

**(U) *Insufficient Data Protections: Anonymization***

100. (U) Although the Final Proposed NSA purported to anonymize some of the data to which ByteDance would continue to have access, the Executive Branch judged that this proposed anonymization was insufficient to mitigate the national-security risk that the PRC or ByteDance could exploit this data in ways that undermine U.S. national security.

101. (U) Open-source reporting has repeatedly raised concern that supposedly anonymized data is rarely, if ever, truly anonymous. As a recent study has explained, for example, “[a]ggregated insights from location data” could be used to damage national security—such as in 2018, when the publication of a global heatmap of anonymized users’ location data collected by a popular fitness app enabled researchers to quickly identify and map the locations of military and government facilities and activities. Similarly, in 2019, *New York Times* writers were able to combine a single set of bulk location data collected from cell phones and bought

[REDACTED]

[REDACTED]

and sold by location-data companies—which was anonymized and represented “just one slice of data, sourced from one company, focused on one city, covering less than one year”—with publicly available information to identify, track, and follow “military officials with security clearances as they drove home at night,” “law enforcement officers as they took their kids to school,” and “lawyers (and their guests) as they traveled from private jets to vacation properties.” A 2019 research study concluded that “99.98% of Americans would be correctly re-identified in any dataset using 15 demographic attributes,” thus “suggest[ing] that even heavily sampled anonymized datasets are unlikely to satisfy the modern standards for anonymization set forth by [the European Union’s General Data Protection Regime] and seriously challenge the technical and legal adequacy of the de-identification release-and-forget model.” Other studies and reports have reported similar results.

102. [REDACTED]

[REDACTED]

103. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

104. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

105. (U) Adversaries can use these datasets to reverse-engineer anonymized data and identify people, subjects, or devices that were supposedly anonymized.

106. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

**(U) *Insufficient Data Protections: Data Security***

107. (U) The Final Proposed NSA would have continued to allow ByteDance, and even PRC, access to Protected Data. The Final Proposed NSA describes the situations in which ByteDance would be permitted to access such data as “Limited Access Protocols.” Despite this innocuous name, the Protocols envisioned ByteDance access to data in a wide range of scenarios. These include validating user regions for proper routing, threats of harm to employees, bots and other malicious accounts associated with hate groups, foreign influence campaigns, transnational organized crime, international fraud, emergency responses including terrorism, suicide attempts by a user, and for legal scenarios including eDiscovery, litigation, regulatory responses, and compliance investigations.

108. (U) Given the constraints identified in paragraph 77, *supra*, monitoring ByteDance’s compliance with the Protocols, and ensuring that Protected Data were accessed only for legitimate ends, would have been impossible.

109. (U) The treatment of Excepted Data represented a large loophole in the Final Proposed NSA’s data protection regime. Users could opt into their data being treated as Excepted, placing U.S. national security interests in private hands.

**(U) *Inadequate Remedies***

110. (U) The penalties for non-compliance would not have been sufficient to deter wrongdoers.

111. (U) The U.S. government’s ability to order the TTP to shutter the TikTok platform would not have been a realistic option to deter noncompliance with the Final Proposed NSA. Most centrally, its use would have required the government to know, in sufficient time to



act, of an imminent threat. For the monitoring reasons described above, that possibility was too remote.

112. (U) In the Executive Branch's estimation, monetary and criminal penalties would also have been insufficient to deter wrongdoers. The national security risk posed by TikTok's operation in the United States, detailed in the Declaration of Casey Blackburn, stems from the potential of direct PRC involvement in exploitation of personal data or manipulation of content.

113. (U) The Executive Branch assesses that agents of the PRC would not fear monetary or criminal penalties in the United States, and even if aware of pressure from the PRC government, TTUSDS personnel here would not resist demands to comply.

114. (U) The "kill switch" would not have been an adequate measure to address the national security risk.

- a. (U) ByteDance and TikTok reference a provision of the Final Proposed NSA that provided a "kill switch" to cut off access to the TikTok app. They claim that the kill switch would have addressed the government's national security concerns without the need for divestment.
- b. (U) The language of the Final Proposed NSA paints a different picture. The provision allowed for a "temporary stop" only for a specific list of narrowly scoped NSA violations. Most of those violations would have been overt and easily recognizable failures to implement provisions of the Final Proposed NSA, such as failing to set up the TikTok U.S. Data Security structure, failing to pay the TTP, preventing the TTP from inspecting the source code, or deploying source code that had not been reviewed. Other temporary stops would have relied on

[REDACTED]

notice from the TTP of some failure, such as failure to store data subject to the access controls proposed in the NSA.

c. (U) The temporary stop would not, however, give the U.S. Government anything resembling complete discretion to shut down the TikTok platform based on its own independent assessment of national security risk and assessments from the U.S. Intelligence Community. For example, the provision does not permit a temporary stop based on concerns related to the algorithm or whether U.S. persons' data is accessible by the PRC government. This provision, like the rest of the Final Proposed NSA, was premised on allowing some flows of U.S. user data back to ByteDance and China, and on allowing ByteDance to continue to be involved in the development and operation of the TikTok platform.

d. (U) The method for actually triggering the temporary stop also had several steps before the TikTok application would actually be stopped. At each point, ByteDance and TikTok could have litigated the application of the temporary stop, both formally and informally.

e. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- f. (U) The Executive Branch thus concluded that the so-called “kill switch” was insufficient to mitigate the national security risks.
- g. (U) All told, any national security agreement is signed with the understanding that some minor noncompliance may result. In this case, the risks were so large, so diffuse, and so unmonitorable that the Executive Branch concluded it could not approve the Final Proposed NSA.

115. (U) As a general matter, the Executive Branch concludes national security agreements in a wide range of contexts, to ameliorate diverse national security risks posed by a variety of private actors. The diversity, specificity, and context-dependency of these risks, alongside the statutory confidentiality obligations the Defense Production Act (under which CFIUS operates) imposes on the Executive Branch, make an apples-to-apples comparison as between the Final Proposed NSA and agreements the Executive Branch has found acceptable difficult to make. Even so, several features of national security agreements the Executive Branch has found acceptable in past CFIUS reviews are absent from the Final Proposed NSA, as elaborated below. For that reason, the risks presented by TikTok’s operation are qualitatively different from those addressed under other national security agreements the Executive Branch has found acceptable.

a. *(U) Absence of Bright-Line Measures to Reduce or Eliminate Risk.*

- i. (U) In the context of many other national security agreements, CFIUS is able to insist on bright-line, ascertainable steps to isolate the investment at issue from malign foreign influence. Suppose a PRC company invested in a U.S. business operating close to a sensitive military installation. To reduce the risk of malign PRC influence on the U.S. business’s operations,

CFIUS could insist that only non-PRC citizens enter the business's facility. It could require, through a national security agreement, certain physical and logical security measures consistent with the National Institute of Standards and Technology (e.g., that the facility have appropriate fences and barricades, that a trusted third-party operate a booth at the entrance, checking the identification of any person seeking to gain access to ensure compliance with the entry restriction).

- ii. (U) In an alternative scenario, suppose the same company was not located near a sensitive installation, but was exposed to certain categories of sensitive information. CFIUS could, through a national security agreement, require that the U.S. business limit access to certain facilities or equipment, and require that only certain personnel could access the information after being subjected to Executive Branch vetting.
- iii. (U) These bright-line restrictions—entry controls, information-sharing controls—would drastically reduce the national security risks stemming from the PRC company's investment in the U.S. business.
- iv. (U) The risks posed by the TikTok platform's continued operation in the United States stem from TikTok's (1) collection and possession of large amounts of U.S. user data; (2) the platform's algorithm; and (3) the company's susceptibility to PRC influence. The nature of these risks makes it impossible to impose bright-line restrictions of the type identified above. Indeed, the company would never agree (and in the negotiations described above, did not agree) to cease collecting U.S. user data or



- i. (U) The scope and scale of the risks posed by TikTok's continued operation in the United States under PRC ownership are qualitatively different from those addressed under national security agreements the Executive Branch has found acceptable, even if the risks addressed by the latter category remain substantial. The Executive Branch has never before sought to limit the data- and content-manipulation-related risks of an application with more than 170 million U.S. users. Non-compliance here, in other words, poses a risk of consequences of an entirely different magnitude than what the Executive Branch often contends in the CFIUS process.

**(U) 2022-2023 Negotiations Held by the Executive Branch and ByteDance**

116. (U) Between August 23, 2022, when ByteDance submitted the Final Proposed NSA to the Executive Branch, and March 6, 2023, when the Executive Branch informed ByteDance that the Final Proposed NSA insufficiently addressed the national security risks posed by the continued operation of TikTok in the United States while under ownership by a PRC company, extensive internal deliberations concerning the Final Proposed NSA's adequacy took place within the Executive Branch. During the same period, the Executive Branch continued to engage with ByteDance concerning its proposal. For example,

- a. (U) On September 3, 2022, representatives of the Department of Justice and Department of Treasury met with ByteDance to discuss Source Code and remedies.
- b. (U) On September 27, 2022, representatives of the Department of Justice discussed TikTok's Source Code with ByteDance's counsel and technical experts.

- [REDACTED]
- c. (U) On October 14, 2022, representatives of the Department of Justice and Department of Treasury corresponded with ByteDance concerning the Executive Branch's review of the Final Proposed NSA, and requesting various updates and materials, including drafts of annexes to the Final Proposed NSA that ByteDance had not provided. One week later, representatives of the Department of Treasury followed up on this request.
  - d. (U) On November 28, 2022, ByteDance requested a meeting to discuss the establishment of TTUSDS. Four days later, representatives from the Department of Treasury responded, indicating that the Final Proposed NSA remained under review within the Executive Branch.
  - e. (U) On January 9, 2023, the Executive Branch emailed ByteDance questions about recent news reporting concerning TikTok. ByteDance responded in two tranches on February 1, 2023 and February 10, 2023, respectively.

117. (U) On March 6, 2023, representatives of the Executive Branch met with ByteDance and TikTok US to inform them that the Final Proposed NSA did not sufficiently address national security risks stemming from the TikTok platform's continued operation in the United States under ByteDance's/TikTok US's ownership. During that discussion, I and other representatives of the Executive Branch made clear to counsel for TikTok that the only viable solution that had been identified by senior Executive Branch officials to resolve the national security concerns involved a divestment of TikTok's U.S. operations to a trusted buyer along with the migration of the source code and algorithm development outside China. That message was reiterated at a March 23, 2023 follow-up meeting.

118. (U) Following the March 2023 discussions between representatives of ByteDance, TikTok US, and the Executive Branch, representatives of the Executive Branch continued to meet with ByteDance but emphasized that the only resolution supported by Executive Branch leadership involved divestment. As recently as September 8, 2023, Executive Branch representatives (including technical experts and subject matter experts) met ByteDance and TikTok US personnel to discuss methods of divesting the source code from ByteDance control in the PRC. Despite considerable review and analysis, the discussions did not provide confidence that ByteDance was prepared to undertake divestment in a manner that would resolve Executive Branch concerns.

**(U) Additional Information about TikTok & ByteDance Practices**

119. (U) The Executive Branch's lack of trust in TikTok and its ability to comply with the strictures of a mitigation agreement—discussed above in paragraphs 86-95—was further reinforced by information gathered by law enforcement. For instance, I have reviewed reports of voluntary interviews of individuals with knowledge of TikTok's operations, who have stated, in sum and in substance, and in part, the following:

- a. (U) TikTok has used a web-suite system developed by ByteDance called Lark, also known as “Feishu,” which hosted TikTok's internal platforms and allowed TikTok employees to interface directly with engineers in China. Lark has served as the primary means by which ByteDance and TikTok employees communicated with one another.
- b. (U) Lark has operated on servers located in China.
- c. (U) TikTok employees have communicated with their co-workers on Lark, and, at various points in time, have sent significant amounts of restricted U.S. user data



(including but not limited to personally identifiable information) to each other through Lark channels to address various operations issues. This resulted in certain sensitive U.S. person data being contained in Lark channels and, therefore, stored on Chinese servers and accessible to ByteDance employees located in China.

- d. (U) TikTok, in or around 2022, created an internal project aimed at identifying and removing certain sensitive U.S. user data improperly maintained on Lark channels.
- e. (U) At least as of 2022, Lark contained multiple internal search tools that had been developed and run by China-based ByteDance engineers for scraping TikTok user data, including U.S. user data.
- f. (U) One of those tools allowed ByteDance and TikTok employees in the United States and China to collect bulk user information based on the user's content or expressions, including views on gun control, abortion, and religion.
- g. (U) Another tool contained policies that allowed both for the collection of bulk user information as well as the triggering of the suppression of content on the platform based on the user's use of certain words. Although this tool contained certain policies that only applied to users based in China, others such policies may have been used to apply to TikTok users outside of China.
- h. (U) TikTok, in or around 2022, was investigating the existence of these policies, and whether and under what circumstances they had ever been used in the United States.

**(U) Legislative Proposals; Briefings**

120. (U) I participated in a series of Congressional briefings related to TikTok and ByteDance in 2023 and 2024. The briefings were related to various legislative proposals Congress was considering to address legislative concerns about the risks posed by TikTok.

121. (U) Also participating in these Congressional proceedings were representatives from the FBI and ODNI. The hearings and briefings were classified, and were held in spaces that were accredited as Secure Compartmented Information Facilities (“SCIFs”), so that classified information could be discussed.

122. (U) The specific legislative proceedings at which I participated in 2024 included the following:

- a. (U) House Homeland Committee - Briefing held on February 15, 2024
  - b. (U) House Energy and Commerce Committee – Hearing held on March 7, 2024
  - c. (U) House All-Member Briefing – Briefing held on March 12, 2024
  - d. (U) Senate Staff for Members of the Commerce, Science, and Transportation Committee and Senate Select Committee on Intelligence – Briefing held on March 19, 2024
  - e. (U) Senate Commerce, Science, and Transportation Committee (CST) and Senate Select Committee on Intelligence (SSCI) – Briefing held on March 20, 2024
123. (U) I attended and actively participated in all of these sessions.

124. (U) I am familiar with the items I discussed, both as the representative for DOJ, as well as the information shared by my colleagues at FBI (which participated in most of the sessions) and ODNI (which participated in all of them).

[REDACTED]

125. (U) At a high level, the matters briefed to the Congressional members and staff in the proceedings listed above involved the following topics:

- a. (U) The threats posed by China, and the risks of actions adverse to U.S. national security.
- b. (U) The formal and informal methods of control the PRC exercises over corporations that do business in China.
- c. (U) The particulars of how the PRC exercises control over ByteDance.

d. [REDACTED]  
[REDACTED]  
[REDACTED]

126. (U) Members asked questions at these meetings. The questions ranged in topics but they generally related to:

- a. (U) the intelligence community's assessment of the risks posed by TikTok's continued operation in the United States;
- b. (U) gaps in the Intelligence Community's ability to collection information related to TikTok;
- c. (U) the mechanics of the Act; and
- d. (U) the legality of and anticipated legal challenges to the Act.

127. (U) I understand that transcripts have been prepared of the classified hearing and one of the classified briefings, described above in paragraphs 122(b) and 122(e), that the House and Senate held on the Act but that the remaining briefings were not transcribed.

128. (U) Although I along with limited other DOJ personnel were authorized to review the transcript of the March 20, 2024 Senate briefing, I understand that a full Senate vote is required before the transcript can be released to the Executive Branch.

Pursuant to 28 U.S.C. § 1746, I declare under penalty of perjury that the foregoing is true and correct.

Executed on July 26, 2024

*David Newman*

---

**David Newman**  
Principal Deputy Assistant Attorney General  
National Security Division  
Department of Justice

# EXHIBIT A

**Declaration of David Newman  
Principal Deputy Assistant Attorney General  
National Security Division  
Department of Justice**



---

# Certification of Translation

---



COUNTY OF SUFFOLK  
COMMONWEALTH OF MASSACHUSETTS

July 24, 2024

This is to certify that the attached translation is, to the best of my knowledge and belief, a true and accurate translation from Simplified Chinese into English of the attached document:

- **National Security Law**

Linguistic Systems, Inc. adheres to an ISO-certified quality management system that ensures best practices are always followed in the selection of linguists skilled in both the languages and subject matters necessary for every translation.



Linguistic Systems, Inc.



260 Franklin Street, Suite 230, Boston MA 02110 • Phone 617-528-7400 • Fax 617-528-7490 • [www.linguist.com](http://www.linguist.com)

Certifications: ISO 9001 • ISO 17100 • ISO 18587 • ISO 27001

# National Security Law of the People's Republic of China (Presidential Decree No. 29)

Central Government Portal Website: www.gov.cn Date: July 1, 2015, 21:59 Source: Xinhua News Agency  
[Font Size: Large Medium Small] Print this page  
Share

## Presidential Decree of the People's Republic of China No. 29

The National Security Law of the People's Republic of China has been adopted by the 15th meeting of the Standing Committee of the 12th National People's Congress on July 1, 2015. It is hereby promulgated and shall take effect from the date of publication.

President of the People's Republic of China: Xi Jinping

July 1, 2015

## **National Security Law of the People's Republic of China**

(Passed at the 15th meeting of the Standing Committee of the 12th National People's Congress on July 1, 2015)

Table of Contents

Chapter 1: General Provisions

Chapter 2: Tasks for Safeguarding National Security

Chapter 3: Responsibilities for Safeguarding National Security

Chapter 4: National Security System

Section 1: General Provisions

Section 2: Intelligence Information

Section 3: Risk Prevention, Assessment, and Warning

Section 4: Review and Supervision

Section 5: Crisis Management

Chapter 5: National Security Guarantee

Chapter 6: Obligations and Rights of Citizens and Organizations

## Chapter 7: Supplementary Provisions

### **Chapter 1: General Provisions**

Article 1: In order to safeguard national security, protect the people's democratic dictatorship and the socialist system with Chinese characteristics, protect the fundamental interests of the people, ensure the smooth progress of reform, opening up, and socialist modernization, and achieve the great rejuvenation of the Chinese nation, this law is formulated based on the Constitution.

Article 2: National security refers to the state where the country's political power, sovereignty, unity and territorial integrity, people's well-being, sustainable economic and social development, and other major national interests are relatively free from danger and internal and external threats, as well as the ability to maintain a continuous state of security.

Article 3: National security work should adhere to the overall national security concept, prioritize the security of the people, focus on political security, be based on economic security, and ensure security in military, cultural, and social aspects, while promoting international security. It should maintain national security in various fields, build a national security system, and follow the path of national security with Chinese characteristics.

Article 4: Adhere to the leadership of the Communist Party of China in national security work and establish a centralized, unified, efficient, and authoritative national security leadership system.

Article 5: The central national security leadership body is responsible for decision-making and coordination in national security work, researching and formulating, guiding the implementation of national security strategies and major policies, coordinating significant national security issues and important tasks, and promoting the rule of law in national security.

Article 6: The state formulates and continuously improves the national security strategy, comprehensively assesses international and domestic security situations, and defines the guiding principles, medium- and long-term goals, key areas of national security policies, work tasks, and measures.

Article 7: Safeguarding national security should comply with the Constitution and laws, adhere to the principle of socialist rule of law, respect and protect human rights, and lawfully protect the rights and freedoms of citizens.

Article 8: Safeguarding national security should be coordinated with economic and social



development.

National security work should integrate internal and external security, territorial and national security, traditional and non-traditional security, and self-security and common security.

Article 9: Safeguarding national security should prioritize prevention, adopt a comprehensive approach, combine specialized work with the mass line, fully utilize the functions of specialized and other relevant agencies in maintaining national security, and widely mobilize citizens and organizations to prevent, stop, and lawfully punish actions that endanger national security.

Article 10: Safeguarding national security should adhere to mutual trust, mutual benefit, equality, and cooperation. Actively engage in security exchanges and cooperation with foreign governments and international organizations, fulfill international security obligations, promote common security, and maintain world peace.

Article 11: Citizens of the People's Republic of China, all state organs and armed forces, political parties and people's organizations, enterprises and institutions, and other social organizations all have the responsibility and obligation to safeguard national security.

China's sovereignty and territorial integrity are inviolable and indivisible. Maintaining national sovereignty, unity, and territorial integrity is a common duty of all Chinese people, including compatriots in Hong Kong, Macau, and Taiwan.

Article 12: The state shall recognize and reward individuals and organizations that make outstanding contributions to safeguarding national security.

Article 13: State organ staff who abuse their power, neglect their duties, or engage in misconduct in national security work or activities related to national security shall be held legally accountable.

Any individual or organization that violates this law and other relevant laws, fails to fulfill their national security obligations, or engages in activities that endanger national security shall be held legally accountable.

Article 14: April 15 of each year is designated as National Security Education Day.

## **Chapter 2: Tasks for Safeguarding National Security**

Article 15: The state upholds the leadership of the Communist Party of China, maintains the socialist system with Chinese characteristics, develops socialist democratic politics, improves socialist rule of law, strengthens mechanisms for restricting and supervising the exercise of power, and ensures the rights of people to be the masters of their own country.

The state prevents, stops, and lawfully punishes acts of treason, separatism, incitement to rebellion, subversion, or incitement to subvert the people's democratic dictatorship; prevents, stops, and lawfully punishes acts that harm national security, such as theft or leakage of state secrets; and prevents, stops, and lawfully punishes infiltration, sabotage, subversion, and separatist activities by foreign forces.

Article 16: The state maintains and develops the fundamental interests of the broadest masses of people, protects people's safety, creates favorable conditions for survival and development, and ensures a stable environment for work and life. It safeguards citizens' life and property safety and other lawful rights and interests.

Article 17: The state strengthens border defense, maritime defense, and air defense construction, adopts all necessary defensive and control measures to protect land, internal waters, territorial seas, and airspace security, and maintains national territorial sovereignty and maritime rights and interests.

Article 18: The state strengthens the revolutionary, modernized, and standardized development of the armed forces, building military forces that meet the needs of safeguarding national security and development interests. It implements an active defense military strategy, defends against and resists aggression, prevents armed subversion and separatism; conducts international military security cooperation, including UN peacekeeping, international rescue, maritime escort, and military actions to protect national overseas interests, maintaining national sovereignty, security, territorial integrity, development interests, and world peace.

Article 19: The state upholds the basic economic system and socialist market economic order, improves the system and mechanisms for preventing and resolving economic security risks, and ensures the security of important industries, key sectors, major infrastructure projects, and other significant economic interests related to the lifeline of the national economy.

Article 20: The state improves macro-prudential management and financial risk prevention

and handling mechanisms, strengthens financial infrastructure and basic capabilities, prevents and resolves systemic and regional financial risks, and guards against external financial risk impacts.

Article 21: The state rationally utilizes and protects resources and energy, effectively manages the development of strategic resources and energy, strengthens strategic resource and energy reserves, improves strategic transportation channels and security measures for resources and energy, enhances international cooperation on resources and energy, and comprehensively improves emergency support capabilities to ensure a continuous, reliable, and effective supply of resources and energy needed for economic and social development.

Article 22: The state improves the food security guarantee system, protects and enhances comprehensive food production capacity, refines food reserve systems, circulation systems, and market regulation mechanisms, establishes a food security early warning system, and ensures food supply and quality safety.

Article 23: The state adheres to the direction of socialist advanced culture, inherits and promotes the excellent traditional culture of the Chinese nation, cultivates and practices socialist core values, prevents and resists the influence of harmful cultures, controls the ideological field, and enhances overall cultural strength and competitiveness.

Article 24: The state strengthens the ability to independently innovate, accelerates the development of controllable strategic high-tech and core technologies in important fields, enhances intellectual property rights protection and technology confidentiality capabilities, and ensures the safety of major technologies and projects.

Article 25: The state builds a network and information security guarantee system, improves network and information security protection capabilities, strengthens innovation research and development of network and information technologies, ensures the security and controllability of core technologies, key infrastructure, and important information systems and data; enhances network management, prevents, stops, and lawfully punishes network crimes such as attacks, intrusions, theft, and dissemination of illegal and harmful information, and maintains sovereignty, security, and development interests in cyberspace.

Article 26: The state adheres to and improves the system of regional ethnic autonomy, consolidates and develops equal, united, mutually supportive, and harmonious socialist ethnic relations. It upholds equality among all ethnic groups, strengthens ethnic exchanges, communication, and integration, prevents, stops, and lawfully punishes ethnic separatist activities, maintains national unity, ethnic solidarity, and social harmony, and promotes common unity, prosperity, and development among all ethnic groups.

Article 27: The state lawfully protects citizens' freedom of religious belief and normal religious activities, adheres to the principle of religious independence and self-management, prevents, stops, and lawfully punishes illegal activities that harm national security under the guise of religion, opposes foreign interference in domestic religious affairs, and maintains normal religious activity order.

The state lawfully bans cult organizations, prevents, stops, and lawfully punishes illegal activities related to cults.

Article 28: The state opposes all forms of terrorism and extremism, strengthens the capacity to prevent and deal with terrorism, conducts intelligence, investigation, prevention, handling, and fund supervision work in accordance with the law, bans terrorist organizations, and severely punishes violent terrorist activities.

Article 29: The state improves effective systems and mechanisms for preventing and resolving social conflicts, enhances the public safety system, actively prevents, reduces, and resolves social conflicts, properly handles public health, social safety, and other emergencies that affect national security and social stability, promotes social harmony, and maintains public safety and social stability.

Article 30: The state improves the ecological and environmental protection system, increases efforts for ecological construction and environmental protection, delineates ecological protection red lines, strengthens early warning and prevention of ecological risks, properly handles sudden environmental incidents, and ensures that natural environments and conditions essential for people's survival and development, such as air, water, and soil, are not threatened or damaged, promoting harmonious development between humans and nature.

Article 31: The state adheres to the peaceful use of nuclear energy and technology, strengthens international cooperation, prevents nuclear proliferation, improves non-proliferation mechanisms, enhances the safety management, supervision, and protection of nuclear facilities, materials, activities, and waste disposal, strengthens emergency systems and capabilities for nuclear accidents, prevents, controls, and eliminates hazards from nuclear accidents to citizens' health and the ecological environment, and continuously improves the ability to respond to and prevent nuclear threats and attacks.

Article 32: The state adheres to the peaceful exploration and utilization of outer space, the international seabed area, and polar regions, enhances the ability to safely enter and exit, conduct scientific research, and develop and utilize these areas, strengthens international cooperation, and protects the safety of China's activities, assets, and other interests in outer space, the international seabed area, and polar regions.

Article 33: The state takes necessary measures according to the law to protect the safety and legitimate rights and interests of Chinese citizens, organizations, and institutions overseas and to safeguard national overseas interests from threats and infringements.

Article 34: The state continuously improves tasks for maintaining national security based on economic and social development and national development interests.

### **Chapter 3: Responsibilities for Safeguarding National Security**

Article 35: The National People's Congress, in accordance with the Constitution, decides on matters of war and peace and exercises other constitutional powers related to national security.

The Standing Committee of the National People's Congress, in accordance with the Constitution, decides on the declaration of a state of war, decides on national or partial mobilization, decides on the declaration of a state of emergency nationwide or in specific provinces, autonomous regions, or municipalities directly under the central government, and exercises other constitutional powers and powers granted by the National People's Congress related to national security.

Article 36: The President of the People's Republic of China, based on the decisions of the National People's Congress and its Standing Committee, announces the state of emergency, declares a state of war, issues mobilization orders, and exercises other constitutional powers related to national security.

Article 37: The State Council, in accordance with the Constitution and laws, formulates administrative regulations related to national security, specifies relevant administrative measures, and issues

relevant decisions and orders; implements national security laws, regulations, and policies; decides, in accordance with the law, on the state of emergency in specific areas within provinces, autonomous regions, or municipalities directly under the central government; and exercises other powers related to national security granted by the Constitution, laws, and the National People's Congress and its Standing Committee.

Article 38: The Central Military Commission leads the national armed forces, decides on military strategies and combat policies, commands military actions to safeguard national security, formulates military regulations related to national security, and issues relevant decisions and orders.

Article 39: Various departments of central state organs, according to their duties, implement national security policies and laws, and manage and guide national security work in their respective systems and fields.

Article 40: People's Congresses at various local levels and the Standing Committees of People's Congresses at or above the county level ensure the observance and implementation of national security laws and regulations within their administrative regions.

Local people's governments at various levels manage national security work within their administrative regions according to laws and regulations.

The Hong Kong Special Administrative Region and the Macao Special Administrative Region shall fulfill their responsibilities for safeguarding national security.

Article 41: People's courts exercise judicial power in accordance with the law, and people's procuratorates exercise prosecutorial power in accordance with the law to punish crimes that harm national security.

Article 42: National security agencies and public security organs lawfully collect intelligence information related to national security, exercise investigation, detention, preliminary examination, arrest, and other legally prescribed powers in national security work.

Relevant military agencies exercise related powers in national security work according to the law.

Article 43: State organs and their staff, in performing their duties, shall adhere to the principle of safeguarding national security.

In national security work and activities related to national security, state organs and their staff must strictly perform their duties according to the law, must not exceed their powers, abuse their powers, or infringe upon the lawful rights and interests of individuals and organizations.

#### **Chapter 4: National Security System**

## Section 1: General Provisions

Article 44: The central national security leadership body shall implement a unified, coordinated, and efficient national security system and work mechanism.

Article 45: The state establishes a coordination mechanism for key areas of national security work to coordinate and promote relevant work by central functional departments.

Article 46: The state establishes a mechanism for supervising and inspecting national security work and for accountability to ensure the implementation of national security strategies and major deployments.

Article 47: Departments and regions should take effective measures to implement national security strategies.

Article 48: The state establishes a cross-departmental consultation mechanism for national security work to discuss and assess major issues related to national security and provide opinions and recommendations.

Article 49: The state establishes a collaborative mechanism for national security between central and local governments, between departments, between the military and civilian sectors, and between regions.

Article 50: The state establishes a national security decision-making consultation mechanism, organizing experts and relevant parties to analyze and assess the national security situation and promote scientific decision-making for national security.

## Section 2: Intelligence Information

Article 51: The state improves the system for collecting, analyzing, and using intelligence information, ensuring it is unified, responsive, accurate, efficient, and smooth, and establishes a coordination mechanism for intelligence information work to achieve timely collection, accurate analysis, effective use, and sharing of intelligence information.

Article 52: National security agencies, public security organs, and relevant military agencies, according to their responsibilities, collect intelligence information related to national security.

Departments of state organs should report relevant national security information obtained during their duties in a timely manner.

Article 53: Intelligence information work should make full use of modern scientific and technological means to enhance the identification, screening, integration, and analysis of intelligence information.

Article 54: The reporting of intelligence information should be timely, accurate, and objective, and must not be delayed, omitted, concealed, or falsified.

### Section 3: Risk Prevention, Assessment, and Warning

Article 55: The state formulates and improves contingency plans for national security risks in various fields.

Article 56: The state establishes a national security risk assessment mechanism, regularly conducts risk surveys and assessments in various fields.

Relevant departments should regularly submit national security risk assessment reports to the central national security leadership body.

Article 57: The state improves the national security risk monitoring and warning system, and issues appropriate risk warnings based on the level of national security risks.

Article 58: For events that may occur or have occurred that threaten national security, local governments at or above the county level and their relevant departments should report immediately to the higher-level government and its relevant departments, and may report directly to the higher levels if necessary.

### Section 4: Review and Supervision

Article 59: The state establishes a system and mechanism for national security review and supervision, conducting national security reviews of foreign investments, specific items and key technologies, network information technology products and services, construction projects related to national security, and other significant matters and activities to effectively prevent and mitigate national security risks.

Article 60: Departments of central state organs exercise national security review responsibilities according to laws and administrative regulations, make national security review decisions or provide review opinions, and supervise their implementation.

Article 61: Provinces, autonomous regions, and municipalities directly under the central government are responsible for national security review and supervision within their administrative regions according to the law.

### Section 5: Crisis Management

Article 62: The state establishes a unified leadership, coordinated, and efficient national security crisis management system.

Article 63: In the event of a major incident threatening national security, relevant central departments and local governments, according to the unified deployment of the central national



security leadership body, shall activate emergency plans and take control measures.

Article 64: In the event of a particularly serious incident threatening national security, if it requires the declaration of a state of emergency, state of war, or nationwide or partial mobilization, such decisions shall be made by the National People's Congress, the Standing Committee of the National People's Congress, or the State Council in accordance with the Constitution and relevant laws.

Article 65: After the state decides to enter an emergency state, state of war, or implement national defense mobilization, the relevant agencies responsible for national security crisis management, according to laws or regulations of the Standing Committee of the National People's Congress, have the authority to take special measures that limit the rights of citizens and organizations and increase their obligations.

Article 66: Agencies responsible for national security crisis management should ensure that the control measures taken are proportional to the nature, degree, and scope of the potential harm posed by the national security crisis; where multiple measures are available, they should choose measures that best protect the rights and interests of citizens and organizations.

Article 67: The state improves the information reporting and release mechanism for national security crises.

After a national security crisis occurs, the responsible agencies should report accurately and promptly according to regulations, and uniformly release information about the occurrence, development, management, and aftermath of the national security crisis to the public.

Article 68: Once the national security threat and harm are controlled or eliminated, the control measures should be lifted in a timely manner, and follow-up work should be properly managed.

## **Chapter 5: National Security Assurance**

Article 69: The state improves the national security assurance system and enhances its ability to safeguard national security.

Article 70: The state improves the national security legal system and promotes the rule of law in national security.

Article 71: The state increases investment in various aspects of national security, ensuring the funding and equipment required for national security work.

Article 72: Units responsible for the strategic material reserves for national security should

store, manage, and maintain national security materials according to relevant national regulations and standards, regularly adjust and replace them, and ensure the effectiveness and safety of the reserves.

Article 73: The state encourages technological innovation in the field of national security and leverages technology in maintaining national security.

Article 74: The state takes necessary measures to recruit, train, and manage specialized and exceptional personnel for national security work.

Based on the needs of national security work, the state protects the identity and legal rights of personnel engaged in national security work, and strengthens personal protection and placement security.

Article 75: National security agencies, public security organs, and relevant military agencies conducting specialized national security work may take necessary measures and methods according to the law, and relevant departments and localities should provide support and cooperation within their responsibilities.

Article 76: The state enhances national security news publicity and public opinion guidance, conducts national security publicity and education activities in various forms, integrates national security education into the national education system and the training system for public officials, and strengthens public awareness of national security.

## **Chapter 6: Obligations and Rights of Citizens and Organizations**

Article 77: Citizens and organizations shall fulfill the following obligations to safeguard national security:

- (1) Abide by the relevant provisions on national security in the Constitution, laws, and regulations;
- (2) Timely report clues about activities that endanger national security;
- (3) Truthfully provide evidence related to activities that endanger national security;
- (4) Provide convenient conditions or other assistance for national security work;

- (5) Offer necessary support and assistance to national security agencies, public security organs, and relevant military agencies;
- (6) Keep national secrets confidential;
- (7) Fulfill other obligations as prescribed by laws and administrative regulations.

No individual or organization shall engage in activities that endanger national security, nor provide any funding or assistance to individuals or organizations that pose a threat to national security.

Article 78: Government agencies, people's organizations, enterprises, and other social organizations shall educate their personnel on safeguarding national security and mobilize and organize them to prevent and stop activities that endanger national security.

Article 79: Enterprises and institutions shall cooperate with relevant departments to implement safety measures as required by national security work.

Article 80: Citizens and organizations that support and assist national security work are protected by law.

If an individual or their close relatives face personal safety risks due to their support or assistance, they may request protection from public security organs or national security agencies. Public security organs and national security agencies, in coordination with relevant departments, shall take protective measures according to the law.

Article 81: Citizens and organizations that suffer property losses due to their support or assistance in national security work shall be compensated according to relevant national regulations; compensation for personal injury or death shall be provided according to relevant national regulations.

Article 82: Citizens and organizations have the right to criticize and suggest improvements to national security work, and to file complaints, accusations, and reports against illegal or negligent behavior of national security agencies and their staff.

Article 83: When special measures that restrict citizens' rights and freedoms are necessary for national security work, such measures must be conducted according to the law and limited to

what is necessary to maintain national security.

### **Chapter 7: Supplementary Provisions**

Article 84: This law shall take effect from the date of its promulgation.

Editor: Ma Juan

### **Related Links**

- [China Implements New National Security Law Starting July 1](#)
- [The 15th meeting of the Standing Committee of the 12th National People's Congress reviewed the draft National Security Law in a group discussion](#)

# 中华人民共和国国家安全法 (主席令第二十九号)

中央政府门户网站 www.gov.cn 2015-07-01 21:59 来源: 新华社

【字体: 大 中 小】打印本页

分享

## 中华人民共和国主席令 第二十九号

《中华人民共和国国家安全法》已由中华人民共和国第十二届全国人民代表大会常务委员会第十五次会议于2015年7月1日通过，现予公布，自公布之日起施行。

中华人民共和国主席 习近平

2015年7月1日

## 中华人民共和国国家安全法

(2015年7月1日第十二届全国人民代表大会常务委员会第十五次会议通过)

### 目录

#### 第一章 总则

#### 第二章 维护国家安全的任务

#### 第三章 维护国家安全的职责

#### 第四章 国家安全制度

##### 第一节 一般规定

##### 第二节 情报信息

##### 第三节 风险预防、评估和预警

##### 第四节 审查监管

##### 第五节 危机管控

#### 第五章 国家安全保障

## 第六章 公民、组织的义务和权利

## 第七章 附则

### 第一章 总则

第一条 为了维护国家安全，保卫人民民主专政的政权和中国特色社会主义制度，保护人民的根本利益，保障改革开放和社会主义现代化建设的顺利进行，实现中华民族伟大复兴，根据宪法，制定本法。

第二条 国家安全是指国家政权、主权、统一和领土完整、人民福祉、经济社会可持续发展和国家其他重大利益相对处于没有危险和不受内外威胁的状态，以及保障持续安全状态的能力。

第三条 国家安全工作应当坚持总体国家安全观，以人民安全为宗旨，以政治安全为根本，以经济安全为基础，以军事、文化、社会安全为保障，以促进国际安全为依托，维护各领域国家安全，构建国家安全体系，走中国特色国家安全道路。

第四条 坚持中国共产党对国家安全工作的领导，建立集中统一、高效权威的国家安全领导体制。

第五条 中央国家安全领导机构负责国家安全工作的决策和议事协调，研究制定、指导实施国家安全战略和有关重大方针政策，统筹协调国家安全重大事项和重要工作，推动国家安全法治建设。

第六条 国家制定并不断完善国家安全战略，全面评估国际、国内安全形势，明确国家安全战略的指导方针、中长期目标、重点领域的国家安全政策、工作任务和措施。

第七条 维护国家安全，应当遵守宪法和法律，坚持社会主义法治原则，尊重和保障人权，依法保护公民的权利和自由。

第八条 维护国家安全，应当与经济社会发展相协调。

国家安全工作应当统筹内部安全和外部安全、国土安全和国民安全、传统安全和非传统安全、自身安全和共同安全。

第九条 维护国家安全，应当坚持预防为主、标本兼治，专门工作与群众路线相结合，充分发挥专门机关和其他有关机关维护国家安全的职能作用，广泛动员公民和组织，防范、制止和依法惩治危害国家安全的行为。

第十条 维护国家安全，应当坚持互信、互利、平等、协作，积极同外国政府和国际组织开展安全交流合作，履行国际安全义务，促进共同安全，维护世界和平。

第十一条 中华人民共和国公民、一切国家机关和武装力量、各政党和各人民团体、企业事业组织和其他社会组织，都有维护国家安全的责任和义务。

中国的主权和领土完整不容侵犯和分割。维护国家主权、统一和领土完整是包括港澳同胞和台湾同胞在内的全中国人民的共同义务。

第十二条 国家对在维护国家安全工作中作出突出贡献的个人和组织给予表彰和奖励。

第十三条 国家机关工作人员在国家安全工作和涉及国家安全活动中，滥用职权、玩忽职守、徇私舞弊的，依法追究法律责任。

任何个人和组织违反本法和有关法律，不履行维护国家安全义务或者从事危害国家安全活动的，依法追究法律责任。

第十四条 每年4月15日为全民国家安全教育日。

## 第二章 维护国家安全的任务

第十五条 国家坚持中国共产党的领导，维护中国特色社会主义制度，发展社会主义民主政治，健全社会主义法治，强化权力运行制约和监督机制，保障人民当家作主的各项权利。

国家防范、制止和依法惩治任何叛国、分裂国家、煽动叛乱、颠覆或者煽动颠覆人民民主专政政权的行为；防范、制止和依法惩治窃取、泄露国家秘密等危害国家安全的行为；防范、制止和依法惩治境外势力的渗透、破坏、颠覆、分裂活动。

第十六条 国家维护和发展最广大人民的根本利益，保卫人民安全，创造良好生存发展条件和安定工作生活环境，保障公民的生命财产安全和其他合法权益。

第十七条 国家加强边防、海防和空防建设，采取一切必要的防卫和管控措施，保卫领陆、内水、领海和领空安全，维护国家领土主权和海洋权益。

第十八条 国家加强武装力量革命化、现代化、正规化建设，建设与保卫国家安全和利益需要相适应的武装力量；实施积极防御军事战略方针，防备和抵御侵略，制止武装颠覆和分裂；开展国际军事安全合作，实施联合国维和、国际救援、海上护航和维护国家海外利益的军事行动，维护国家主权、安全、领土完整、发展利益和世界和平。

第十九条 国家维护国家基本经济制度和社会主义市场经济秩序，健全预防和化解经济安全风险的制度机制，保障关系国民经济命脉的重要行业和关键领域、重点产业、重大基础设施和重大建设项目以及其他重大经济利益安全。

第二十条 国家健全金融宏观审慎管理和金融风险防范、处置机制，加强金融基础设施和基础能力建设，防范和化解系统性、区域性金融风险，防范和抵御外部金融风险的冲击。

第二十一条 国家合理利用和保护资源能源，有效管控战略资源能源的开发，加强战略资源能源储备，完善资源能源运输战略通道建设和安全保护措施，加强国际资源能源合作，全面提升应急保障能力，保障经济社会发展所需的资源能源持续、可靠和有效供给。

第二十二条 国家健全粮食安全保障体系，保护和提高粮食综合生产能力，完善粮食储备制度、流通体系和市场调控机制，健全粮食安全预警制度，保障粮食供给和质量安全。

第二十三条 国家坚持社会主义先进文化前进方向，继承和弘扬中华民族优秀传统文化，培育和践行社会主义核心价值观，防范和抵制不良文化的影响，掌握意识形态领域主导权，增强文化整体实力和竞争力。

第二十四条 国家加强自主创新能力建设，加快发展自主可控的战略高新技术和重要领域核心关键技术，加强知识产权的运用、保护和科技保密能力建设，保障重大技术和工程的安全。

第二十五条 国家建设网络与信息安全保障体系，提升网络与信息网络安全保护能力，加强网络和信息技术的创新研究和开发应用，实现网络和信息核心技术、关键基础设施和重要领域信息系统及数据的安全可控；加强网络管理，防范、制止和依法惩治网络攻击、网络入侵、网络窃密、散布违法有害信息等网络违法犯罪行为，维护国家网络空间主权、安全和发展利益。

第二十六条 国家坚持和完善民族区域自治制度，巩固和发展平等团结互助和谐的社会主义民族关系。坚持各民族一律平等，加强民族交往、交流、交融，防范、制止和依法惩治民族分裂活动，维护国家统一、民族团结和社会和谐，实现各民族共同团结奋斗、共同繁荣发展。

第二十七条 国家依法保护公民宗教信仰自由和正常宗教活动，坚持宗教独立自主自办的原则，防范、制止和依法惩治利用宗教名义进行危害国家安全的违法犯罪活动，反对境外势力干涉境内宗教事务，维护正常宗教活动秩序。

国家依法取缔邪教组织，防范、制止和依法惩治邪教违法犯罪活动。

第二十八条 国家反对一切形式的恐怖主义和极端主义，加强防范和处置恐怖主义的能力建设，依法开展情报、调查、防范、处置以及资金监管等工作，依法取缔恐怖活动组织和严厉惩治暴力恐怖活动。



第二十九条 国家健全有效预防和化解社会矛盾的体制机制，健全公共安全体系，积极预防、减少和化解社会矛盾，妥善处置公共卫生、社会安全等影响国家安全和社会稳定的突发事件，促进社会和谐，维护公共安全和社会安定。

第三十条 国家完善生态环境保护制度体系，加大生态建设和环境保护力度，划定生态保护红线，强化生态风险的预警和防控，妥善处置突发环境事件，保障人民赖以生存发展的大气、水、土壤等自然环境和条件不受威胁和破坏，促进人与自然和谐发展。

第三十一条 国家坚持和平利用核能和核技术，加强国际合作，防止核扩散，完善防扩散机制，加强对核设施、核材料、核活动和核废料处置的安全管理、监管和保护，加强核事故应急体系和应急能力建设，防止、控制和消除核事故对公民生命健康和生态环境的危害，不断增强有效应对和防范核威胁、核攻击的能力。

第三十二条 国家坚持和平探索和利用外层空间、国际海底区域和极地，增强安全进出、科学考察、开发利用的能力，加强国际合作，维护我国在外层空间、国际海底区域和极地的活动、资产和其他利益的安全。

第三十三条 国家依法采取必要措施，保护海外中国公民、组织和机构的安全和正当权益，保护国家的海外利益不受威胁和侵害。

第三十四条 国家根据经济社会发展和国家发展利益的需要，不断完善维护国家安全的任务。

### **第三章 维护国家安全的职责**

第三十五条 全国人民代表大会依照宪法规定，决定战争和和平的问题，行使宪法规定的涉及国家安全的其他职权。

全国人民代表大会常务委员会依照宪法规定，决定战争状态的宣布，决定全国总动员或者局部动员，决定全国或者个别省、自治区、直辖市进入紧急状态，行使宪法规定的和全国人民代表大会授予的涉及国家安全的其他职权。

第三十六条 中华人民共和国主席根据全国人民代表大会的决定和全国人民代表大会常务委员会的决定，宣布进入紧急状态，宣布战争状态，发布动员令，行使宪法规定的涉及国家安全的其他职权。

第三十七条 国务院根据宪法和法律，制定涉及国家安全的行政法规，规定有关行政措施，发布有关决定和命令；实施国家安全法律法规和政策；依照法律规定决定省、自治区、直辖市的范围内部分地区进入紧急状态；行使宪法法律规定的和全国人民代表大会及其常务委员会授予的涉及国家安全的其他职权。

第三十八条 中央军事委员会领导全国武装力量，决定军事战略和武装力量的作战方针，统一指挥维护国家安全的军事行动，制定涉及国家安全的军事法规，发布有关决定和命令。

第三十九条 中央国家机关各部门按照职责分工，贯彻执行国家安全方针政策和法律法规，管理指导本系统、本领域国家安全工作。

第四十条 地方各级人民代表大会和县级以上地方各级人民代表大会常务委员会在本行政区域内，保证国家安全法律法规的遵守和执行。

地方各级人民政府依照法律法规规定管理本行政区域内的国家安全工作。

香港特别行政区、澳门特别行政区应当履行维护国家安全的责任。

第四十一条 人民法院依照法律规定行使审判权，人民检察院依照法律规定行使检察权，惩治危害国家安全的犯罪。

第四十二条 国家安全机关、公安机关依法搜集涉及国家安全的情报信息，在国家安全工作中依法行使侦查、拘留、预审和执行逮捕以及法律规定的其他职权。

有关军事机关在国家安全工作中依法行使相关职权。

第四十三条 国家机关及其工作人员在履行职责时，应当贯彻维护国家安全的原则。

国家机关及其工作人员在国家安全工作和涉及国家安全活动中，应当严格依法履行职责，不得超越职权、滥用职权，不得侵犯个人和组织的合法权益。

## 第四章 国家安全制度

### 第一节 一般规定

第四十四条 中央国家安全领导机构实行统分结合、协调高效的国家安全制度与工作机制。

第四十五条 国家建立国家安全重点领域工作协调机制，统筹协调中央有关职能部门推进相关工作。

第四十六条 国家建立国家安全工作督促检查和责任追究机制，确保国家安全战略和重大部署贯彻落实。

第四十七条 各部门、各地区应当采取有效措施，贯彻实施国家安全战略。

第四十八条 国家根据维护国家安全工作需要，建立跨部门会商工作机制，就维护国家安全工作的重大事项进行会商研判，提出意见和建议。

第四十九条 国家建立中央与地方之间、部门之间、军地之间以及地区之间关于国家安全的协同联动机制。

第五十条 国家建立国家安全决策咨询机制，组织专家和有关方面开展对国家安全形势的分析研判，推进国家安全的科学决策。

## 第二节 情报信息

第五十一条 国家健全统一归口、反应灵敏、准确高效、运转顺畅的情报信息收集、研判和使用制度，建立情报信息工作协调机制，实现情报信息的及时收集、准确研判、有效使用和共享。

第五十二条 国家安全机关、公安机关、有关军事机关根据职责分工，依法搜集涉及国家安全的情报信息。

国家机关各部门在履行职责过程中，对于获取的涉及国家安全的有关信息应当及时上报。

第五十三条 开展情报信息工作，应当充分运用现代科学技术手段，加强对情报信息的鉴别、筛选、综合和研判分析。

第五十四条 情报信息的报送应当及时、准确、客观，不得迟报、漏报、瞒报和谎报。

## 第三节 风险预防、评估和预警

第五十五条 国家制定完善应对各领域国家安全风险预案。

第五十六条 国家建立国家安全风险评估机制，定期开展各领域国家安全风险调查评估。

有关部门应当定期向中央国家安全领导机构提交国家安全风险评估报告。

第五十七条 国家健全国家安全风险监测预警制度，根据国家安全风险程度，及时发布相应风险预警。

第五十八条 对可能即将发生或者已经发生的危害国家安全的事件，县级以上地方人民政府及其有关主管部门应当立即按照规定向上级人民政府及其有关主管部门报告，必要时可以越级上报。

## 第四节 审查监管

第五十九条 国家建立国家安全审查和监管的制度和机制，对影响或者可能影响国家安全的外商投资、特定物项和关键技术、网络信息技术产品和服务、涉及国家安全事项的

建设项目，以及其他重大事项和活动，进行国家安全审查，有效预防和化解国家安全风险。

第六十条 中央国家机关各部门依照法律、行政法规行使国家安全审查职责，依法作出国家安全审查决定或者提出安全审查意见并监督执行。

第六十一条 省、自治区、直辖市依法负责本行政区域内有关国家安全审查和监管工作。

#### 第五节 危机管控

第六十二条 国家建立统一领导、协同联动、有序高效的国家安全危机管控制度。

第六十三条 发生危及国家安全的重大事件，中央有关部门和有关地方根据中央国家安全领导机构的统一部署，依法启动应急预案，采取管控处置措施。

第六十四条 发生危及国家安全的特别重大事件，需要进入紧急状态、战争状态或者进行全国总动员、局部动员的，由全国人民代表大会、全国人民代表大会常务委员会或者国务院依照宪法和有关法律规定的权限和程序决定。

第六十五条 国家决定进入紧急状态、战争状态或者实施国防动员后，履行国家安全危机管控职责的有关机关依照法律规定或者全国人民代表大会常务委员会规定，有权采取限制公民和组织权利、增加公民和组织义务的特别措施。

第六十六条 履行国家安全危机管控职责的有关机关依法采取处置国家安全危机的管控措施，应当与国家安全危机可能造成的危害的性质、程度和范围相适应；有多种措施可供选择的，应当选择有利于最大程度保护公民、组织权益的措施。

第六十七条 国家健全国家安全危机的信息报告和发布机制。

国家安全危机事件发生后，履行国家安全危机管控职责的有关机关，应当按照规定准确、及时报告，并依法将有关国家安全危机事件发生、发展、管控处置及善后情况统一向社会发布。

第六十八条 国家安全威胁和危害得到控制或者消除后，应当及时解除管控处置措施，做好善后工作。

#### 第五章 国家安全保障

第六十九条 国家健全国家安全保障体系，增强维护国家安全的能力。

第七十条 国家健全国家安全法律制度体系，推动国家安全法治建设。

第七十一条 国家加大对国家安全各项建设的投入，保障国家安全工作所需经费和装备。

第七十二条 承担国家安全战略物资储备任务的单位，应当按照国家有关规定和标准对国家安全物资进行收储、保管和维护，定期调整更换，保证储备物资的使用效能和安全。

第七十三条 鼓励国家安全领域科技创新，发挥科技在维护国家安全中的作用。

第七十四条 国家采取必要措施，招录、培养和管理国家安全工作专门人才和特殊人才。

根据维护国家安全工作的需要，国家依法保护有关机关专门从事国家安全工作人员的身份和合法权益，加大人身保护和安置保障力度。

第七十五条 国家安全机关、公安机关、有关军事机关开展国家安全专门工作，可以依法采取必要手段和方式，有关部门和地方应当在职责范围内提供支持和配合。

第七十六条 国家加强国家安全新闻宣传和舆论引导，通过多种形式开展国家安全宣传教育活动，将国家安全教育纳入国民教育体系和公务员教育培训体系，增强全民国家安全意识。

## 第六章 公民、组织的义务和权利

第七十七条 公民和组织应当履行下列维护国家安全的义务：

- （一）遵守宪法、法律法规关于国家安全的有关规定；
- （二）及时报告危害国家安全活动的线索；
- （三）如实提供所知悉的涉及危害国家安全活动的证据；
- （四）为国家安全工作提供便利条件或者其他协助；
- （五）向国家安全机关、公安机关和有关军事机关提供必要的支持和协助；
- （六）保守所知悉的国家秘密；
- （七）法律、行政法规规定的其他义务。

任何个人和组织不得有危害国家安全的行为，不得向危害国家安全的个人或者组织提供任何资助或者协助。

第七十八条 机关、人民团体、企业事业组织和其他社会组织应当对本单位的人员进行维护国家安全的教育，动员、组织本单位的人员防范、制止危害国家安全的行为。

第七十九条 企业事业组织根据国家安全工作的要求，应当配合有关部门采取相关安全措施。

第八十条 公民和组织支持、协助国家安全工作的行为受法律保护。

因支持、协助国家安全工作，本人或者其近亲属的人身安全面临危险的，可以向公安机关、国家安全机关请求予以保护。公安机关、国家安全机关应当会同有关部门依法采取保护措施。

第八十一条 公民和组织因支持、协助国家安全工作导致财产损失的，按照国家有关规定给予补偿；造成人身伤害或者死亡的，按照国家有关规定给予抚恤优待。

第八十二条 公民和组织对国家安全工作有向国家机关提出批评建议的权利，对国家机关及其工作人员在国家安全工作中的违法失职行为有提出申诉、控告和检举的权利。

第八十三条 在国家安全工作中，需要采取限制公民权利和自由的特别措施时，应当依法进行，并以维护国家安全的实际需要为限度。

## 第七章 附则

第八十四条 本法自公布之日起施行。

责任编辑：马娟

## 相关链接

- [我国通过新国家安全法 于7月1日起施行](#)
- [十二届全国人大常委会第十五次会议分组审议国家安全法草案](#)

# EXHIBIT B

**Declaration of David Newman  
Principal Deputy Assistant Attorney General  
National Security Division  
Department of Justice**



---

# Certification of Translation

---



COUNTY OF SUFFOLK  
COMMONWEALTH OF MASSACHUSETTS

July 24, 2024

This is to certify that the attached translation is, to the best of my knowledge and belief, a true and accurate translation from Simplified Chinese into English of the attached document:

- **Cybersecurity Law**

Linguistic Systems, Inc. adheres to an ISO-certified quality management system that ensures best practices are always followed in the selection of linguists skilled in both the languages and subject matters necessary for every translation.



Linguistic Systems, Inc.



260 Franklin Street, Suite 230, Boston MA 02110 • Phone 617-528-7400 • Fax 617-528-7490 • [www.linguist.com](http://www.linguist.com)

Certifications: ISO 9001 • ISO 17100 • ISO 18587 • ISO 27001



# Cybersecurity Law of the People's Republic of China

November 7, 2016, 19:05 Source: Xinhua News Agency

Font Size: [Default](#) [Large](#) [Extra Large](#) | [Print](#) |

Xinhua News Agency, Beijing, November 7

## **Cybersecurity Law of the People's Republic of China**

**(Passed at the 24th Meeting of the Standing Committee of the 12th National People's Congress on November 7, 2016)**

### Contents

#### Chapter 1 General Provisions

#### Chapter 2 Cybersecurity Support and Promotion

#### Chapter 3 Cyber Operation Security

#### Section 1 General Provisions

#### Section 2 Security of Critical Information Infrastructure Operation

#### Chapter 4 Cyber Information Security

#### Chapter 5 Monitoring, Early Warning, and Emergency Response

#### Chapter 6 Legal Liability

#### Chapter 7 Supplementary Provisions

Article 1: This law is formulated to ensure cybersecurity, safeguard cyberspace sovereignty and national security, protect public interests, protect the legitimate rights and interests of citizens, legal persons, and other organizations, and promote the healthy development of economic and social informatization.

Article 2: This law applies to the construction, operation, maintenance, and use of networks, as well as the supervision and management of cybersecurity within the territory of the People's Republic of China.

Article 3: The state upholds the principle of simultaneously advancing cybersecurity and information technology development, adhering to the guidelines of active utilization, scientific development, lawful management, and ensuring security. It promotes the construction and interconnectivity of network infrastructure, encourages technological innovation and application, supports the cultivation of cybersecurity talent, and establishes and improves the cybersecurity protection system to enhance cybersecurity protection capabilities.

Article 4: The state formulates and continually improves cybersecurity strategies, clarifying the basic requirements and main objectives for ensuring cybersecurity, and proposes cybersecurity policies, tasks, and measures for key areas.

Article 5: The state takes measures to monitor, defend against, and handle cybersecurity risks and threats originating both inside and outside the People's Republic of China, protect critical information infrastructure from attacks, intrusions, interference, and destruction, and lawfully punish cybercriminal activities to maintain cybersecurity and order.

Article 6: The state advocates honest, trustworthy, healthy, and civilized online behavior, promotes the dissemination of socialist core values, takes measures to improve cybersecurity awareness and proficiency across society, and fosters a favorable environment for the entire society to participate in promoting cybersecurity.

Article 7: The state actively engages in international exchanges and cooperation in cyberspace governance, network technology research and development, standard-setting, and combating cybercrime. It strives to build a peaceful, secure, open, and cooperative cyberspace and establish a multilateral, democratic, and transparent network governance system.

Article 8: The national cybersecurity and informatization department is responsible for overall coordination of cybersecurity work and related supervision and management efforts. The State Council's telecommunications authority, public security departments, and other relevant agencies

are responsible for cybersecurity protection and supervision within their respective areas of responsibility, in accordance with this law and other relevant laws and administrative regulations.

The cybersecurity protection and supervision responsibilities of relevant departments of local people's governments at or above the county level are determined according to state regulations.

Article 9: Network operators must comply with laws and administrative regulations, respect social morals, adhere to business ethics, maintain honesty and trustworthiness, fulfill cybersecurity protection obligations, accept supervision from the government and society, and bear social responsibility while conducting business and service activities.

Article 10: Entities building, operating networks, or providing services through networks must comply with laws, administrative regulations, and mandatory national standards, and adopt technical measures and other necessary measures to ensure network security and stable operation, effectively respond to cybersecurity incidents, prevent cyber crimes, and maintain the integrity, confidentiality, and availability of network data.

Article 11: Network-related industry organizations should strengthen industry self-discipline, formulate cybersecurity conduct standards according to their charters, guide members to enhance cybersecurity protection, improve cybersecurity protection levels, and promote healthy industry development.

Article 12: The state protects the rights of citizens, legal persons, and other organizations to use networks in accordance with the law, promotes widespread access to networks, improves network service levels, provides secure and convenient network services to society, and ensures the lawful and orderly free flow of network information.

Individuals and organizations using networks must comply with the Constitution, laws, and public order, respect social ethics, and must not endanger network security or use the network to harm national security, honor, and interests; incite subversion of state power or overthrow the socialist system; incite secession or undermine national unity; advocate terrorism, extremism, ethnic hatred, or ethnic discrimination; spread violence, obscene and pornographic information; fabricate or spread false information that disrupts economic order and social order; or engage in activities that infringe upon others' reputations, privacy, intellectual property rights, and other legitimate rights and interests.

Article 13: The state supports the research and development of network products and services beneficial to the healthy growth of information and communication technologies and prohibits activities that harm the physical and

mental health of minors through the network in accordance with the law, and provides a safe and healthy network environment for minors.

Article 14: Any individual and organization has the right to report actions endangering cybersecurity to cybersecurity, telecommunications, public security, and other departments. Departments receiving such reports must promptly handle them in accordance with the law; if the matter does not fall within the department's responsibilities, it should promptly transfer the report to the competent department.

Relevant departments should keep the reporter's information confidential and protect the legitimate rights and interests of the reporter.

## **Chapter 2: Support and Promotion of Cybersecurity**

Article 15: The state establishes and improves the cybersecurity standards system. The Standardization Administration of the State Council and other relevant departments of the State Council, according to their respective responsibilities, organize the development and timely revision of national standards, industry standards for cybersecurity management, and the safety of network products, services, and operations.

The state supports enterprises, research institutions, universities, and industry organizations in participating in the development of national and industry cybersecurity standards.

Article 16: The State Council and the governments of provinces, autonomous regions, and municipalities directly under the central government should coordinate planning, increase investment, support key cybersecurity technology industries and projects, and promote the research, development, and application of cybersecurity technologies. They should also promote the use of safe and reliable network products and services, protect intellectual property rights in network technology, and support enterprises, research institutions, and universities in participating in national cybersecurity technology innovation projects.

Article 17: The state advances the construction of a socialized cybersecurity service system, encouraging relevant enterprises and institutions to provide cybersecurity certification, testing, and risk assessment services.

Article 18: The state encourages the development of technologies for protecting and utilizing network data, promotes the opening of public data resources, and fosters technological innovation

and economic and social development.

The state supports innovative methods for cybersecurity management, using new network technologies to enhance the level of cybersecurity protection.

Article 19: Governments at all levels and their relevant departments should organize regular cybersecurity publicity and education, and guide and supervise relevant units in their cybersecurity publicity and education work.

Public media should conduct targeted cybersecurity publicity and education for society.

Article 20: The state supports enterprises, universities, vocational schools, and other educational training institutions in conducting cybersecurity-related education and training. It encourages various methods to cultivate cybersecurity talent and promotes the exchange of cybersecurity professionals.

### **Chapter 3: Network Operation Security**

#### **Section 1: General Provisions**

Article 21: The state implements a network security level protection system. Network operators must fulfill the following security protection obligations according to the requirements of the network security level protection system to ensure the network is protected from interference, damage, or unauthorized access, and to prevent network data from being leaked, stolen, or tampered with:

- (1) Develop internal security management systems and operational procedures, designate a network security responsible person, and implement network security protection responsibilities;
- (2) Take technical measures to prevent computer viruses, network attacks, and intrusions that threaten network security;
- (3) Implement technical measures to monitor and record network operation status and network security incidents, and retain relevant network logs for no less than six months as required;
- (4) Adopt measures such as data classification, important data backup, and encryption;
- (5) Other obligations specified by laws and administrative regulations.

Article 22: Network products and services must meet the mandatory requirements of relevant national standards. Providers of network products and services must not install malicious programs. If they discover security defects, vulnerabilities, or other risks in their products or services, they must immediately take remedial measures, notify users in a timely manner as required, and report to the relevant authorities.

Providers of network products and services must continuously provide security maintenance for their products and services. They must not terminate security maintenance within the specified or agreed period.

For network products and services that have the capability to collect user information, providers must clearly inform users and obtain their consent. They must also comply with this law and other relevant laws and regulations regarding personal information protection.

Article 23: Network critical equipment and network security-specific products must comply with relevant national standards and may only be sold or provided after passing security certification or testing by qualified institutions. The national cybersecurity department, along with relevant State Council departments, will develop and publish a catalog of network critical equipment and network security-specific products and promote mutual recognition of security certification and testing results to avoid redundant certification and testing.

Article 24: When network operators provide users with network access, domain name registration services, fixed-line or mobile phone network procedures, or services such as information publishing and instant messaging, they must require users to provide true identity information when signing agreements or confirming service provision. Network operators must not provide these services if users do not provide true identity information.

The state implements a trusted network identity strategy, supports the research and development of secure and convenient electronic identity authentication technologies, and promotes mutual recognition among different electronic identity authentications.

Article 25: Network operators must develop emergency response plans for network security incidents and promptly address risks such as system vulnerabilities, computer viruses, network attacks, and network intrusions. In the event of a network security incident, they must immediately activate the emergency plan, take appropriate remedial measures, and report to the relevant authorities as required.

Article 26 : Activities related to network security certification, testing, risk assessment, and the public release of information about system vulnerabilities, computer viruses, network attacks, and network intrusions must comply with national regulations.

Article 27: No individual or organization may engage in activities that harm network security,

such as illegally accessing others' networks, interfering with others' network functions, or stealing network data. They must not provide programs or tools specifically used for network intrusion, disrupting network functions, or stealing network data. If they know that others are engaging in activities that harm network security, they must not provide technical support, advertising, promotion, or payment services.

Article 28: Network operators must provide technical support and assistance to public security and national security organs in their lawful activities to maintain national security and investigate crimes.

Article 29: The state supports cooperation among network operators in the collection, analysis, reporting, and emergency handling of network security information to enhance their security capabilities.

Industry organizations should establish and improve network security protection standards and collaboration mechanisms, strengthen the analysis and assessment of network security risks, issue risk warnings to members regularly, and support and assist members in addressing network security risks.

Article 30: Information obtained by the cyberspace administration and relevant departments while performing network security protection duties may only be used for maintaining network security and must not be used for other purposes.

## Section 2: Operational Security of Critical Information Infrastructure

Article 31 : The state implements special protection measures for critical information infrastructure in key sectors such as public communication and information services, energy, transportation, water conservancy, finance, public services, and e-government. This includes other infrastructure that, if damaged, loses functionality, or experiences data leakage, could severely threaten national security, the economy, public welfare, or national interests. This protection is based on the network security classification protection system. The specific scope and security protection measures for critical information infrastructure are determined by the State Council.

The state encourages network operators outside the critical information infrastructure to voluntarily participate in the protection system for critical information infrastructure.

Article 32: According to the division of responsibilities prescribed by the State Council, the departments responsible for the security protection of critical information infrastructure shall respectively develop and implement security plans for critical information infrastructure within their industry or field. They shall guide and supervise the operational security protection of critical information infrastructure.

Article 33: When constructing critical information infrastructure, it must ensure that it supports stable and continuous operation and that security technical measures are planned, constructed, and used in synchronization.

Article 34: In addition to the provisions of Article 21 of this law, operators of critical information infrastructure must also fulfill the following security protection obligations:

(1) Establish specialized security management institutions and designate a security management officer, and conduct security background checks on this officer and personnel in key positions;

(2) Regularly provide network security education, technical training, and skill assessments for employees;

(3) Implement disaster recovery backups for important systems and databases;

(4) Develop emergency response plans for network security incidents and conduct regular drills;

(5) Fulfill other obligations as stipulated by laws and administrative regulations.

Article 35: When operators of critical information infrastructure purchase network products and services that may impact national security, they must undergo a national security review organized by the national internet information department together with relevant State Council departments.

Article 36: Operators of critical information infrastructure should sign security confidentiality agreements with providers when purchasing network products and services, specifying security and confidentiality obligations and responsibilities.

Article 37: Operators of critical information infrastructure must store personal information and important data collected and generated within the People's Republic of China domestically. If there is a business need to provide this data overseas, a security assessment must be conducted according to the methods established by the national internet information department and relevant



State Council departments; if there are other legal or administrative regulations, those regulations apply.

Article 38: Operators of critical information infrastructure must either conduct or delegate a network security service organization to perform a security and risk assessment of their network at least once a year, and report the assessment results and improvement measures to the relevant departments responsible for critical information infrastructure security protection.

Article 39: The national internet information department shall coordinate relevant departments to take the following measures for the security protection of critical information infrastructure:

(1) Conduct spot checks and assessments of security risks for critical information infrastructure, propose improvements, and, if necessary, entrust cybersecurity service agencies to assess the risks.

(2) Regularly organize cybersecurity emergency drills for operators of critical information infrastructure to enhance their capability to respond to cybersecurity incidents and improve coordination.

(3) Promote the sharing of cybersecurity information between relevant departments, operators of critical information infrastructure, research institutions, and cybersecurity service agencies.

(4) Provide technical support and assistance for the emergency response to cybersecurity incidents and the recovery of network functions.

#### **Chapter 4 Network Information Security**

Article 40: Network operators must keep the user information they collect strictly confidential and establish and improve user information protection systems.

Article 41: When collecting and using personal information, network operators must follow the principles of legality, propriety, and necessity, publicly disclose the rules for collection and use, clearly state the purpose, method, and scope of the collection and use, and obtain consent from the individuals whose information is being collected. Network operators may not collect personal information that is unrelated to the services they provide, and must not collect or use personal

information in violation of laws, administrative regulations, or agreements. They must handle the personal information they retain in accordance with legal and regulatory requirements and agreements with users.

Article 42: Network operators must not disclose, alter, or destroy the personal information they collect; they may not provide personal information to others without the consent of the individuals whose information is being collected. However, this does not apply to information that has been processed in such a way that individuals cannot be identified and the information cannot be restored.

Network operators must take technical and other necessary measures to ensure the security of the personal information they collect, and to prevent information leakage, damage, or loss. In the event of or potential for personal information leakage, damage, or loss, they must immediately take remedial measures, notify users in a timely manner as required, and report to the relevant authorities.

Article 43: Individuals who find that network operators are collecting or using their personal information in violation of laws, administrative regulations, or agreements have the right to request the deletion of their personal information from the network operators. If individuals find that their personal information collected or stored by network operators is incorrect, they have the right to request correction. Network operators must take measures to delete or correct the information.

Article 44: No individual or organization may steal or otherwise illegally obtain personal information, or illegally sell or provide personal information to others.

Article 45: Departments and their staff who are legally responsible for network security supervision and management must keep confidential any personal information, privacy, and commercial secrets they become aware of in the course of their duties. They must not disclose, sell, or illegally provide such information to others.

Article 46: Individuals and organizations must be responsible for their actions on the internet. They may not establish websites, communication groups, or other platforms for fraud, teaching criminal methods, producing or selling prohibited or controlled items, or other illegal activities. They may not use the internet to publish information related to fraud, the production or sale of prohibited or controlled items, or other criminal activities.

Article 47: Network operators must strengthen the management of information published

by their users. If they find information that is prohibited from being published or transmitted by laws or administrative regulations, they must immediately stop transmitting that information, take measures to eliminate it and prevent its spread, keep relevant records, and report to the relevant authorities.

Article 48: Electronic information or application software provided by any individual or organization must not contain malicious programs and must not include information prohibited from being published or transmitted by laws or administrative regulations.

Providers of electronic information sending services and application software downloading services must fulfill their security management duties. If they are aware that their users engage in the aforementioned prohibited activities, they must stop providing services, take measures to eliminate the problematic content, keep relevant records, and report to the relevant authorities.

Article 49: Network operators must establish a complaint and reporting system for network information security, publicize information about how to make complaints and reports, and promptly handle and address complaints and reports related to network information security.

Network operators must cooperate with the supervision and inspection conducted by the internet information departments and other relevant authorities in accordance with the law.

Article 50: The national internet information departments and other relevant authorities, in performing their duties of network information security supervision and management, must require network operators to stop transmitting information that is prohibited from being published or transmitted by laws and administrative regulations, take measures to eliminate such information, and keep relevant records. For information of this nature originating from outside the People's Republic of China, they must notify the relevant institutions to take technical and other necessary measures to block its dissemination.

### **Chapter 5 Monitoring, Early Warning, and Emergency Response**

Article 51: The state establishes a network security monitoring, early warning, and information notification system. The national internet information departments should coordinate with relevant departments to enhance the collection, analysis, and reporting of network security information, and issue unified network security monitoring and early warning information according to regulations.

Article 52: Departments responsible for the security protection of critical information infrastructure should establish and improve network security monitoring, early warning, and information notification systems for their respective industries and fields, and report network security monitoring and early warning information according to regulations.

Article 53: The national internet information departments should coordinate with relevant departments to establish and improve mechanisms for network security risk assessment and emergency response. They should formulate emergency plans for network security incidents and organize regular drills.

Departments responsible for the security protection of critical information infrastructure should develop emergency plans for network security incidents specific to their industries and fields and organize regular drills.

Emergency plans for network security incidents should classify incidents according to their severity, impact range, and other factors, and stipulate corresponding emergency response measures.

Article 54: When the risk of network security incidents increases, relevant departments of provincial-level and higher governments should take the following measures according to their prescribed authority and procedures, considering the characteristics and potential harm of the network security risks:

- (1) Require relevant departments, institutions, and personnel to promptly collect and report relevant information and enhance monitoring of network security risks.
- (2) Organize relevant departments, institutions, and professionals to analyze and assess network security risk information, forecasting the likelihood, impact range, and severity of potential incidents.
- (3) Issue network security risk warnings to the public and release measures to avoid or mitigate harm.

Article 55: When a network security incident occurs, the network security incident emergency response plan should be activated immediately. Investigate and assess the incident, require network operators to take technical and other necessary measures to eliminate security risks and prevent

further harm, and promptly issue public warning information related to the incident.

Article 56: If departments of provincial level or above discover significant security risks or incidents while performing network security supervision and management duties, they may, according to their authority and procedures, conduct interviews with the legal representatives or key persons in charge of the network operators. Network operators must take corrective actions as required to eliminate risks.

Article 57: In the event of a network security incident that leads to emergencies or production safety accidents, the handling should be in accordance with the "Emergency Response Law of the People's Republic of China," "Production Safety Law of the People's Republic of China," and other relevant laws and regulations.

Article 58: For the purpose of safeguarding national security and public order and handling major sudden social security incidents, the State Council may, upon decision or approval, implement temporary measures such as restrictions on network communication in specific areas.

## **Chapter 6: Legal Responsibilities**

Article 59: If a network operator fails to fulfill the network security protection obligations stipulated in Articles 21 and 25 of this law, the relevant supervisory departments will order correction and issue a warning. If the operator refuses to correct the situation or causes harm to network security, a fine of more than 10,000 yuan but less than 100,000 yuan will be imposed. The directly responsible personnel will be fined between 5,000 yuan and 50,000 yuan.

If an operator of critical information infrastructure fails to fulfill the network security protection obligations stipulated in Articles 33, 34, 36, and 38 of this law, the relevant supervisory departments will order correction and issue a warning. If the operator refuses to correct the situation or causes harm to network security, a fine of more than 100,000 yuan but less than 1,000,000 yuan will be imposed. The directly responsible personnel will be fined between 10,000 yuan and 100,000 yuan.

Article 60: If the provisions of the first and second paragraphs of Article 22 or the first paragraph of Article 48 of this law are violated, and any of the following behaviors occur, the relevant supervisory departments will order correction and issue a warning. If the operator refuses to correct the situation or causes harm to network security, a fine of more than 50,000 yuan but less than

500,000 yuan will be imposed. The directly responsible personnel will be fined between 10,000 yuan and 100,000 yuan:

(1) Setting up malicious programs;

(2) Failing to promptly take remedial measures for security defects or risks in products or services, or failing to notify users and relevant supervisory departments as required;

(3) Unilaterally terminating the provision of security maintenance for products or services.

Article 61: If a network operator violates the provisions of the first paragraph of Article 24 by failing to require users to provide true identity information, or by providing related services to users who do not provide true identity information, the relevant competent authority shall order correction and issue a warning. If the correction is not made or the circumstances are serious, a fine ranging from 50,000 to 500,000 yuan may be imposed, and the relevant competent authority may order the suspension of related business, business rectification, website closure, revocation of relevant business licenses, or revocation of the business license. For the directly responsible managers and other directly responsible personnel, a fine ranging from 10,000 to 100,000 yuan may be imposed.

Article 62: If a network security certification, testing, risk assessment, or the release of information on system vulnerabilities, computer viruses, network attacks, or network intrusions is conducted in violation of the provisions of Article 26, the relevant competent authority shall order correction and issue a warning. If the correction is not made or the circumstances are serious, a fine ranging from 10,000 to 100,000 yuan may be imposed, and the relevant competent authority may order the suspension of related business, business rectification, website closure, revocation of relevant business licenses, or revocation of the business license. For the directly responsible managers and other directly responsible personnel, a fine ranging from 5,000 to 50,000 yuan may be imposed.

Article 63: If a person or organization engages in activities that harm network security, provides programs or tools specifically used for such activities, or provides technical support, advertising, promotion, payment settlement, or other assistance for such activities, and this does not constitute a crime, the public security organs may confiscate illegal gains, impose detention of up to five days, and/or impose a fine ranging from 50,000 to 500,000 yuan. For more serious circumstances, detention of more than five days but less than fifteen days may be imposed, and/or a fine

ranging from 100,000 to 1,000,000 yuan.

For entities that engage in the behaviors described in the previous paragraph, the public security organs shall confiscate illegal gains and impose fines ranging from 100,000 to 1,000,000 yuan. Directly responsible managers and other directly responsible personnel shall be penalized according to the provisions of the previous paragraph.

Individuals who have been subjected to administrative penalties for violations of Article 27 of this law shall be prohibited from engaging in network security management and key positions in network operation for five years. Those who have been criminally punished shall be permanently prohibited from engaging in such roles.

Article 64: Network operators and providers of network products or services that violate the provisions of Paragraph 3 of Article 22, Articles 41 to 43 of this law, infringing on the legally protected rights of personal information, shall be ordered to make corrections by the relevant competent authorities. Depending on the severity, they may be given a warning, have their illegal gains confiscated, and fined between one and ten times the amount of the illegal gains. If there are no illegal gains, a fine of up to one million yuan may be imposed. The directly responsible persons in charge and other directly responsible personnel shall be fined between ten thousand and one hundred thousand yuan. In serious cases, they may be ordered to suspend related business, suspend operations for rectification, close websites, revoke related business licenses, or revoke business licenses.

Those who violate the provisions of Article 44 of this law by stealing or otherwise illegally obtaining, selling, or providing personal information to others, without constituting a crime, shall have their illegal gains confiscated by the public security organs and be fined between one and ten times the amount of the illegal gains. If there are no illegal gains, a fine of up to one million yuan shall be imposed.

Article 65: If a key information infrastructure operator violates the provisions of Article 35 by using network products or services that have not passed security review or are not subject to security review, the relevant competent authority shall order the cessation of use and impose fines ranging from one to ten times the amount of the procurement cost. For directly responsible managers and other directly responsible personnel, fines ranging from 10,000 to 100,000 yuan may be imposed.

Article 66: If a key information infrastructure operator violates the provisions of Article 37 by storing network data abroad or providing network data to foreign entities, the relevant competent authority shall order correction, issue a warning, confiscate illegal gains, and impose fines ranging from 50,000 to 500,000 yuan. The authority may also order the suspension of related business, business rectification, website closure, revocation of relevant business licenses, or revocation of the business license. For directly responsible managers and other directly responsible personnel, fines ranging from 10,000 to 100,000 yuan may be imposed.

Article 67: If a website or communication group is established for illegal activities or if the network is used to publish information related to illegal activities in violation of Article 46, and such actions do not constitute a crime, the public security authorities may impose detention of up to five days,

and fines ranging from 10,000 to 100,000 yuan. In more severe cases, detention of more than five days but less than fifteen days may be imposed, along with fines ranging from 50,000 to 500,000 yuan. Websites or communication groups used for illegal activities will be shut down.

If an organization engages in such behavior, the public security authorities will impose fines ranging from 100,000 to 500,000 yuan and punish the directly responsible managers and other directly responsible personnel according to the same standards.

Article 68: If a network operator violates Article 47 by failing to stop the transmission of information prohibited by laws or administrative regulations, does not take elimination measures or preserve relevant records, the competent authority will order correction, issue a warning, and confiscate illegal gains. If correction is not made or the situation is severe, fines ranging from 100,000 to 500,000 yuan may be imposed. The authority may also order the suspension of related business, business rectification, website closure, revocation of business licenses, or revocation of the business license. For directly responsible managers and other directly responsible personnel, fines ranging from 10,000 to 100,000 yuan may be imposed.

Electronic information transmission service providers and application download service providers that fail to perform the security management duties stipulated in Article 48 will be punished according to the same standards.

Article 69: If a network operator violates the provisions of this law and engages in any of the following behaviors, the competent authority will order correction. If correction is not made or the



situation is severe, fines ranging from 50,000 to 500,000 yuan will be imposed. For directly responsible managers and other directly responsible personnel, fines ranging from 10,000 to 100,000 yuan may be imposed:

- (1) Failing to take measures to stop the transmission or eliminate information that is prohibited by laws and administrative regulations according to the requirements of relevant departments;
- (2) Refusing or obstructing the lawful supervision and inspection conducted by relevant departments;
- (3) Refusing to provide technical support and assistance to public security organs and national security organs.

Article 70: For the release or transmission of information prohibited by Article 12, Paragraph 2 of this law and other laws or administrative regulations, penalties shall be imposed according to relevant laws and administrative regulations.

Article 71: For illegal activities specified in this law, the violations shall be recorded in the credit file and publicly disclosed according to relevant laws and administrative regulations.

Article 72: If the operator of a government affairs network of a state organ fails to fulfill the network security protection obligations specified in this law, their superior authority or relevant agency shall order correction; disciplinary action shall be taken against the directly responsible managerial personnel and other directly responsible individuals according to the law.

Article 73: If the Cyberspace Administration and relevant departments violate the provisions of Article 30 of this law by using information obtained during their network security protection duties for other purposes, disciplinary action shall be taken against the directly responsible managerial personnel and other directly responsible individuals according to the law.

If staff members of the Cyberspace Administration and relevant departments neglect their duties, abuse their power, or engage in favoritism and corruption, and such actions do not constitute a crime, they shall be disciplined according to the law.

Article 74: If violations of this law cause damage to others, civil liability shall be borne according to the law.

If violations of this law constitute a public security offense, public security penalties shall be

imposed according to the law; if they constitute a crime, criminal responsibility shall be pursued according to the law.

Article 75: Foreign institutions, organizations, or individuals engaging in activities that attack, intrude, interfere with, or damage the critical information infrastructure of the People's Republic of China, resulting in severe consequences, shall be held legally responsible according to the law. The State Council's public security departments and relevant authorities may also decide to freeze the assets of or impose other necessary sanctions on such institutions, organizations, or individuals.

### **Chapter 7: Supplementary Provisions**

Article 76: The meanings of the following terms in this law are:

(1) Network: Refers to a system composed of computers or other information terminals and related devices that collect, store, transmit, exchange, and process information according to certain rules and procedures.

(2) Cybersecurity: Refers to the capability to maintain a network in a stable and reliable state by taking necessary measures to prevent attacks, intrusions, interference, destruction, and illegal use, as well as accidental incidents, and to ensure the integrity, confidentiality, and availability of network data.

(3) Network Operator: Refers to the owner, manager, and service provider of a network.

(4) Network Data: Refers to various electronic data collected, stored, transmitted, processed, and generated through a network.

(5) Personal Information: Refers to various information recorded electronically or otherwise that can identify an individual's identity alone or in combination with other information, including but not limited to the individual's name, date of birth, ID number, personal biometric information, address, and phone number.

Article 77: The operation and security protection of networks involving state secrets, in addition to complying with this law, shall also comply with the provisions of confidentiality laws and administrative regulations.

Article 78: The security protection of military networks shall be separately stipulated by the Central Military Commission.

Article 79: This law shall come into effect on June 1, 2017.

# 中华人民共和国网络安全法

2016-11-07 19:05 来源： 新华社

字号：默认 大 超大 | 打印 |

新华社北京11月7日电

## 中华人民共和国网络安全法

(2016年11月7日第十二届全国人民代表大会常务委员会第二十四次会议通过)

### 目 录

第一章 总 则

第二章 网络安全支持与促进

第三章 网络运行安全

第一节 一般规定

第二节 关键信息基础设施的运行安全

第四章 网络信息安全

第五章 监测预警与应急处置

第六章 法律责任

第七章 附 则

### 第一章 总 则

第一条 为了保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展，制定本法。

第二条 在中华人民共和国境内建设、运营、维护和使用网络，以及网络安全的监督管理，适用本法。

第三条 国家坚持网络安全与信息化发展并重，遵循积极利用、科学发展、依法管理、确保安全的方针，推进网络基础设施建设和互联互通，鼓励网络技术创新和应用，支持培养网络安全人才，建立健全网络安全保障体系，提高网络安全保护能力。

第四条 国家制定并不断完善网络安全战略，明确保障网络安全的基本要求和主要目标，提出重点领域的网络安全政策、工作任务和措施。

第五条 国家采取措施，监测、防御、处置来源于中华人民共和国境内外的网络安全风险和威胁，保护关键信息基础设施免受攻击、侵入、干扰和破坏，依法惩治网络违法犯罪活动，维护网络空间安全和秩序。

第六条 国家倡导诚实守信、健康文明的网络行为，推动传播社会主义核心价值观，采取措施提高全社会的网络安全意识和水平，形成全社会共同参与促进网络安全的良好环境。

第七条 国家积极开展网络空间治理、网络技术研发和标准制定、打击网络违法犯罪等方面的国际交流与合作，推动构建和平、安全、开放、合作的网络空间，建立多边、民主、透明的网络治理体系。

第八条 国家网信部门负责统筹协调网络安全工作和相关监督管理工作。国务院电信主管部门、公安部门和其他有关机关依照本法和有关法律、行政法规的规定，在各自职责范围内负责网络安全保护和监督管理工作。

县级以上地方人民政府有关部门的网络安全保护和监督管理职责，按照国家有关规定确定。

第九条 网络运营者开展经营和服务活动，必须遵守法律、行政法规，尊重社会公德，遵守商业道德，诚实信用，履行网络安全保护义务，接受政府和社会的监督，承担社会责任。

第十条 建设、运营网络或者通过网络提供服务，应当依照法律、行政法规的规定和国家标准的强制性要求，采取技术措施和其他必要措施，保障网络安全、稳定运行，有效应对网络安全事件，防范网络违法犯罪活动，维护网络数据的完整性、保密性和可用性。

第十一条 网络相关行业组织按照章程，加强行业自律，制定网络安全行为规范，指导会员加强网络安全保护，提高网络安全保护水平，促进行业健康发展。

第十二条 国家保护公民、法人和其他组织依法使用网络的权利，促进网络接入普及，提升网络服务水平，为社会提供安全、便利的网络服务，保障网络信息依法有序自由流动。

任何个人和组织使用网络应当遵守宪法法律，遵守公共秩序，尊重社会公德，不得危害网络安全，不得利用网络从事危害国家安全、荣誉和利益，煽动颠覆国家政权、推翻社会主义制度，煽动分裂国家、破坏国家统一，宣扬恐怖主义、极端主义，宣扬民族仇恨、民族歧视，传播暴力、淫秽色情信息，编造、传播虚假信息扰乱经济秩序和社会秩序，以及侵害他人名誉、隐私、知识产权和其他合法权益等活动。

第十三条 国家支持研究开发有利于未成年人健康成长的网络产品和服务，依法惩治利用网络从事危害未成年人身心健康的活动，为未成年人提供安全、健康的网络环境。

第十四条 任何个人和组织有权对危害网络安全的行为向网信、电信、公安等部门举报。收到举报的部门应当及时依法作出处理；不属于本部门职责的，应当及时移送有权处理的部门。

有关部门应当对举报人的相关信息予以保密，保护举报人的合法权益。

## 第二章 网络安全支持与促进

第十五条 国家建立和完善网络安全标准体系。国务院标准化行政主管部门和国务院其他有关部门根据各自的职责，组织制定并适时修订有关网络安全管理以及网络产品、服务和运行安全的国家标准、行业标准。

国家支持企业、研究机构、高等学校、网络相关行业组织参与网络安全国家标准、行业标准的制定。

第十六条 国务院和省、自治区、直辖市人民政府应当统筹规划，加大投入，扶持重点网络安全技术产业和项目，支持网络安全技术的研究开发和应用，推广安全可信的网络产品和服务，保护网络技术知识产权，支持企业、研究机构 and 高等学校等参与国家网络安全技术创新项目。

第十七条 国家推进网络安全社会化服务体系建设，鼓励有关企业、机构开展网络安全认证、检测和风险评估等安全服务。

第十八条 国家鼓励开发网络数据安全保护和利用技术，促进公共数据资源开放，推动技术创新和经济社会发展。

国家支持创新网络安全管理方式，运用网络新技术，提升网络安全保护水平。

第十九条 各级人民政府及其有关部门应当组织开展经常性的网络安全宣传教育，并指导、督促有关单位做好网络安全宣传教育工作。

大众传播媒介应当有针对性地面向社会进行网络安全宣传教育。

第二十条 国家支持企业和高等学校、职业学校等教育培训机构开展网络安全相关教育与培训，采取多种方式培养网络安全人才，促进网络安全人才交流。

### 第三章 网络运行安全

#### 第一节 一般规定

第二十一条 国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改：

(一) 制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任；

(二) 采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施；

(三) 采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月；

(四) 采取数据分类、重要数据备份和加密等措施；

(五) 法律、行政法规规定的其他义务。

第二十二条 网络产品、服务应当符合相关国家标准的强制性要求。网络产品、服务的提供者不得设置恶意程序；发现其网络产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。

网络产品、服务的提供者应当为其产品、服务持续提供安全维护；在规定或者当事人约定的期限内，不得终止提供安全维护。

网络产品、服务具有收集用户信息功能的，其提供者应当向用户明示并取得同意；涉及用户个人信息的，还应当遵守本法和有关法律、行政法规关于个人信息保护的规定。

第二十三条 网络关键设备和网络安全专用产品应当按照相关国家标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求后，方可销售或者提供。国家网信部门会同国务院有关部门制定、公布网络关键设备和网络安全专用产品目录，并推动安全认证和安全检测结果互认，避免重复认证、检测。

第二十四条 网络运营者为用户办理网络接入、域名注册服务，办理固定电话、移动电话等入网手续，或者为用户提供信息发布、即时通讯等服务，在与用户签订协议或者确认提供服务时，应当要求用户提供真实身份信息。用户不提供真实身份信息的，网络运营者不得为其提供相关服务。

国家实施网络可信身份战略，支持研究开发安全、方便的电子身份认证技术，推动不同电子身份认证之间的互认。



第二十五条 网络运营者应当制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险；在发生危害网络安全的事件时，立即启动应急预案，采取相应的补救措施，并按照规定向有关主管部门报告。

第二十六条 开展网络安全认证、检测、风险评估等活动，向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全信息，应当遵守国家有关规定。

第二十七条 任何个人和组织不得从事非法侵入他人网络、干扰他人网络正常功能、窃取网络数据等危害网络安全的活动；不得提供专门用于从事侵入网络、干扰网络正常功能及防护措施、窃取网络数据等危害网络安全活动的程序、工具；明知他人从事危害网络安全的活动的，不得为其提供技术支持、广告推广、支付结算等帮助。

第二十八条 网络运营者应当为公安机关、国家安全机关依法维护国家安全和侦查犯罪的活动提供技术支持和协助。

第二十九条 国家支持网络运营者之间在网络安全信息收集、分析、通报和应急处置等方面进行合作，提高网络运营者的安全保障能力。

有关行业组织建立健全本行业的网络安全保护规范和协作机制，加强对网络安全风险的分析评估，定期向会员进行风险警示，支持、协助会员应对网络安全风险。

第三十条 网信部门和有关部门在履行网络安全保护职责中获取的信息，只能用于维护网络安全的需要，不得用于其他用途。

## 第二节 关键信息基础设施的运行安全

第三十一条 国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。关键信息基础设施的具体范围和安全保护办法由国务院制定。

国家鼓励关键信息基础设施以外的网络运营者自愿参与关键信息基础设施保护体系。

第三十二条 按照国务院规定的职责分工，负责关键信息基础设施安全保护工作的部门分别编制并组织实施本行业、本领域的关键信息基础设施安全规划，指导和监督关键信息基础设施运行安全保护工作。

第三十三条 建设关键信息基础设施应当确保其具有支持业务稳定、持续运行的性能，并保证安全技术措施同步规划、同步建设、同步使用。

第三十四条 除本法第二十一条的规定外，关键信息基础设施的运营者还应当履行下列安全保护义务：

（一）设置专门安全管理机构和安全管理负责人，并对该负责人和关键岗位的人员进行安全背景审查；

（二）定期对从业人员进行网络安全教育、技术培训和技能考核；

（三）对重要系统和数据库进行容灾备份；

（四）制定网络安全事件应急预案，并定期进行演练；

（五）法律、行政法规规定的其他义务。

第三十五条 关键信息基础设施的运营者采购网络产品和服务，可能影响国家安全的，应当通过国家网信部门会同国务院有关部门组织的国家安全审查。

第三十六条 关键信息基础设施的运营者采购网络产品和服务，应当按照规定与提供者签订安全保密协议，明确安全和保密义务与责任。

第三十七条 关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其规定。

第三十八条 关键信息基础设施的运营者应当自行或者委托网络安全服务机构对其网络的安全性和可能存在的风险每年至少进行一次检测评估，并将检测评估情况和改进措施报送相关负责关键信息基础设施安全保护工作的部门。

第三十九条 国家网信部门应当统筹协调有关部门对关键信息基础设施的安全保护采取下列措施：

（一）对关键信息基础设施的安全风险进行抽查检测，提出改进措施，必要时可以委托网络安全服务机构对网络存在的安全风险进行检测评估；

（二）定期组织关键信息基础设施的运营者进行网络安全应急演练，提高应对网络安全事件的水平和协同配合能力；

（三）促进有关部门、关键信息基础设施的运营者以及有关研究机构、网络安全服务机构等之间的网络安全信息共享；

（四）对网络安全事件的应急处置与网络功能的恢复等，提供技术支持和协助。

#### 第四章 网络信息安全

第四十条 网络运营者应当对其收集的用户信息严格保密，并建立健全用户信息保护制度。

第四十一条 网络运营者收集、使用个人信息，应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。

网络运营者不得收集与其提供的服务无关的个人信息，不得违反法律、行政法规的规定和双方的约定收集、使用个人信息，并应当依照法律、行政法规的规定和与用户的约定，处理其保存的个人信息。

第四十二条 网络运营者不得泄露、篡改、毁损其收集的个人信息；未经被收集者同意，不得向他人提供个人信息。但是，经过处理无法识别特定个人且不能复原的除外。

网络运营者应当采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失。在发生或者可能发生个人信息泄露、毁损、丢失的情况时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。

第四十三条 个人发现网络运营者违反法律、行政法规的规定或者双方的约定收集、使用其个人信息的，有权要求网络运营者删除其个人信息；发现网络运营者收集、存储的其个人信息有错误的，有权要求网络运营者予以更正。网络运营者应当采取措施予以删除或者更正。

第四十四条 任何个人和组织不得窃取或者以其他非法方式获取个人信息，不得非法出售或者非法向他人提供个人信息。

第四十五条 依法负有网络安全监督管理职责的部门及其工作人员，必须对在履行职责中知悉的个人信息、隐私和商业秘密严格保密，不得泄露、出售或者非法向他人提供。

第四十六条 任何个人和组织应当对其使用网络的行为负责，不得设立用于实施诈骗，传授犯罪方法，制作或者销售违禁物品、管制物品等违法犯罪活动的网站、通讯群组，不得利用网络发布涉及实施诈骗，制作或者销售违禁物品、管制物品以及其他违法犯罪活动的信息。

第四十七条 网络运营者应当加强对其用户发布的信息的管理，发现法律、行政法规禁止发布或者传输的信息的，应当立即停止传输该信息，采取消除等处置措施，防止信息扩散，保存有关记录，并向有关主管部门报告。

第四十八条 任何个人和组织发送的电子信息、提供的应用软件，不得设置恶意程序，不得含有法律、行政法规禁止发布或者传输的信息。

电子信息发送服务提供者和应用软件下载服务提供者，应当履行安全管理义务，知道其用户有前款规定行为的，应当停止提供服务，采取消除等处置措施，保存有关记录，并向有关主管部门报告。

第四十九条 网络运营者应当建立网络信息安全投诉、举报制度，公布投诉、举报方式等信息，及时受理并处理有关网络信息安全的投诉和举报。

网络运营者对网信部门和有关部门依法实施的监督检查，应当予以配合。

第五十条 国家网信部门和有关部门依法履行网络信息安全监督管理职责，发现法律、行政法规禁止发布或者传输的信息的，应当要求网络运营者停止传输，采取删除等处置措施，保存有关记录；对来源于中华人民共和国境外的上述信息，应当通知有关机构采取技术措施和其他必要措施阻断传播。

## 第五章 监测预警与应急处置

第五十一条 国家建立网络安全监测预警和信息通报制度。国家网信部门应当统筹协调有关部门加强网络安全信息收集、分析和通报工作，按照规定统一发布网络安全监测预警信息。

第五十二条 负责关键信息基础设施安全保护工作的部门，应当建立健全本行业、本领域的网络安全监测预警和信息通报制度，并按照规定报送网络安全监测预警信息。

第五十三条 国家网信部门协调有关部门建立健全网络安全风险评估和应急工作机制，制定网络安全事件应急预案，并定期组织演练。

负责关键信息基础设施安全保护工作的部门应当制定本行业、本领域的网络安全事件应急预案，并定期组织演练。

网络安全事件应急预案应当按照事件发生后的危害程度、影响范围等因素对网络安全事件进行分级，并规定相应的应急处置措施。

第五十四条 网络安全事件发生的风险增大时，省级以上人民政府有关部门应当按照规定的权限和程序，并根据网络安全风险的特点和可能造成的危害，采取下列措施：

（一）要求有关部门、机构和人员及时收集、报告有关信息，加强对网络安全风险的监测；

(二) 组织有关部门、机构和专业人员，对网络安全风险信息进行分析评估，预测事件发生的可能性、影响范围和危害程度；

(三) 向社会发布网络安全风险预警，发布避免、减轻危害的措施。

第五十五条 发生网络安全事件，应当立即启动网络安全事件应急预案，对网络安全事件进行调查和评估，要求网络运营者采取技术措施和其他必要措施，消除安全隐患，防止危害扩大，并及时向社会发布与公众有关的警示信息。

第五十六条 省级以上人民政府有关部门在履行网络安全监督管理职责中，发现网络存在较大安全风险或者发生安全事件的，可以按照规定的权限和程序对该网络的运营者的法定代表人或者主要负责人进行约谈。网络运营者应当按照要求采取措施，进行整改，消除隐患。

第五十七条 因网络安全事件，发生突发事件或者生产安全事故的，应当依照《中华人民共和国突发事件应对法》、《中华人民共和国安全生产法》等有关法律、行政法规的规定处置。

第五十八条 因维护国家安全和社会公共秩序，处置重大突发社会安全事件的需要，经国务院决定或者批准，可以在特定区域对网络通信采取限制等临时措施。

## 第六章 法律责任

第五十九条 网络运营者不履行本法第二十一条、第二十五条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处一万元以上十万元以下罚款，对直接负责的主管人员处五千元以上五万元以下罚款。

关键信息基础设施的运营者不履行本法第三十三条、第三十四条、第三十六条、第三十八条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处十万元以上一百万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款。

第六十条 违反本法第二十二条第一款、第二款和第四十八条第一款规定，有下列行为之一的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处五万元以上五十万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款：

（一）设置恶意程序的；

（二）对其产品、服务存在的安全缺陷、漏洞等风险未立即采取补救措施，或者未按照规定及时告知用户并向有关主管部门报告的；

（三）擅自终止为其产品、服务提供安全维护的。

第六十一条 网络运营者违反本法第二十四条第一款规定，未要求用户提供真实身份信息，或者对不提供真实身份信息的用户提供相关服务的，由有关主管部门责令改正；拒不改正或者情节严重的，处五万元以上五十万元以下罚款，并可以由有关主管部门责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

第六十二条 违反本法第二十六条规定，开展网络安全认证、检测、风险评估等活动，或者向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全信息的，由有关主管部门责令改正，给予警告；拒不改正或者情节严重的，处一万元以上十万元以下罚款，并可以由有关主管部门责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处五千元以上五万元以下罚款。

第六十三条 违反本法第二十七条规定，从事危害网络安全的活动，或者提供专门用于从事危害网络安全活动的程序、工具，或者为他人从事危害网络安全的活动提供技术支持、广告推广、支付结算等帮助，尚不构成犯罪的，由公安机关没收违法所得，处五日以下拘留，可以并处五万元以上五十万元以下罚款；情节较重的，处五日以上十五日以下拘留，可以并处十万元以上一百万元以下罚款。

单位有前款行为的，由公安机关没收违法所得，处十万元以上一百万元以下罚款，并对直接负责的主管人员和其他直接责任人员依照前款规定处罚。

违反本法第二十七条规定，受到治安管理处罚的人员，五年内不得从事网络安全管理和网络运营关键岗位的工作；受到刑事处罚的人员，终身不得从事网络安全管理和网络运营关键岗位的工作。

第六十四条 网络运营者、网络产品或者服务的提供者违反本法第二十二条第三款、第四十一条至第四十三条规定，侵害个人信息依法得到保护的权利的，由有关主管部门责令改正，可以根据情节单处或者并处警告、没收违法所得、处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款；情节严重的，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照。

违反本法第四十四条规定，窃取或者以其他非法方式获取、非法出售或者非法向他人提供个人信息，尚不构成犯罪的，由公安机关没收违法所得，并处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款。

第六十五条 关键信息基础设施的运营者违反本法第三十五条规定，使用未经安全审查或者安全审查未通过的网络产品或者服务的，由有关主管部门责令停止使用，处采购金额一倍以上十倍以下罚款；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

第六十六条 关键信息基础设施的运营者违反本法第三十七条规定，在境外存储网络数据，或者向境外提供网络数据的，由有关主管部门责令改正，给予警告，没收违法所得，处五万元以上五十万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。



第六十七条 违反本法第四十六条规定，设立用于实施违法犯罪活动的网站、通讯群组，或者利用网络发布涉及实施违法犯罪活动的信息，尚不构成犯罪的，由公安机关处五日以下拘留，

可以并处一万元以上十万元以下罚款；情节较重的，处五日以上十五日以下拘留，可以并处五万元以上五十万元以下罚款。关闭用于实施违法犯罪活动的网站、通讯群组。

单位有前款行为的，由公安机关处十万元以上五十万元以下罚款，并对直接负责的主管人员和其他直接责任人员依照前款规定处罚。

第六十八条 网络运营者违反本法第四十七条规定，对法律、行政法规禁止发布或者传输的信息未停止传输、采取消除等处置措施、保存有关记录的，由有关主管部门责令改正，给予警告，没收违法所得；拒不改正或者情节严重的，处十万元以上五十万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

电子信息发送服务提供者、应用软件下载服务提供者，不履行本法第四十八条第二款规定的安全管理义务的，依照前款规定处罚。

第六十九条 网络运营者违反本法规定，有下列行为之一的，由有关主管部门责令改正；拒不改正或者情节严重的，处五万元以上五十万元以下罚款，对直接负责的主管人员和其他直接责任人员，处一万元以上十万元以下罚款：

（一）不按照有关部门的要求对法律、行政法规禁止发布或者传输的信息，采取停止传输、消除等处置措施的；

（二）拒绝、阻碍有关部门依法实施的监督检查的；

（三）拒不向公安机关、国家安全机关提供技术支持和协助的。

第七十条 发布或者传输本法第十二条第二款和其他法律、行政法规禁止发布或者传输的信息的，依照有关法律、行政法规的规定处罚。

第七十一条 有本法规定的违法行为的，依照有关法律、行政法规的规定记入信用档案，并予以公示。

第七十二条 国家机关政务网络的运营者不履行本法规定的网络安全保护义务的，由其上级机关或者有关机关责令改正；对直接负责的主管人员和其他直接责任人员依法给予处分。

第七十三条 网信部门和有关部门违反本法第三十条规定，将在履行网络安全保护职责中获取的信息用于其他用途的，对直接负责的主管人员和其他直接责任人员依法给予处分。

网信部门和有关部门的工作人员玩忽职守、滥用职权、徇私舞弊，尚不构成犯罪的，依法给予处分。

第七十四条 违反本法规定，给他人造成损害的，依法承担民事责任。

违反本法规定，构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。

第七十五条 境外的机构、组织、个人从事攻击、侵入、干扰、破坏等危害中华人民共和国的关键信息基础设施的活动，造成严重后果的，依法追究法律责任；国务院公安部门和有关部门并可以决定对该机构、组织、个人采取冻结财产或者其他必要的制裁措施。

## 第七章 附 则

第七十六条 本法下列用语的含义：

（一）网络，是指由计算机或者其他信息终端及相关设备组成的按照一定的规则和程序对信息进行收集、存储、传输、交换、处理的系统。

（二）网络安全，是指通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

(三) 网络运营者，是指网络的所有者、管理者和网络服务提供者。

(四) 网络数据，是指通过网络收集、存储、传输、处理和产生的各种电子数据。

(五) 个人信息，是指以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。

第七十七条 存储、处理涉及国家秘密信息的网络的运行安全保护，除应当遵守本法外，还应当遵守保密法律、行政法规的规定。

第七十八条 军事网络的安全保护，由中央军事委员会另行规定。

第七十九条 本法自2017年6月1日起施行。

# EXHIBIT C

**Declaration of David Newman  
Principal Deputy Assistant Attorney General  
National Security Division  
Department of Justice**



---

# Certification of Translation

---



COUNTY OF SUFFOLK  
COMMONWEALTH OF MASSACHUSETTS

July 24, 2024

This is to certify that the attached translation is, to the best of my knowledge and belief, a true and accurate translation from Simplified Chinese into English of the attached document:

- **Counterterrorism Law**

Linguistic Systems, Inc. adheres to an ISO-certified quality management system that ensures best practices are always followed in the selection of linguists skilled in both the languages and subject matters necessary for every translation.



Linguistic Systems, Inc.



Linguistic Systems, Inc.

260 Franklin Street, Suite 230, Boston MA 02110 • Phone 617-528-7400 • Fax 617-528-7490 • [www.linguist.com](http://www.linguist.com)

Certifications: ISO 9001 • ISO 17100 • ISO 18587 • ISO 27001

## Anti-Terrorism Law of the People's Republic of China

(Adopted at the 18th Meeting of the Standing Committee of the Twelfth National People's Congress on December 27, 2015; amended according to the "Decision on Amending the Frontier Health and Quarantine Law of the People's Republic of China and Other Six Laws" at the 2nd Meeting of the Standing Committee of the Thirteenth National People's Congress on April 27, 2018)

Browse Font Size: Large Medium Small Source: National People's Congress of China Website June 12, 2018, 14:47:43

### Table of Contents

- Chapter 1: General Provisions
- Chapter 2: Identification of Terrorist Organizations and Personnel
- Chapter 3: Security Precautions
- Chapter 4: Intelligence Information
- Chapter 5: Investigation
- Chapter 6: Response and Handling
- Chapter 7: International Cooperation
- Chapter 8: Safeguard Measures
- Chapter 9: Legal Responsibility
- Chapter 10: Supplementary Provisions

### Chapter 1: General Provisions

Article 1: This Law is formulated in accordance with the Constitution in order to prevent and punish terrorist activities, strengthen anti-terrorism work, and safeguard national security, public safety, and the safety of people's lives and property.

Article 2: The state opposes all forms of terrorism, bans terrorist organizations according to law, and holds accountable anyone who organizes, plans, prepares, or carries out terrorist activities, promotes terrorism, incites the implementation of terrorist activities, organizes, leads, or participates in terrorist organizations, or provides assistance for terrorist activities, according to law.

The state does not compromise with any terrorist organization or personnel and does not provide asylum or refugee status to any terrorist personnel.

Article 3: For the purposes of this Law, terrorism refers to propositions and actions that, through violence, destruction, intimidation, and other means, create social panic, endanger public safety, infringe on personal and property rights, or coerce state organs or international organizations to achieve their political, ideological, and other objectives.

For the purposes of this Law, terrorist activities refer to the following acts of a terrorist nature:

- (1) Organizing, planning, preparing to implement, or implementing activities that cause or intend to cause casualties, significant property damage, damage to public facilities, or severe disruption of social order;
- (2) Promoting terrorism, inciting the implementation of terrorist activities, or illegally possessing items that promote terrorism, and forcing others to wear clothing or symbols promoting terrorism in public places;
- (3) Organizing, leading, or participating in terrorist organizations;
- (4) Providing information, funds, materials, labor, technology, venues, or other support, assistance, or convenience to terrorist organizations, terrorist personnel, the implementation of terrorist activities, or terrorist training;
- (5) Other terrorist activities.

For the purposes of this Law, a terrorist organization refers to a criminal organization composed of three or more persons formed to carry out terrorist activities.

Terrorist personnel refers to individuals who carry out terrorist activities and members of terrorist organizations.

A terrorist incident refers to ongoing or already occurred terrorist activities that cause or may cause significant social harm.

Article 4: The state incorporates anti-terrorism into the national security strategy, adopts comprehensive measures, addresses both symptoms and root causes, strengthens anti-terrorism capabilities, and uses political, economic, legal, cultural, educational, diplomatic, and military means to carry out anti-terrorism work.

The state opposes all forms of extremism that incite hatred, incite discrimination, or promote violence by distorting religious doctrines or other methods, and eliminates the ideological foundation of terrorism.

Article 5: Anti-terrorism work adheres to the principles of combining specialized work with mass participation, prioritizing prevention, combining punishment and prevention, taking preemptive measures, and maintaining initiative.

Article 6: Anti-terrorism work shall be conducted in accordance with the law, respecting and safeguarding human rights, and protecting the legitimate rights and interests of citizens and organizations.

In anti-terrorism work, citizens' freedom of religious belief and ethnic customs and habits shall be respected, and any discriminatory practices based on region, ethnicity, religion, or other reasons are prohibited.

Article 7: The state establishes a leading body for anti-terrorism work to unify the leadership and command of anti-terrorism work nationwide.

Municipal governments at the prefecture level and above shall establish leading bodies for anti-terrorism work, and county-level governments shall establish such bodies as needed. These bodies are responsible for anti-terrorism work in their respective areas under the leadership and command of higher-level anti-terrorism bodies.

Article 8: Public security organs, national security organs, people's procuratorates, people's courts, judicial administrative organs, and other relevant state organs shall, according to their division of labor, implement a work responsibility system and lawfully carry out anti-terrorism work.

The People's Liberation Army, the People's Armed Police Force, and militia organizations shall, in accordance with this law, other relevant laws, administrative regulations, military regulations, and orders from the State Council and the Central Military Commission, as well as the deployment by the anti-terrorism leading bodies, prevent and handle terrorist activities.

Relevant departments shall establish a coordinated mechanism, relying on and mobilizing village committees, neighborhood committees, enterprises, institutions, and social organizations to jointly carry out anti-terrorism work.

Article 9: Any unit or individual has the obligation to assist and cooperate with relevant departments in anti-terrorism work. If terrorist activity suspects or suspected terrorist personnel are discovered, they shall promptly report to public security organs or relevant departments.

Article 10: Units and individuals who make outstanding contributions in reporting terrorist activities or assisting in preventing and stopping terrorist activities, as well as those who make other notable contributions in anti-terrorism work, shall be recognized and rewarded according to relevant national regulations.



Article 11: The People's Republic of China shall exercise criminal jurisdiction and pursue criminal responsibility for terrorist activities or crimes committed outside the territory of the People's Republic of China against its state, citizens, or institutions, or for terrorist activities or crimes defined in international treaties concluded or participated in by the People's Republic of China.

## Chapter 2: Identification of Terrorist Organizations and Personnel

Article 12: The national anti-terrorism work leading body shall, in accordance with the provisions of Article 3 of this Law, identify terrorist organizations and personnel, and such identifications shall be announced by the office of the national anti-terrorism work leading body.

Article 13: Public security departments, national security departments, diplomatic departments of the State Council, and provincial-level anti-terrorism work leading bodies that need to identify terrorist organizations and personnel shall apply to the national anti-terrorism work leading body.

Article 14: Financial institutions and specific non-financial institutions shall immediately freeze the funds or other assets of the terrorist organizations and personnel announced by the office of the national anti-terrorism work leading body, and report to the State Council's public security departments, national security departments, and anti-money laundering administrative authorities in accordance with regulations.

Article 15: Terrorist organizations and personnel identified as such may apply for re-evaluation through the office of the national anti-terrorism work leading body if they disagree with the identification. The national anti-terrorism work leading body shall promptly conduct the re-evaluation and make a decision to either uphold or revoke the identification. The re-evaluation decision is final.

If the national anti-terrorism work leading body decides to revoke an identification, the office of the national anti-terrorism work leading body shall announce it; if funds or assets were frozen, the freeze shall be lifted.

Article 16: According to the Criminal Procedure Law, intermediate or higher-level people's courts with jurisdiction may lawfully identify terrorist organizations and personnel during the trial of criminal cases. For those that need to be announced by the office of the national anti-terrorism work leading body after the judgment becomes effective, the relevant provisions of this chapter shall apply.

## Chapter 3: Security Precautions

Article 17: Governments at all levels and relevant departments shall organize and conduct anti-terrorism publicity education to raise citizens' awareness of anti-terrorism.

Education, human resources administrative departments, schools, and relevant vocational training institutions shall include terrorism prevention and emergency knowledge in their educational, teaching, and training content.

Media, broadcasting, television, culture, religious organizations, and internet-related units shall carry out targeted anti-terrorism publicity education for the public.

Village committees and neighborhood committees shall assist governments and relevant departments in strengthening anti-terrorism publicity education.

Article 18: Telecommunications operators and internet service providers shall provide technical interfaces and decryption and other technical support and assistance to public security organs and national security organs for the prevention and investigation of terrorist activities according to the law.

Article 19: Telecommunications operators and internet service providers shall implement network security and information content supervision systems, and apply security technical measures according to laws and regulations to prevent the dissemination of information containing terrorism or extremism content. If such information is found, they must immediately stop transmission, retain relevant records, delete the information, and report it to public security organs or relevant departments.

Relevant departments such as cyberspace, telecommunications, public security, and national security shall, according to their responsibilities, promptly instruct relevant units to stop transmission, delete relevant information, or shut down relevant websites and services. The relevant units must immediately comply, retain relevant records, and assist in investigations. For information containing terrorism or extremism content that is transmitted across borders on the internet, telecommunications authorities shall take technical measures to block its dissemination.

Article 20: Freight and logistics operators in railways, highways, waterways, aviation, as well as postal and courier services, shall implement a security inspection system, verify customer identities, and conduct safety checks or open and inspect items according to regulations. Items that are prohibited from transport or delivery, pose significant safety risks, or are items for which customers refuse security checks, must not be transported or delivered.

The logistics operators mentioned in the previous paragraph shall implement a registration system for customer identities and item information for transportation and delivery.

Article 21: Telecommunications, internet, financial, accommodation, long-distance passenger transport, motor vehicle rental, and other service providers shall verify customer identities. Services shall not be provided to individuals with unknown identities or those who refuse identity verification.

Article 22: Production and import units shall, according to regulations, provide electronic tracking labels for firearms, weapons, ammunition, controlled tools, hazardous chemicals, civil explosives, and nuclear and radioactive materials, and add security inspection tracking labels to civil explosives.

Transportation units shall monitor the transportation vehicles of hazardous chemicals, civil explosives, and nuclear and radioactive materials using a positioning system as required by regulations.

Relevant units shall strictly supervise and manage substances such as infectious disease pathogens, and rigorously prevent the spread of infectious disease pathogens or their entry into illegal channels.

For controlled tools, hazardous chemicals, and civil explosives, relevant departments of the State Council or provincial governments may, as needed, impose controls on production, import, export, transportation, sale, use, and disposal within specific areas and times. They may also prohibit transactions using cash or physical goods, or impose other restrictions on transactions.

Article 23: If firearms, weapons, ammunition, hazardous chemicals, civil explosives, nuclear and radioactive materials, or infectious disease pathogens are stolen, robbed, lost, or otherwise misappropriated, the unit where the incident occurred shall immediately take necessary control measures and report to the public security organs without delay, while also reporting to the relevant supervisory departments as required. Upon receiving the report, public security organs shall promptly conduct an investigation. Relevant supervisory departments shall cooperate with the public security organs in their work.

No unit or individual shall illegally manufacture, produce, store, transport, import, export, sell, provide, purchase, use, possess, dispose of, or destroy the items specified in the preceding

paragraph. Items discovered by public security organs shall be seized; items discovered by other supervisory departments shall be seized and reported to the public security organs immediately; items discovered by other units or individuals shall be reported to the public security organs immediately.

Article 24: The State Council's anti-money laundering administrative department, along with relevant departments and institutions of the State Council, shall supervise and manage financial institutions and specific non-financial institutions' compliance with anti-terrorism financing obligations.

If the State Council's anti-money laundering administrative department suspects terrorism financing, it may conduct an investigation and take provisional freezing measures according to the law.

Article 25: During the supervision and inspection of relevant units by auditing, finance, and tax departments according to laws and administrative regulations, if they discover that funds flowing in and out are suspected of terrorism financing, they shall promptly report to the public security organs.

Article 26: Customs shall, during the supervision of cash and bearer securities carried by persons entering or leaving the country, immediately report any suspicion of terrorism financing to the State Council's anti-money laundering administrative department and the competent public security organs.

Article 27: Local people's governments at all levels shall ensure that urban and rural planning complies with the needs of anti-terrorism work.

Local people's governments at all levels shall, as needed, organize and urge relevant construction units to equip and install public safety video surveillance systems and other technical and physical preventive equipment and facilities at key locations on major roads, transportation hubs, and urban public areas to prevent terrorist attacks.

Article 28: Public security organs and relevant departments shall promptly stop and legally pursue those who advocate extremism, use extremism to harm public safety, disrupt public order, infringe on personal property, or obstruct social management.

When public security organs discover extremism activities, they shall order an immediate halt, forcibly remove and register the identities of those involved, confiscate related items and

materials, and seal off illegal activity locations.

Any unit or individual who discovers items, materials, or information promoting extremism shall report to the public security organs immediately.

Article 29: For individuals who are incited, coerced, or lured into participating in terrorism or extremism activities, or who participate in such activities in a minor capacity that does not constitute a crime, public security organs shall organize relevant departments, village committees, residential committees, workplaces, schools, families, and guardians to provide assistance and education.

Prisons, detention centers, and community correction institutions shall strengthen management, education, and correctional work for convicted terrorists and extremists. Prisons and detention centers may, based on the needs of education and correction and maintaining order, either mix terrorists and extremists with ordinary criminals or isolate them.

Article 30: For criminals convicted of terrorist activities and extremist crimes who have been sentenced to imprisonment or higher penalties, prisons and detention centers shall conduct an assessment of social danger before their release, based on the nature of their crimes, circumstances, degree of social harm, behavior during imprisonment, and the impact on the community where they will reside after release. In conducting the social danger assessment, opinions from relevant grassroots organizations and the original investigating authorities should be heard. If the assessment indicates a social danger, the prison or detention center shall propose resettlement and education suggestions to the Intermediate People's Court where the criminal is serving the sentence, and a copy of the proposal shall be sent to the People's Procuratorate at the same level.

Criminals who are assessed as having social danger by the Intermediate People's Court where they are serving their sentences should be ordered to receive resettlement and education after their release. The decision should be made before the criminal's release, and a copy of the decision should be sent to the People's Procuratorate at the same level. Individuals who disagree with the resettlement and education decision can apply for reconsideration to a higher People's Court.

Resettlement and education are organized and implemented by the provincial government. The resettlement and education institutions should evaluate the individuals annually. For those who show true repentance and are no longer deemed a threat to society, the institution should

promptly propose lifting the resettlement and education measure, which will be decided by the Intermediate People's Court that initially decided on the resettlement and education. Individuals under resettlement and education have the right to apply for its termination.

The people's procuratorate shall supervise the decisions and implementation of education placement.

Article 31: Public security organs, together with relevant departments, shall identify units, locations, activities, and facilities that are at high risk of terrorist attacks and could cause significant personal injury, property damage, or social impact as key targets for terrorism prevention. These identifications shall be reported to the anti-terrorism work leadership organization at the same level for record-keeping.

Article 32: The management units of key targets shall fulfill the following responsibilities:

- (1) Develop plans and measures for preventing and responding to terrorist activities, and conduct regular training and drills.
- (2) Establish a special fund guarantee system for anti-terrorism work and equip and update prevention and response equipment and facilities.
- (3) Designate relevant agencies or assign responsible personnel, and clearly define their duties.
- (4) Implement risk assessments, monitor security threats in real-time, and improve internal security management.
- (5) Regularly report the implementation of prevention measures to public security organs and relevant departments.

Management units of key targets shall design, construct, and operate anti-terrorism technical and physical prevention equipment and facilities in accordance with urban and rural planning, relevant standards, and actual needs, as specified in Article 27 of this law.

Management units of key targets shall establish management systems for public safety video surveillance, including duty monitoring, information storage and use, and operation and maintenance, to ensure the normal operation of related systems. The video surveillance footage must be stored for no less than ninety days.

For other units, locations, activities, and facilities related to public safety that are not key targets, their supervisory departments and management units shall establish and improve safety management systems and fulfill safety responsibilities according to laws and administrative regulations.

Article 33: Management units of key targets shall conduct background checks on personnel

in important positions. Personnel with unsuitable circumstances should be reassigned, and the relevant situation should be reported to the public security organs.

Article 34: Large event organizers and management units of key targets shall, according to regulations, conduct security checks on personnel, items, and vehicles entering large event venues, airports, train stations, docks, urban rail transit stations, highway long-distance passenger stations, ports, and other key targets. Prohibited and controlled items should be seized and reported to the public security organs immediately; suspected illegal or criminal personnel should also be reported to the public security organs immediately.

Article 35: For public transportation vehicles such as aircraft, trains, ships, urban rail vehicles, and public buses, operating units shall provide security personnel and corresponding equipment and facilities according to regulations, and strengthen security checks and protective work.

Article 36: Public security organs and relevant departments shall keep track of basic information and important developments of key targets, and guide and supervise management units of key targets in fulfilling their anti-terrorism responsibilities.

Public security organs and the People's Armed Police Force of China shall conduct vigilance, patrols, and inspections on key targets in accordance with relevant regulations.

Article 37: Flight control, civil aviation, and public security departments shall, according to their respective duties, strengthen the management of airspace, aircraft, and flight activities, and rigorously prevent terrorist activities targeting aircraft or using flight activities.

Article 38: All levels of people's governments and military agencies shall set up barriers, video surveillance, and anti-crossing alarm facilities at key national (border) areas and ports.

Public security organs and the People's Liberation Army of China shall organize border patrols rigorously and, according to regulations, inspect personnel, transportation vehicles, and items at the border, border management areas, and border passages and ports, as well as vessels in coastal and border regions.

Article 39: Issuing authorities of exit and entry documents and border inspection authorities have the right to decide to deny the exit or entry of individuals involved in terrorist activities or suspected of such activities, not issue exit or entry documents, or declare their exit or entry documents invalid.

Article 40: Customs and border inspection authorities shall detain suspected terrorist individuals or items related to terrorist activities in accordance with the law, and immediately transfer them to public security organs or national security organs.

Article 41: The State Council's departments for foreign affairs, public security, national security, development and reform, industry and information technology, commerce, and tourism shall establish safety risk assessment systems for overseas investment, cooperation, and tourism. They shall strengthen security protection for Chinese citizens abroad, and for overseas institutions, facilities, and property to prevent and respond to terrorist attacks.

Article 42: Overseas institutions shall establish and improve safety prevention systems and response plans, and enhance the protection of relevant personnel, facilities, and property.

#### Chapter 4: Intelligence and Information

Article 43: The National Anti-Terrorism Work Leadership Agency shall establish the National Anti-Terrorism Intelligence Center, implementing an inter-departmental and inter-regional intelligence information work mechanism to coordinate anti-terrorism intelligence information work.

Relevant departments shall strengthen the collection of anti-terrorism intelligence information. Information on relevant clues, individuals, and actions should be promptly and uniformly submitted to the National Anti-Terrorism Intelligence Center in accordance with regulations.

Local anti-terrorism work leadership agencies shall establish inter-departmental intelligence information work mechanisms, organize anti-terrorism intelligence information work, and report important intelligence information to higher-level anti-terrorism work leadership agencies in a timely manner. Emergency intelligence information involving other regions should be promptly communicated to the relevant local authorities.

Article 44: Public security organs, national security organs, and relevant departments should rely on the public, strengthen grassroots work, establish grassroots intelligence information work forces, and enhance the capability of anti-terrorism intelligence information work.

Article 45: Public security organs, national security organs, and military agencies, within their scope of responsibilities and based on the needs of anti-terrorism intelligence information work, may adopt technical reconnaissance measures according to national regulations, following



strict approval procedures.

Materials obtained through such measures can only be used for anti-terrorism response, investigation, prosecution, and trial of terrorism-related and extremism crimes, and not for other purposes.

Article 46: Relevant departments shall provide information obtained during the security prevention work outlined in Chapter 3 of this law, as required by the National Anti-Terrorism Intelligence Center, in a timely manner.

Article 47: The National Anti-Terrorism Intelligence Center, local anti-terrorism work leadership agencies, and relevant departments such as public security organs shall screen, analyze, verify, and monitor relevant intelligence information. If they believe there is a danger of terrorist events and that corresponding safety prevention and response measures are needed, they shall promptly notify relevant departments and units and may issue warnings based on the situation. Relevant departments and units should carry out safety prevention and response measures based on the notification.

Article 48: Anti-terrorism work leadership agencies, relevant departments, units, and individuals must keep state secrets, commercial secrets, and personal privacy confidential when performing their anti-terrorism duties and obligations.

Those who violate regulations and disclose state secrets, commercial secrets, or personal privacy will be held legally accountable.

#### Chapter 5: Investigation

Article 49: When public security organs receive a report of suspected terrorist activities or discover a suspicion of terrorist activities that requires investigation and verification, they shall promptly conduct an investigation.

Article 50: In investigating suspected terrorist activities, public security organs may, in accordance with relevant laws, interrogate, inspect, and summon the suspects. They may collect or extract biometric information such as photographs, fingerprints, iris images, and biological samples like blood, urine, and shed cells, and retain their signatures.

Public security organs investigating suspected terrorist activities may notify individuals with relevant information to come to the public security organs or other locations for questioning.

Article 51: Public security organs investigating suspected terrorist activities have the authority to collect and obtain relevant information and materials from relevant units and individuals. These units and individuals must provide the information truthfully.

Article 52: Public security organs investigating suspected terrorist activities may, with the approval of the head of the public security organ at or above the county level, investigate the suspect's assets, including bank deposits, remittances, bonds, stocks, and fund shares, and may implement measures such as sealing, seizing, or freezing assets. The period for such measures must not exceed two months. If the situation is complex, the period may be extended for one month with the approval of a higher-level public security organ.

Article 53: Public security organs investigating suspected terrorist activities, with the approval of the head of the public security organ at or above the county level, may impose one or more of the following restrictive measures on suspects of terrorist activities, depending on the degree of danger:

Article 53: Public security organs investigating suspected terrorist activities, with the approval of the head of the public security organ at or above the county level, may impose one or more of the following restrictive measures on suspects of terrorist activities, depending on the degree of danger:

(1) Without the approval of the public security organ, the suspect must not leave the city, county, or designated place where they reside.

(2) The suspect must not participate in large-scale mass activities or engage in specific activities.

(3) Without the approval of the public security organ, the suspect must not use public transportation or enter specific locations.

(4) The suspect must not meet or communicate with certain individuals.

(5) The suspect must regularly report their activities to the public security organ.

(6) The suspect must surrender their passport, identification documents, and driver's license to the public security organ for safekeeping.

Public security organs may supervise compliance with these restrictive measures through electronic monitoring, irregular inspections, and other methods.

The duration of the restrictive measures specified in the previous two paragraphs shall not exceed three months. If there is no need to continue the restrictive measures, they shall be lifted

promptly.

Article 54: If the public security organs discover criminal facts or suspects through investigation, they shall initiate a criminal investigation in accordance with the Criminal Procedure Law. If the relevant deadlines specified in this chapter expire and the public security organs have not initiated a criminal investigation, the relevant measures shall be lifted.

#### Chapter 6: Response and Disposal

Article 55: The state shall establish and improve the response and disposal plan system for terrorist incidents.

The national anti-terrorism work leadership agency shall develop national response and disposal plans for terrorist incidents based on the patterns, characteristics, and potential social harm of such incidents. These plans shall specify the organizational command system for responding to and handling terrorist incidents, as well as the procedures for security prevention, response, and post-incident restoration of social order.

Relevant departments and local anti-terrorism work leadership agencies shall formulate corresponding response and disposal plans.

Article 56: For the response and disposal of terrorist incidents, anti-terrorism work leadership agencies at all levels shall establish command institutions with participation from relevant departments, implementing a system of command responsibility. The head of the anti-terrorism work leadership agency can serve as the commander or designate a leader from the public security agency or other member units of the anti-terrorism work leadership agency to serve as the commander.

In the case of terrorist incidents or particularly severe terrorist incidents occurring across provinces, autonomous regions, or municipalities directly under the central government, the national anti-terrorism work leadership agency shall be responsible for commanding the response and disposal. For terrorist incidents or major terrorist incidents involving multiple administrative regions within a province, autonomous region, or municipality, the provincial anti-terrorism work leadership agency shall be responsible for commanding the response and disposal.

Article 57: After a terrorist incident occurs, the anti-terrorism work leadership agency at the incident location shall immediately activate the terrorist incident response and disposal plan and

appoint a commander. Relevant departments, the People's Liberation Army, the People's Armed Police Force, and militia organizations shall, under the unified leadership and command of the anti-terrorism work leadership agency and the commander, jointly carry out on-site response and disposal work including suppression, control, rescue, and medical assistance.

Higher-level anti-terrorism work leadership agencies may provide guidance on the response and disposal work and, if necessary, mobilize relevant anti-terrorism forces for support.

If an emergency state needs to be declared, the Standing Committee of the National People's Congress or the State Council shall decide according to the Constitution and other relevant legal provisions.

Article 58: Upon discovering a terrorist incident or suspected terrorist incident, the public security organ shall immediately handle the situation and report to the anti-terrorism work leadership agency. If the People's Liberation Army or the People's Armed Police Force discovers that a terrorist activity is in progress, they shall immediately control the situation and promptly transfer the case to the public security organ.

If the anti-terrorism work leadership agency has not yet appointed a commander, the highest-ranking officer from the public security organ present at the scene shall serve as the on-site commander. If the public security organ has not arrived at the scene, the highest-ranking officer from the People's Liberation Army or the People's Armed Police Force present shall serve as the on-site commander. All on-site response personnel, regardless of their unit or system affiliation, shall follow the commands of the on-site commander.

Once the commander is appointed, the on-site commander shall consult with and report to the commander regarding work or relevant situations.

Article 59: When institutions, personnel, or important facilities of the People's Republic of China abroad suffer or are likely to suffer from terrorist attacks, the relevant departments of the State Council, including foreign affairs, public security, national security, commerce, finance, state asset supervision, tourism, and transportation, shall promptly activate the response and disposal plans. The foreign affairs department of the State Council shall coordinate with the relevant countries to take appropriate measures.

After a severe terrorist attack on institutions, personnel, or important facilities of the People's Republic of China abroad, and with the consent of the relevant countries, the national anti-terrorism work leadership agency may organize staff from the foreign affairs, public security, and

national security departments to go abroad to carry out response and disposal work.\*

Article 60: In responding to and disposing of terrorist incidents, priority shall be given to protecting the personal safety of individuals directly harmed or threatened by the terrorist activity

Article 61: After a terrorist incident occurs, the anti-terrorism work leadership agency responsible for the response and disposal may decide that relevant departments and units take one or more of the following response and disposal measures:

(1) Organize the rescue and medical treatment of victims, evacuate, relocate, and properly arrange for threatened individuals, and take other relief measures.

(2) Seal off the scene and surrounding roads, verify the identification documents of individuals at the scene, and set up temporary security perimeters near relevant locations.

(3) Implement airspace and maritime control in specific areas, and inspect transportation vehicles within those areas.

(4) Enforce internet, radio, and communication controls in specific areas.

(5) Implement exit and entry controls in specific areas or for specific individuals.

(6) Prohibit or restrict the use of relevant equipment and facilities, close or restrict access to specific locations, and suspend activities with large crowds or production operations that might exacerbate the threat.

(7) Repair damaged public facilities, including transportation, telecommunications, internet, broadcasting, water supply, drainage, electricity, gas, and heating services.

(8) Organize volunteers for anti-terrorism rescue work and request the services of individuals with specific expertise.

(9) Implement other necessary response and disposal measures.

Measures for response and disposal as outlined in items 3 through 5 of the previous paragraph shall be decided or approved by anti-terrorism work leadership agencies at the provincial level or higher. Measures for response and disposal as outlined in item 6 of the previous paragraph shall be decided by anti-terrorism work leadership agencies at the municipal level or higher. The response and disposal measures should clearly define the applicable time and spatial scope and be announced to the public.

Article 62: People's police, armed police, and other personnel legally equipped with and carrying weapons may use weapons against individuals who, at the scene, are wielding firearms, knives, or other deadly weapons, or using other dangerous methods, and are either currently or

preparing to engage in violent acts, if warnings are ineffective. In emergencies or where warnings might lead to more severe consequences, weapons may be used directly.

Article 63: Information on the occurrence, development, and response to terrorism incidents shall be uniformly issued by the provincial anti-terrorism work leadership agency at the site of the incident. For terrorism incidents occurring across provinces, autonomous regions, or directly governed municipalities, the designated provincial anti-terrorism work leadership agency shall issue the information uniformly.

No organization or individual shall fabricate or spread false information about terrorist incidents. It is prohibited to report or disseminate the details of terrorist activities that could incite imitation, or to publish cruel and inhumane scenes from terrorist incidents. During the handling and response to terrorist incidents, except for news media approved by the leading anti-terrorism authority responsible for releasing information, it is forbidden to report or disseminate the identities of on-site response personnel, hostages, or details of the response actions.

Article 64: After the conclusion of the response to a terrorist incident, people's governments at all levels shall organize relevant departments to assist affected units and individuals in promptly restoring their lives and production, and stabilize social order and public sentiment in the affected areas.

Article 65: Local people's governments shall promptly provide appropriate assistance to the victims of terrorist incidents and their close relatives and timely provide basic living security to those who have lost basic living conditions. Departments responsible for health and medical security shall provide psychological and medical assistance to the victims of terrorist incidents and their close relatives.

Article 66: Public security organs shall promptly file a case for investigation of terrorist incidents, ascertain the causes, process, and outcomes of the incidents, and legally hold the terrorist organizations and individuals criminally responsible.

Article 67: Anti-terrorism work leadership agencies should comprehensively analyze, summarize, and evaluate the occurrence and handling of terrorist events. They should propose improvements for prevention and response measures and report to the higher-level anti-terrorism work leadership agency.

#### Chapter 7 International Cooperation

Article 68: The People's Republic of China, based on international treaties it has concluded

or joined, or according to the principle of equality and mutual benefit, will conduct anti-terrorism cooperation with other countries, regions, and international organizations.

Article 69: Relevant departments of the State Council, authorized by the State Council, represent the Chinese government in anti-terrorism policy dialogues, intelligence information exchanges, law enforcement cooperation, and international financial regulation cooperation with foreign governments and relevant international organizations.

Without violating Chinese law, local governments at the county level or above in border areas and their competent departments, with approval from the State Council or relevant central departments, may engage in anti-terrorism intelligence information exchanges, law enforcement cooperation, and international financial regulation cooperation with neighboring countries or regions.

Article 70: Criminal justice assistance, extradition, and the transfer of convicted persons involved in terrorist activities will be carried out in accordance with relevant legal provisions.

Article 71: With agreements reached with relevant countries and approved by the State Council, the State Council's public security and national security departments may send personnel abroad to carry out anti-terrorism tasks.

Personnel from the People's Liberation Army and the People's Armed Police Force who are sent abroad to carry out anti-terrorism tasks must be approved by the Central Military Commission.

Article 72: Materials obtained through international anti-terrorism cooperation may be used as evidence in administrative penalties and criminal proceedings, except where China has committed not to use them as evidence.

## Chapter 8: Safeguard Measures

Article 73: The State Council and local governments at or above the county level should allocate anti-terrorism work funds separately in their respective budgets according to their responsibilities.

The state will provide necessary financial support to key anti-terrorism areas and ensure funding for responding to and handling large-scale terrorist incidents.

Article 74: Public security organs, state security organs, and relevant departments, as well as the People's Liberation Army and the People's Armed Police Force, should establish specialized

anti-terrorism forces, strengthen professional training, and equip necessary anti-terrorism professional equipment and facilities according to their legal responsibilities.

County-level and township-level people's governments should, as needed, guide relevant units, village committees, and neighborhood committees to establish anti-terrorism work forces and volunteer teams, assisting and cooperating with relevant departments in anti-terrorism work.

Article 75: Personnel who are injured or killed while performing anti-terrorism duties or assisting and cooperating with relevant departments in anti-terrorism work shall be given corresponding treatment according to national regulations.

Article 76: For individuals or their immediate family members whose personal safety is at risk due to reporting and stopping terrorist activities, testifying in terrorist criminal cases, or engaging in anti-terrorism work, upon application by the individual or their immediate family members, public security organs and relevant departments shall take one or more of the following protective measures:

- (1) Not disclosing personal information such as real name, address, and work unit;
- (2) Prohibiting specific individuals from contacting the protected person;
- (3) Implementing specialized protective measures for personal safety and residence;
- (4) Changing the protected person's name, and reassigning their residence and work unit;
- (5) Other necessary protective measures.

Public security organs and relevant departments shall, in accordance with the preceding provisions, take measures such as not disclosing the real name and address of the protected unit, prohibiting specific individuals from approaching the protected unit, implementing specialized protective measures for the office and operational premises of the protected unit, and other necessary protective measures.

Article 77: The state encourages and supports scientific research and technological innovation in anti-terrorism, and the development and promotion of advanced anti-terrorism technologies and equipment.

Article 78: In cases of urgent needs arising from fulfilling anti-terrorism duties, public security organs, national security organs, the People's Liberation Army, and the People's Armed Police Force may requisition property from units and individuals according to national regulations. After the task is completed, the property should be promptly returned or restored to its original state, and corresponding costs should be paid as stipulated; if losses are incurred, compensation should be provided.



If the implementation of counter-terrorism work causes damage to the legal rights and interests of relevant units and individuals, compensation and restitution should be provided according to the law. Relevant units and individuals have the right to request compensation and restitution in accordance with the law.

#### Chapter 9 Legal Responsibilities

Article 79: Those who organize, plan, prepare for, or carry out terrorist activities, promote terrorism, incite terrorist activities, illegally possess items that promote terrorism, force others to wear clothing or display symbols that promote terrorism in public places, organize, lead, or participate in terrorist organizations, or provide assistance to terrorist organizations, terrorist personnel, or in the execution of terrorist activities or training, shall be held criminally liable according to the law.

Article 80: Those who participate in any of the following activities, where the circumstances are minor and do not yet constitute a crime, shall be detained by the public security organs for not less than ten days and not more than fifteen days, and may also be fined up to ten thousand yuan:

- (1) Promoting terrorism, extremism, or inciting terrorist or extremist activities;
- (2) Producing, disseminating, or illegally possessing items that promote terrorism or extremism;
- (3) Forcing others to wear clothing or display symbols that promote terrorism or extremism in public places;
- (4) Providing information, funds, materials, services, technology, or venues to support, assist, or facilitate the promotion of terrorism or extremism, or the execution of terrorist or extremist activities.

Article 81: Utilizing extremism to engage in any of the following acts, where the circumstances are minor and do not constitute a crime, shall be punished by the public security organs with detention of not less than five days but not more than fifteen days, and may also be fined up to ten thousand yuan:

- (1) Forcing others to participate in religious activities, or compelling others to provide property or labor to religious places or religious personnel;
- (2) Intimidating, harassing, or otherwise driving away people of other ethnic groups or those with different beliefs from their place of residence;

(3) Intimidating, harassing, or otherwise interfering with others' interactions and cohabitation with people of other ethnic groups or different beliefs;

(4) Intimidating, harassing, or otherwise interfering with others' customs, lifestyle, and business operations;

(5) Obstructing state officials from performing their duties in accordance with the law;

(6) Distorting or defaming national policies, laws, or administrative regulations, inciting or instigating resistance to the lawful management of the people's government;

(7) Inciting or coercing the public to destroy or intentionally damage national legal documents such as resident identity cards, household registration books, or currency;

(8) Inciting or coercing others to replace marriage or divorce registration with religious ceremonies;

(9) Inciting or coercing minors to refuse compulsory education;

(10) Other actions that use extremism to undermine the implementation of national legal systems.

Article 82: If a person, knowing that others are involved in terrorist activities or extremist crimes, shelters or harbors them, and the circumstances are minor and do not constitute a crime, or if they refuse to provide information when judicial organs investigate or collect evidence related to the case, they shall be detained by the public security organs for not less than ten days but not more than fifteen days, and may also be fined up to ten thousand yuan.

Article 83: If financial institutions and specific non-financial institutions fail to immediately freeze the funds or other assets of terrorist organizations and personnel announced by the national anti-terrorism leadership institution, they shall be fined by the public security organs between two hundred thousand yuan and five hundred thousand yuan. Additionally, directly responsible directors, senior management, and other directly responsible personnel shall be fined up to one hundred thousand yuan. If the circumstances are severe, they shall be fined between five hundred thousand yuan and one million yuan, and the directly responsible directors, senior management, and other directly responsible personnel shall be fined between one hundred thousand yuan and five hundred thousand yuan, and may also be detained by the public security organs for not less than five days but not more than fifteen days.

Article 84: If telecommunications operators or internet service providers engage in any of the following situations, they shall be fined by the competent department between two hundred thousand yuan and five hundred thousand yuan. Additionally, directly responsible managers and

other directly responsible personnel shall be fined up to one hundred thousand yuan. If the circumstances are severe, they shall be fined more than five hundred thousand yuan, and the directly responsible managers and other directly responsible personnel shall be fined between one hundred thousand yuan and five hundred thousand yuan. The public security organs may also detain the directly responsible managers and other directly responsible personnel for not less than five days but not more than fifteen days:

(1) Failing to provide technical interfaces, decryption, and other technical support and assistance to public security organs or national security organs for the prevention and investigation of terrorist activities as required by regulations.

(2) Failing to stop the transmission or delete information containing terrorism or extremism content, failing to save relevant records, or failing to close related websites or shut down related services as required by the competent department.

(3) Failing to implement cybersecurity, information content supervision systems, and security technical prevention measures, resulting in the dissemination of information containing terrorism or extremism content, with serious circumstances.

Article 85: If railway, highway, maritime, aviation freight, and postal or express delivery logistics operators are involved in any of the following situations, they shall be fined by the competent department between one hundred thousand yuan and five hundred thousand yuan. Additionally, directly responsible managers and other directly responsible personnel shall be fined up to one hundred thousand yuan:

(1) Failing to implement a security inspection system to verify the identity of customers, or not performing security checks or unsealing inspections of transported or delivered items as required;

(2) Transporting or delivering items that are prohibited, pose significant security risks, or whose customers refuse security inspections;

(3) Failing to implement a registration system for the identity of customers and information on items being transported or delivered.

Article 86: If telecommunications, internet, and financial business operators and service

providers fail to verify customer identities as required, or provide services to customers with unknown identities or those who refuse identity verification, the competent department shall order them to make corrections. If they refuse to make corrections, they shall be fined between two hundred thousand yuan and five hundred thousand yuan. Directly responsible managers and other directly responsible personnel shall be fined up to one hundred thousand yuan. If the situation is severe, they shall be fined more than five hundred thousand yuan, and directly responsible managers and other directly responsible personnel shall be fined between one hundred thousand yuan and five hundred thousand yuan.

For accommodation, long-distance passenger transport, and motor vehicle rental operators and service providers involved in the above-mentioned situations, the competent department shall impose a fine between one hundred thousand yuan and five hundred thousand yuan, and directly responsible managers and other directly responsible personnel shall be fined up to one hundred thousand yuan.

Article 87 For violations of this law with the following circumstances, the competent department shall issue a warning and order corrections; if corrections are not made, a fine of up to one hundred thousand yuan shall be imposed, and directly responsible managers and other directly responsible personnel shall be fined up to ten thousand yuan:

(1) Failure to electronically track and label weapons such as firearms, ammunition, control devices, hazardous chemicals, civilian explosives, nuclear and radioactive materials, or to add security traceable markers to civilian explosives as required.

(2) Failure to monitor transportation vehicles carrying hazardous chemicals, civilian explosives, nuclear and radioactive materials through a positioning system as required.

(3) Failure to strictly supervise and manage infectious disease pathogens and other substances as required, in severe cases.

(4) Violation of control or restriction measures imposed by the relevant State Council departments or provincial-level people's governments on controlled devices, hazardous chemicals, or civilian explosives.

Article 88: For management and operational units of key targets for preventing terrorist attacks that violate this law with the following circumstances, the public security organ shall issue a warning and order corrections; if corrections are not made, a fine of up to one hundred thousand yuan shall be imposed, and directly responsible managers and other directly responsible personnel

shall be fined up to ten thousand yuan:

- (1) Failure to develop preventive and response plans or measures for terrorist activities.
- (2) Failure to establish a special fund system for anti-terrorism work or to equip preventive and response equipment and facilities.
- (3) Failure to establish working institutions or designate responsible personnel.
- (4) Failure to conduct security background checks on key personnel or to adjust positions for those with unsuitable circumstances.
- (5) Failure to equip public transportation vehicles with security personnel and corresponding equipment and facilities as required.
- (6) Failure to establish management systems for public security video surveillance systems, including monitoring, information storage, usage, and operation maintenance.

For large event organizers and key target management units that fail to conduct security checks on personnel, items, and transportation vehicles entering large event venues, airports, train stations, docks, urban rail transit stations, long-distance bus stations, or ports as required, the public security organ shall order corrections; if corrections are not made, a fine of up to one hundred thousand yuan shall be imposed, and directly responsible managers and other directly responsible personnel shall be fined up to ten thousand yuan.

Article 89: If a person suspected of terrorist activities violates the restraint measures ordered by the public security organ, the public security organ shall issue a warning and order corrections; if corrections are not made, detention for five to fifteen days may be imposed.

Article 90: Units such as news media that fabricate or spread false information about terrorist events, report or spread details of terrorist activities that could incite imitation, publish cruel or inhumane scenes from terrorist events, or report or spread information about on-site responders, hostage identities, and response actions without approval, shall be fined up to two hundred thousand yuan by the public security organ, and directly responsible managers and other directly responsible personnel shall be detained for five to fifteen days and may be fined up to fifty thousand yuan.

Individuals engaging in the above-mentioned activities shall be detained for five to fifteen

days by the public security organ and may be fined up to ten thousand yuan.

Article 91: If a person refuses to cooperate with relevant departments in anti-terrorism security prevention, intelligence information, investigation, or response actions, the competent department shall impose a fine of up to two thousand yuan; if severe consequences result, detention for five to fifteen days may be imposed and a fine of up to ten thousand yuan may also be imposed.

For units engaging in the above-mentioned activities, the competent department shall impose a fine of up to fifty thousand yuan; if severe consequences result, a fine of up to one hundred thousand yuan shall be imposed; directly responsible managers and other directly responsible personnel shall be punished according to the above provisions.

Article 92: If a person obstructs relevant departments from conducting anti-terrorism work, the public security organ shall impose detention for five to fifteen days and may also impose a fine of up to fifty thousand yuan.

For units engaging in the above-mentioned activities, the public security organ shall impose a fine of up to two hundred thousand yuan and punish directly responsible managers and other directly responsible personnel according to the above provisions.

If a person obstructs the lawful execution of duties by public police, the People's Liberation Army, or the armed police, heavier penalties shall be applied.

Article 93: If a unit violates this law and the circumstances are serious, the competent department shall order the cessation of relevant business or services, or suspend production or business operations; if severe consequences result, relevant licenses shall be revoked or registration shall be canceled.

Article 94: Staff members of anti-terrorism work leadership institutions and relevant departments who abuse their power, neglect their duties, or engage in corruption, or violate regulations by disclosing state secrets, commercial secrets, or personal privacy in anti-terrorism work, shall be held criminally liable if their actions constitute a crime; if not, they shall be disciplined according to the law.

Any unit or individual has the right to report or accuse anti-terrorism work leadership institutions, relevant departments, and their staff of abuse of power, neglect of duties, corruption, or other illegal and disciplinary violations. Relevant departments shall handle and respond to reports

and accusations in a timely manner.

Article 95: For items, funds, and other assets that are sealed, detained, frozen, or confiscated according to this law, if it is found upon review that they are unrelated to terrorism, the relevant measures shall be lifted and the items shall be returned in a timely manner.

Article 96: Units and individuals dissatisfied with administrative penalties or administrative compulsory measures made in accordance with this law may apply for administrative reconsideration or initiate administrative litigation according to the law.

#### Chapter 10 Supplementary Provisions

Article 97: This law shall come into effect on January 1, 2016. The “Decision of the Standing Committee of the National People’s Congress on Strengthening Anti-Terrorism Work” adopted at the 23rd Meeting of the Standing Committee of the 11th National People’s Congress on October 29, 2011, is hereby repealed.

# 中华人民共和国反恐怖主义法

(2015年12月27日第十二届全国人民代表大会常务委员会第十八次会议通过 根据2018年4月27日第十三届全国人民代表大会常务委员会第二次会议《关于修改〈中华人民共和国国境卫生检疫法〉等六部法律的决定》修正)

浏览字号: 大 中 小来源: 中国人大网 2018年6月12日 14:47:43

## 目 录

第一章 总 则

第二章 恐怖活动组织和人员的认定

第三章 安全防范

第四章 情报信息

第五章 调 查

第六章 应对处置

第七章 国际合作

第八章 保障措施

第九章 法律责任

第十章 附 则

## 第一章 总 则

**第一条** 为了防范和惩治恐怖活动，加强反恐怖主义工作，维护国家安全、公共安全和人民生命财产安全，根据宪法，制定本法。

**第二条** 国家反对一切形式的恐怖主义，依法取缔恐怖活动组织，对任何组织、策划、准备实施、实施恐怖活动，宣扬恐怖主义，煽动实施恐怖活动，组织、领导、参加恐怖活动组织，为恐怖活动提供帮助的，依法追究法律责任。

国家不向任何恐怖活动组织和人员作出妥协，不向任何恐怖活动人员提供庇护或者给予难民地位。

**第三条** 本法所称恐怖主义，是指通过暴力、破坏、恐吓等手段，制造社会恐慌、危害公共安全、侵犯人身财产，或者胁迫国家机关、国际组织，以实现其政治、意识形态等目的的主张和行为。



本法所称恐怖活动，是指恐怖主义性质的下列行为：

（一）组织、策划、准备实施、实施造成或者意图造成人员伤亡、重大财产损失、公共设施损坏、社会秩序混乱等严重社会危害的活动的；

（二）宣扬恐怖主义，煽动实施恐怖活动，或者非法持有宣扬恐怖主义的物品，强制他人在公共场所穿戴宣扬恐怖主义的服饰、标志的；

（三）组织、领导、参加恐怖活动组织的；

（四）为恐怖活动组织、恐怖活动人员、实施恐怖活动或者恐怖活动培训提供信息、资金、物资、劳务、技术、场所等支持、协助、便利的；

（五）其他恐怖活动。

本法所称恐怖活动组织，是指三人以上为实施恐怖活动而组成的犯罪组织。

本法所称恐怖活动人员，是指实施恐怖活动的人和恐怖活动组织的成员。

本法所称恐怖事件，是指正在发生或者已经发生的造成或者可能造成重大社会危害的恐怖活动。

**第四条** 国家将反恐怖主义纳入国家安全战略，综合施策，标本兼治，加强反恐怖主义的能力建设，运用政治、经济、法律、文化、教育、外交、军事等手段，开展反恐怖主义工作。

国家反对一切形式的以歪曲宗教教义或者其他方法煽动仇恨、煽动歧视、鼓吹暴力等极端主义，消除恐怖主义的思想基础。

**第五条** 反恐怖主义工作坚持专门工作与群众路线相结合，防范为主、惩防结合和先发制敌、保持主动的原则。

**第六条** 反恐怖主义工作应当依法进行，尊重和保障人权，维护公民和组织的合法权益。

在反恐怖主义工作中，应当尊重公民的宗教信仰自由和民族风俗习惯，禁止任何基于地域、民族、宗教等理由的歧视性做法。

**第七条** 国家设立反恐怖主义工作领导机构，统一领导和指挥全国反恐怖主义工作。

设区的市级以上地方人民政府设立反恐怖主义工作领导机构，县级人民政府根据需要设立反恐怖主义工作领导机构，在上级反恐怖主义工作领导机构的领导和指挥下，负责本地区反恐怖主义工作。

**第八条** 公安机关、国家安全机关和人民检察院、人民法院、司法行政机关以及其他有关国家机关，应当根据分工，实行工作责任制，依法做好反恐怖主义工作。

中国人民解放军、中国人民武装警察部队和民兵组织依照本法和其他有关法律、行政法规、军事法规以及国务院、中央军事委员会的命令，并根据反恐怖主义工作领导机构的部署，防范和处置恐怖活动。

有关部门应当建立联动配合机制，依靠、动员村民委员会、居民委员会、企业事业单位、社会组织，共同开展反恐怖主义工作。

**第九条** 任何单位和个人都有协助、配合有关部门开展反恐怖主义工作的义务，发现恐怖活动嫌疑或者恐怖活动嫌疑人员的，应当及时向公安机关或者有关部门报告。

**第十条** 对举报恐怖活动或者协助防范、制止恐怖活动有突出贡献的单位和个人，以及在反恐怖主义工作中作出其他突出贡献的单位和个人，按照国家有关规定给予表彰、奖励。

**第十一条** 对在中华人民共和国领域外对中华人民共和国国家、公民或者机构实施的恐怖活动犯罪，或者实施的中华人民共和国缔结、参加的国际条约所规定的恐怖活动犯罪，中华人民共和国行使刑事管辖权，依法追究刑事责任。

## **第二章 恐怖活动组织和人员的认定**

**第十二条** 国家反恐怖主义工作领导机构根据本法第三条的规定，认定恐怖活动组织和人员，由国家反恐怖主义工作领导机构的办事机构予以公告。

**第十三条** 国务院公安部门、国家安全部门、外交部门和省级反恐怖主义工作领导机构对于需要认定恐怖活动组织和人员的，应当向国家反恐怖主义工作领导机构提出申请。

**第十四条** 金融机构和特定非金融机构对国家反恐怖主义工作领导机构的办事机构公告的恐怖活动组织和人员的资金或者其他资产，应当立即予以冻结，并按照规定及时向国务院公安部门、国家安全部门和反洗钱行政主管部门报告。

**第十五条** 被认定的恐怖活动组织和人员对认定不服的，可以通过国家反恐怖主义工作领导机构的办事机构申请复核。国家反恐怖主义工作领导机构应当及时进行复核，作出维持或者撤销认定的决定。复核决定为最终决定。

国家反恐怖主义工作领导机构作出撤销认定的决定的，由国家反恐怖主义工作领导机构的办事机构予以公告；资金、资产已被冻结的，应当解除冻结。

**第十六条** 根据刑事诉讼法的规定，有管辖权的中级人民法院在审判刑事案件的过程中，可以依法认定恐怖活动组织和人员。对于在判决生效后需要由国家反恐怖主义工作领导机构的办事机构予以公告的，适用本章的有关规定。

### 第三章 安 全 防 范

**第十七条** 各级人民政府和有关部门应当组织开展反恐怖主义宣传教育，提高公民的反恐怖主义意识。

教育、人力资源行政主管部门和学校、有关职业培训机构应当将恐怖活动预防、应急知识纳入教育、教学、培训的内容。

新闻、广播、电视、文化、宗教、互联网等有关单位，应当有针对性地面向社会进行反恐怖主义宣传教育。

村民委员会、居民委员会应当协助人民政府以及有关部门，加强反恐怖主义宣传教育。

**第十八条** 电信业务经营者、互联网服务提供者应当为公安机关、国家安全机关依法进行防范、调查恐怖活动提供技术接口和解密等技术支持和协助。

**第十九条** 电信业务经营者、互联网服务提供者应当依照法律、行政法规规定，落实网络安全、信息内容监督制度和安全技术防范措施，防止含有恐怖主义、极端主义内容的信息传播；发现含有恐怖主义、极端主义内容的信息的，应当立即停止传输，保存相关记录，删除相关信息，并向公安机关或者有关部门报告。

网信、电信、公安、国家安全等主管部门对含有恐怖主义、极端主义内容的信息，应当按照职责分工，及时责令有关单位停止传输、删除相关信息，或者关闭相关网站、关停相关服务。有关单位应当立即执行，并保存相关记录，协助进行调查。对互联网上跨境传输的含有恐怖主义、极端主义内容的信息，电信主管部门应当采取技术措施，阻断传播。

**第二十条** 铁路、公路、水上、航空的货运和邮政、快递等物流运营单位应当实行安全查验制度，对客户身份进行查验，依照规定对运输、寄递物品进行安全检查或者开封验视。对禁止运输、寄递，存在重大安全隐患，或者客户拒绝安全查验的物品，不得运输、寄递。

前款规定的物流运营单位，应当实行运输、寄递客户身份、物品信息登记制度。

**第二十一条** 电信、互联网、金融、住宿、长途客运、机动车租赁等业务经营者、服务提供者，应当对客户身份进行查验。对身份不明或者拒绝身份查验的，不得提供服务。

**第二十二条** 生产和进口单位应当依照规定对枪支等武器、弹药、管制器具、危险化学品、民用爆炸物品、核与放射物品作出电子追踪标识，对民用爆炸物品添加安检示踪标识物。

运输单位应当依照规定对运营中的危险化学品、民用爆炸物品、核与放射物品的运输工具通过定位系统实行监控。

有关单位应当依照规定对传染病病原体等物质实行严格的监督管理，严密防范传染病病原体等物质扩散或者流入非法渠道。

对管制器具、危险化学品、民用爆炸物品，国务院有关主管部门或者省级人民政府根据需要，在特定区域、特定时间，可以决定对生产、进出口、运输、销售、使用、报废实施管制，可以禁止使用现金、实物进行交易或者对交易活动作出其他限制。

**第二十三条** 发生枪支等武器、弹药、危险化学品、民用爆炸物品、核与放射物品、传染病病原体等物质被盗、被抢、丢失或者其他流失的情形，案发单位应当立即采取必要的控制措施，并立即向公安机关报告，同时依照规定向有关主管部门报告。公安机关接到报告后，应当及时开展调查。有关主管部门应当配合公安机关开展工作。

任何单位和个人不得非法制作、生产、储存、运输、进出口、销售、提供、购买、使用、持有、报废、销毁前款规定的物品。公安机关发现的，应当予以扣押；其他主管部门发现的，应当予以扣押，并立即通报公安机关；其他单位、个人发现的，应当立即向公安机关报告。

**第二十四条** 国务院反洗钱行政主管部门、国务院有关部门、机构依法对金融机构和特定非金融机构履行反恐怖主义融资义务的情况进行监督管理。

国务院反洗钱行政主管部门发现涉嫌恐怖主义融资的，可以依法进行调查，采取临时冻结措施。

**第二十五条** 审计、财政、税务等部门在依照法律、行政法规的规定对有关单位实施监督检查的过程中，发现资金流入流出涉嫌恐怖主义融资的，应当及时通报公安机关。

**第二十六条** 海关在对进出境人员携带现金和无记名有价证券实施监管的过程中，发现涉嫌恐怖主义融资的，应当立即通报国务院反洗钱行政主管部门和有管辖权的公安机关。

**第二十七条** 地方各级人民政府制定、组织实施城乡规划，应当符合反恐怖主义工作的需要。

地方各级人民政府应当根据需要，组织、督促有关建设单位在主要道路、交通枢纽、城市公共区域的重点部位，配备、安装公共安全视频图像信息系统等防范恐怖袭击的技防、物防设备、设施。

**第二十八条** 公安机关和有关部门对宣扬极端主义，利用极端主义危害公共安全、扰乱公共秩序、侵犯人身财产、妨害社会管理的，应当及时予以制止，依法追究法律责任。

公安机关发现极端主义活动的，应当责令立即停止，将有关人员强行带离现场并登记身份信息，对有关物品、资料予以收缴，对非法活动场所予以查封。

任何单位和个人发现宣扬极端主义的物品、资料、信息的，应当立即向公安机关报告。

**第二十九条** 对被教唆、胁迫、引诱参与恐怖活动、极端主义活动，或者参与恐怖活动、极端主义活动情节轻微，尚不构成犯罪的人员，公安机关应当组织有关部门、村民委员会、居民委员会、所在单位、就读学校、家庭和监护人对其进行帮教。

监狱、看守所、社区矫正机构应当加强对服刑的恐怖活动罪犯和极端主义罪犯的管理、教育、矫正等工作。监狱、看守所对恐怖活动罪犯和极端主义罪犯，根据教育改造和维护监管秩序的需要，可以与普通刑事罪犯混合关押，也可以个别关押。

**第三十条** 对恐怖活动罪犯和极端主义罪犯被判处徒刑以上刑罚的，监狱、看守所应当在刑满释放前根据其犯罪性质、情节和社会危害程度，服刑期间的表现，释放后对所居住社区的影响等进行社会危险性评估。进行社会危险性评估，应当听取有关基层组织和原办案机关的意见。经评估具有社会危险性的，监狱、看守所应当向罪犯服刑地的中级人民法院提出安置教育建议，并将建议书副本抄送同级人民检察院。

罪犯服刑地的中级人民法院对于确有社会危险性的，应当在罪犯刑满释放前作出责令其在刑满释放后接受安置教育的决定。决定书副本应当抄送同级人民检察院。被决定安置教育的人员对决定不服的，可以向上一级人民法院申请复议。

安置教育由省级人民政府组织实施。安置教育机构应当每年对被安置教育人员进行评估，对于确有悔改表现，不致再危害社会的，应当及时提出解除安置教育的意见，报决定安置教育的中级人民法院作出决定。被安置教育人员有权申请解除安置教育。

人民检察院对安置教育的决定和执行实行监督。

**第三十一条** 公安机关应当会同有关部门，将遭受恐怖袭击的可能性较大以及遭受恐怖袭击可能造成重大的人身伤亡、财产损失或者社会影响的单位、场所、活动、设施等确定为防范恐怖袭击的重点目标，报本级反恐怖主义工作领导小组备案。

**第三十二条** 重点目标的管理单位应当履行下列职责：

- （一）制定防范和应对处置恐怖活动的预案、措施，定期进行培训和演练；
- （二）建立反恐怖主义工作专项经费保障制度，配备、更新防范和处置设备、设施；
- （三）指定相关机构或者落实责任人员，明确岗位职责；
- （四）实行风险评估，实时监测安全威胁，完善内部安全管理；
- （五）定期向公安机关和有关部门报告防范措施落实情况。

重点目标的管理单位应当根据城乡规划、相关标准和实际需要，对重点目标同步设计、同步建设、同步运行符合本法第二十七条规定的技防、物防设备、设施。

重点目标的管理单位应当建立公共安全视频图像信息系统值班监看、信息保存使用、运行维护等管理制度，保障相关系统正常运行。采集的视频图像信息保存期限不得少于九十日。

对重点目标以外的涉及公共安全的其他单位、场所、活动、设施，其主管部门和管理单位应当依照法律、行政法规规定，建立健全安全管理制度，落实安全责任。

**第三十三条** 重点目标的管理单位应当对重要岗位人员进行安全背景审查。对有不适合情形的人员，应当调整工作岗位，并将有关情况通报公安机关。

**第三十四条** 大型活动承办单位以及重点目标的管理单位应当依照规定，对进入大型活动场所、机场、火车站、码头、城市轨道交通站、公路长途客运站、口岸等重点目标的人员、物品和交通工具进行安全检查。发现违禁品和管制物品，应当予以扣留并立即向公安机关报告；发现涉嫌违法犯罪人员，应当立即向公安机关报告。

**第三十五条** 对航空器、列车、船舶、城市轨道车辆、公共电汽车等公共交通运输工具，营运单位应当依照规定配备安保人员和相应设备、设施，加强安全检查和保卫工作。

**第三十六条** 公安机关和有关部门应当掌握重点目标的基础信息和重要动态，指导、监督重点目标的管理单位履行防范恐怖袭击的各项职责。

公安机关、中国人民武装警察部队应当依照有关规定对重点目标进行警戒、巡逻、检查。

**第三十七条** 飞行管制、民用航空、公安等主管部门应当按照职责分工，加强空域、航空器和飞行活动管理，严密防范针对航空器或者利用飞行活动实施的恐怖活动。

**第三十八条** 各级人民政府和军事机关应当在重点国（边）境地段和口岸设置拦阻隔离网、视频图像采集和防越境报警设施。

公安机关和中国人民解放军应当严密组织国（边）境巡逻，依照规定对抵离国（边）境前沿、进出国（边）境管理区和国（边）境通道、口岸的人员、交通运输工具、物品，以及沿海沿边地区的船舶进行查验。

**第三十九条** 出入境证件签发机关、出入境边防检查机关对恐怖活动人员和恐怖活动嫌疑人员，有权决定不准其出境入境、不予签发出境入境证件或者宣布其出境入境证件作废。

**第四十条** 海关、出入境边防检查机关发现恐怖活动嫌疑人员或者涉嫌恐怖活动物品的，应当依法扣留，并立即移送公安机关或者国家安全机关。

**第四十一条** 国务院外交、公安、国家安全、发展改革、工业和信息化、商务、旅游等主管部门应当建立境外投资合作、旅游等安全风险评估制度，对中国在境外的公民以及驻外机构、设施、财产加强安全保护，防范和应对恐怖袭击。

**第四十二条** 驻外机构应当建立健全安全防范制度和应对处置预案，加强对有关人员、设施、财产的安全保护。

#### 第四章 情报信息

**第四十三条** 国家反恐怖主义工作领导机构建立国家反恐怖主义情报中心，实行跨部门、跨地区情报信息工作机制，统筹反恐怖主义情报信息工作。

有关部门应当加强反恐怖主义情报信息搜集工作，对搜集的有关线索、人员、行动类情报信息，应当依照规定及时统一归口报送国家反恐怖主义情报中心。



地方反恐怖主义工作领导机构应当建立跨部门情报信息工作机制，组织开展反恐怖主义情报信息工作，对重要的情报信息，应当及时向上级反恐怖主义工作领导机构报告，对涉及其他地方的紧急情报信息，应当及时通报相关地方。

**第四十四条** 公安机关、国家安全机关和有关部门应当依靠群众，加强基层基础工作，建立基层情报信息工作力量，提高反恐怖主义情报信息工作能力。

**第四十五条** 公安机关、国家安全机关、军事机关在其职责范围内，因反恐怖主义情报信息工作的需要，根据国家有关规定，经过严格的批准手续，可以采取技术侦察措施。

依照前款规定获取的材料，只能用于反恐怖主义应对处置和对恐怖活动犯罪、极端主义犯罪的侦查、起诉和审判，不得用于其他用途。

**第四十六条** 有关部门对于在本法第三章规定的安全防范工作中获取的信息，应当根据国家反恐怖主义情报中心的要求，及时提供。

**第四十七条** 国家反恐怖主义情报中心、地方反恐怖主义工作领导机构以及公安机关等有关部门应当对有关情报信息进行筛查、研判、核查、监控，认为有发生恐怖事件危险，需要采取相应的安全防范、应对处置措施的，应当及时通报有关部门和单位，并可以根据情况发出预警。有关部门和单位应当根据通报做好安全防范、应对处置工作。

**第四十八条** 反恐怖主义工作领导机构、有关部门和单位、个人应当对履行反恐怖主义工作职责、义务过程中知悉的国家秘密、商业秘密和个人隐私予以保密。

违反规定泄露国家秘密、商业秘密和个人隐私的，依法追究法律责任。

## 第五章 调 查

**第四十九条** 公安机关接到恐怖活动嫌疑的报告或者发现恐怖活动嫌疑，需要调查核实的，应当迅速进行调查。

**第五十条** 公安机关调查恐怖活动嫌疑，可以依照有关法律规定对嫌疑人员进行盘问、检查、传唤，可以提取或者采集肖像、指纹、虹膜图像等人体生物识别信息和血液、尿液、脱落细胞等生物样本，并留存其签名。

公安机关调查恐怖活动嫌疑，可以通知了解有关情况的人员到公安机关或者其他地点接受询问。

**第五十一条** 公安机关调查恐怖活动嫌疑，有权向有关单位和个人收集、调取相关信息和材料。有关单位和个人应当如实提供。

**第五十二条** 公安机关调查恐怖活动嫌疑，经县级以上公安机关负责人批准，可以查询嫌疑人员的存款、汇款、债券、股票、基金份额等财产，可以采取查封、扣押、冻结措施。查封、扣押、冻结的期限不得超过二个月，情况复杂的，可以经上一级公安机关负责人批准延长一个月。

**第五十三条** 公安机关调查恐怖活动嫌疑，经县级以上公安机关负责人批准，可以根据其危险程度，责令恐怖活动嫌疑人员遵守下列一项或者多项约束措施：

- (一) 未经公安机关批准不得离开所居住的市、县或者指定的处所；
- (二) 不得参加大型群众性活动或者从事特定的活动；
- (三) 未经公安机关批准不得乘坐公共交通工具或者进入特定的场所；
- (四) 不得与特定的人员会见或者通信；
- (五) 定期向公安机关报告活动情况；
- (六) 将护照等出入境证件、身份证件、驾驶证件交公安机关保存。

公安机关可以采取电子监控、不定期检查等方式对其遵守约束措施的情况进行监督。

采取前两款规定的约束措施的期限不得超过三个月。对不需要继续采取约束措施的，应当及时解除。

**第五十四条** 公安机关经调查，发现犯罪事实或者犯罪嫌疑人的，应当依照刑事诉讼法的规定立案侦查。本章规定的有关期限届满，公安机关未立案侦查的，应当解除有关措施。

## 第六章 应 对 处 置

**第五十五条** 国家建立健全恐怖事件应对处置预案体系。

国家反恐怖主义工作领导机构应当针对恐怖事件的规律、特点和可能造成的社会危害，分级、分类制定国家应对处置预案，具体规定恐怖事件应对处置的组织指挥体系和恐怖事件安全防范、应对处置程序以及事后社会秩序恢复等内容。

有关部门、地方反恐怖主义工作领导机构应当制定相应的应对处置预案。

**第五十六条** 应对处置恐怖事件，各级反恐怖主义工作领导机构应当成立由有关部门参加的指挥机构，实行指挥长负责制。反恐怖主义工作领导机构负责人可以担任指挥长，也可以确定公安机关负责人或者反恐怖主义工作领导机构的其他成员单位负责人担任指挥长。

跨省、自治区、直辖市发生的恐怖事件或者特别重大恐怖事件的应对处置，由国家反恐怖主义工作领导机构负责指挥；在省、自治区、直辖市范围内发生的涉及多个行政区域的恐怖事件或者重大恐怖事件的应对处置，由省级反恐怖主义工作领导机构负责指挥。

**第五十七条** 恐怖事件发生后，发生地反恐怖主义工作领导机构应当立即启动恐怖事件应对处置预案，确定指挥长。有关部门和中国人民解放军、中国人民武装警察部队、民兵组织，按照反恐怖主义工作领导机构和指挥长的统一领导、指挥，协同开展打击、控制、救援、救护等现场应对处置工作。

上级反恐怖主义工作领导机构可以对应对处置工作进行指导，必要时调动有关反恐怖主义力量进行支援。

需要进入紧急状态的，由全国人民代表大会常务委员会或者国务院依照宪法和其他有关法律规定的权限和程序决定。

**第五十八条** 发现恐怖事件或者疑似恐怖事件后，公安机关应当立即进行处置，并向反恐怖主义工作领导机构报告；中国人民解放军、中国人民武装警察部队发现正在实施恐怖活动的，应当立即予以控制并将案件及时移交公安机关。

反恐怖主义工作领导机构尚未确定指挥长的，由在场处置的公安机关职级最高的人员担任现场指挥员。公安机关未能到达现场的，由在场处置的中国人民解放军或者中国人民

武装警察部队职级最高的人员担任现场指挥员。现场应对处置人员无论是否属于同一单位、系统，均应当服从现场指挥员的指挥。

指挥长确定后，现场指挥员应当向其请示、报告工作或者有关情况。

**第五十九条** 中华人民共和国在境外的机构、人员、重要设施遭受或者可能遭受恐怖袭击的，国务院外交、公安、国家安全、商务、金融、国有资产监督管理、旅游、交通运输等主管部门应当及时启动应对处置预案。国务院外交部门应当协调有关国家采取相应措施。

中华人民共和国在境外的机构、人员、重要设施遭受严重恐怖袭击后，经与有关国家协商同意，国家反恐怖主义工作领导机构可以组织外交、公安、国家安全等部门派出工作人员赴境外开展应对处置工作。

**第六十条** 应对处置恐怖事件，应当优先保护直接受到恐怖活动危害、威胁人员的人身安全。

**第六十一条** 恐怖事件发生后，负责应对处置的反恐怖主义工作领导机构可以决定由有关部门和单位采取下列一项或者多项应对处置措施：

（一）组织营救和救治受害人员，疏散、撤离并妥善安置受到威胁的人员以及采取其他救助措施；

（二）封锁现场和周边道路，查验现场人员的身份证件，在有关场所附近设置临时警戒线；

（三）在特定区域内实施空域、海（水）域管制，对特定区域内的交通运输工具进行检查；

（四）在特定区域内实施互联网、无线电、通讯管制；

（五）在特定区域内或者针对特定人员实施出境入境管制；

（六）禁止或者限制使用有关设备、设施，关闭或者限制使用有关场所，中止人员密集的活动或者可能导致危害扩大的生产经营活动；

(七) 抢修被损坏的交通、电信、互联网、广播电视、供水、排水、供电、供气、供热等公共设施；

(八) 组织志愿人员参加反恐怖主义救援工作，要求具有特定专长的人员提供服务；

(九) 其他必要的应对处置措施。

采取前款第三项至第五项规定的应对处置措施，由省级以上反恐怖主义工作领导小组决定或者批准；采取前款第六项规定的应对处置措施，由设区的市级以上反恐怖主义工作领导小组决定。应对处置措施应当明确适用的时间和空间范围，并向社会公布。

**第六十二条** 人民警察、人民武装警察以及其他依法配备、携带武器的应对处置人员，对在现场持枪支、刀具等凶器或者使用其他危险方法，正在或者准备实施暴力行为的人员，经警告无效的，可以使用武器；紧急情况下或者警告后可能导致更为严重危害后果的，可以直接使用武器。

**第六十三条** 恐怖事件发生、发展和应对处置信息，由恐怖事件发生地的省级反恐怖主义工作领导小组统一发布；跨省、自治区、直辖市发生的恐怖事件，由指定的省级反恐怖主义工作领导小组统一发布。

任何单位和个人不得编造、传播虚假恐怖事件信息；不得报道、传播可能引起模仿的恐怖活动的实施细节；不得发布恐怖事件中残忍、不人道的场景；在恐怖事件的应对处置过程中，除新闻媒体经负责发布信息的反恐怖主义工作领导小组批准外，不得报道、传播现场应对处置的工作人员、人质身份信息和应对处置行动情况。

**第六十四条** 恐怖事件应对处置结束后，各级人民政府应当组织有关部门帮助受影响的单位和个人尽快恢复生活、生产，稳定受影响地区的社会秩序和公众情绪。

**第六十五条** 当地人民政府应当及时给予恐怖事件受害人员及其近亲属适当的救助，并向失去基本生活条件的受害人员及其近亲属及时提供基本生活保障。卫生、医疗保障等主管部门应当为恐怖事件受害人员及其近亲属提供心理、医疗等方面的援助。

**第六十六条** 公安机关应当及时对恐怖事件立案侦查，查明事件发生的原因、经过和结果，依法追究恐怖活动组织、人员的刑事责任。

**第六十七条** 反恐怖主义工作领导机构应当对恐怖事件的发生和应对处置工作进行全面分析、总结评估，提出防范和应对处置改进措施，向上一级反恐怖主义工作领导机构报告。

## 第七章 国际 合 作

**第六十八条** 中华人民共和国根据缔结或者参加的国际条约，或者按照平等互惠原则，与其他国家、地区、国际组织开展反恐怖主义合作。

**第六十九条** 国务院有关部门根据国务院授权，代表中国政府与外国政府和有关国际组织开展反恐怖主义政策对话、情报信息交流、执法合作和国际资金监管合作。

在不违背我国法律的前提下，边境地区的县级以上地方人民政府及其主管部门，经国务院或者中央有关部门批准，可以与相邻国家或者地区开展反恐怖主义情报信息交流、执法合作和国际资金监管合作。

**第七十条** 涉及恐怖活动犯罪的刑事司法协助、引渡和被判刑人移管，依照有关法律的规定执行。

**第七十一条** 经与有关国家达成协议，并报国务院批准，国务院公安部门、国家安全部门可以派员出境执行反恐怖主义任务。

中国人民解放军、中国人民武装警察部队派员出境执行反恐怖主义任务，由中央军事委员会批准。

**第七十二条** 通过反恐怖主义国际合作取得的材料可以在行政处罚、刑事诉讼中作为证据使用，但我方承诺不作为证据使用的除外。

## 第八章 保 障 措 施

**第七十三条** 国务院和县级以上地方各级人民政府应当按照事权划分，将反恐怖主义工作经费分别列入同级财政预算。

国家对反恐怖主义重点地区给予必要的经费支持，对应对处置大规模恐怖事件给予经费保障。

**第七十四条** 公安机关、国家安全机关和有关部门，以及中国人民解放军、中国人民武装警察部队，应当依照法律规定的职责，建立反恐怖主义专业力量，加强专业训练，配备必要的反恐怖主义专业设备、设施。

县级、乡级人民政府根据需要，指导有关单位、村民委员会、居民委员会建立反恐怖主义工作力量、志愿者队伍，协助、配合有关部门开展反恐怖主义工作。

**第七十五条** 对因履行反恐怖主义工作职责或者协助、配合有关部门开展反恐怖主义工作导致伤残或者死亡的人员，按照国家有关规定给予相应的待遇。

**第七十六条** 因报告和制止恐怖活动，在恐怖活动犯罪案件中作证，或者从事反恐怖主义工作，本人或者其近亲属的人身安全面临危险的，经本人或者其近亲属提出申请，公安机关、有关部门应当采取下列一项或者多项保护措施：

- （一）不公开真实姓名、住址和工作单位等个人信息；
- （二）禁止特定的人接触被保护人员；
- （三）对人身和住宅采取专门性保护措施；
- （四）变更被保护人员的姓名，重新安排住所和工作单位；
- （五）其他必要的保护措施。

公安机关、有关部门应当依照前款规定，采取不公开被保护单位的真实名称、地址，禁止特定的人接近被保护单位，对被保护单位办公、经营场所采取专门性保护措施，以及其他必要的保护措施。

**第七十七条** 国家鼓励、支持反恐怖主义科学研究和技术创新，开发和推广使用先进的反恐怖主义技术、设备。

**第七十八条** 公安机关、国家安全机关、中国人民解放军、中国人民武装警察部队因履行反恐怖主义职责的紧急需要，根据国家有关规定，可以征用单位和个人的财产。任务完成后应当及时归还或者恢复原状，并依照规定支付相应费用；造成损失的，应当补偿。

因开展反恐怖主义工作对有关单位和个人的合法权益造成损害的，应当依法给予赔偿、补偿。有关单位和个人有权依法请求赔偿、补偿。

## 第九章 法律 责任

**第七十九条** 组织、策划、准备实施、实施恐怖活动，宣扬恐怖主义，煽动实施恐怖活动，非法持有宣扬恐怖主义的物品，强制他人在公共场所穿戴宣扬恐怖主义的服饰、标志，组织、领导、参加恐怖活动组织，为恐怖活动组织、恐怖活动人员、实施恐怖活动或者恐怖活动培训提供帮助的，依法追究刑事责任。

**第八十条** 参与下列活动之一，情节轻微，尚不构成犯罪的，由公安机关处十日以上十五日以下拘留，可以并处一万元以下罚款：

- （一）宣扬恐怖主义、极端主义或者煽动实施恐怖活动、极端主义活动的；
- （二）制作、传播、非法持有宣扬恐怖主义、极端主义的物品的；
- （三）强制他人在公共场所穿戴宣扬恐怖主义、极端主义的服饰、标志的；
- （四）为宣扬恐怖主义、极端主义或者实施恐怖主义、极端主义活动提供信息、资金、物资、劳务、技术、场所等支持、协助、便利的。

**第八十一条** 利用极端主义，实施下列行为之一，情节轻微，尚不构成犯罪的，由公安机关处五日以上十五日以下拘留，可以并处一万元以下罚款：

- （一）强迫他人参加宗教活动，或者强迫他人向宗教活动场所、宗教教职人员提供财物或者劳务的；
- （二）以恐吓、骚扰等方式驱赶其他民族或者有其他信仰的人员离开居住地的；
- （三）以恐吓、骚扰等方式干涉他人与其他民族或者有其他信仰的人员交往、共同生活的；
- （四）以恐吓、骚扰等方式干涉他人生活习俗、方式和生产经营的；
- （五）阻碍国家机关工作人员依法执行职务的；



- (六) 歪曲、诋毁国家政策、法律、行政法规，煽动、教唆抵制人民政府依法管理的；
- (七) 煽动、胁迫群众损毁或者故意损毁居民身份证、户口簿等国家法定证件以及人民币的；
- (八) 煽动、胁迫他人以宗教仪式取代结婚、离婚登记的；
- (九) 煽动、胁迫未成年人不接受义务教育的；
- (十) 其他利用极端主义破坏国家法律制度实施的。

**第八十二条** 明知他人有恐怖活动犯罪、极端主义犯罪行为，窝藏、包庇，情节轻微，尚不构成犯罪的，或者在司法机关向其调查有关情况、收集有关证据时，拒绝提供的，由公安机关处十日以上十五日以下拘留，可以并处一万元以下罚款。

**第八十三条** 金融机构和特定非金融机构对国家反恐怖主义工作领导机构的办事机构公告的恐怖活动组织及恐怖活动人员的资金或者其他资产，未立即予以冻结的，由公安机关处二十万元以上五十万元以下罚款，并对直接负责的董事、高级管理人员和其他直接责任人员处十万元以下罚款；情节严重的，处五十万元以上罚款，并对直接负责的董事、高级管理人员和其他直接责任人员，处十万元以上五十万元以下罚款，可以并处五日以上十五日以下拘留。

**第八十四条** 电信业务经营者、互联网信息服务提供者有下列情形之一的，由主管部门处二十万元以上五十万元以下罚款，并对其直接负责的主管人员和其他直接责任人员处十万元以下罚款；情节严重的，处五十万元以上罚款，并对其直接负责的主管人员和其他直接责任人员，处十万元以上五十万元以下罚款，可以由公安机关对其直接负责的主管人员和其他直接责任人员，处五日以上十五日以下拘留：

- (一) 未依照规定为公安机关、国家安全机关依法进行防范、调查恐怖活动提供技术接口和解密等技术支持和协助的；

(二) 未按照主管部门的要求，停止传输、删除含有恐怖主义、极端主义内容的信息，保存相关记录，关闭相关网站或者关停相关服务的；

(三) 未落实网络安全、信息内容监督制度和安全技术防范措施，造成含有恐怖主义、极端主义内容的信息传播，情节严重的。

**第八十五条** 铁路、公路、水上、航空的货运和邮政、快递等物流运营单位有下列情形之一的，由主管部门处十万元以上五十万元以下罚款，并对其直接负责的主管人员和其他直接责任人员处十万元以下罚款：

(一) 未实行安全查验制度，对客户身份进行查验，或者未依照规定对运输、寄递物品进行安全检查或者开封验视的；

(二) 对禁止运输、寄递，存在重大安全隐患，或者客户拒绝安全查验的物品予以运输、寄递的；

(三) 未实行运输、寄递客户身份、物品信息登记制度的。

**第八十六条** 电信、互联网、金融业务经营者、服务提供者未按规定对客户身份进行查验，或者对身份不明、拒绝身份查验的客户提供服务的，主管部门应当责令改正；拒不改正的，处二十万元以上五十万元以下罚款，并对其直接负责的主管人员和其他直接责任人员处十万元以下罚款；情节严重的，处五十万元以上罚款，并对其直接负责的主管人员和其他直接责任人员，处十万元以上五十万元以下罚款。

住宿、长途客运、机动车租赁等业务经营者、服务提供者有前款规定情形的，由主管部门处十万元以上五十万元以下罚款，并对其直接负责的主管人员和其他直接责任人员处十万元以下罚款。

**第八十七条** 违反本法规定，有下列情形之一的，由主管部门给予警告，并责令改正；拒不改正的，处十万元以下罚款，并对其直接负责的主管人员和其他直接责任人员处一万元以下罚款：

(一) 未依照规定对枪支等武器、弹药、管制器具、危险化学品、民用爆炸物品、核与放射物品作出电子追踪标识, 对民用爆炸物品添加安检示踪标识物的;

(二) 未依照规定对运营中的危险化学品、民用爆炸物品、核与放射物品的运输工具通过定位系统实行监控的;

(三) 未依照规定对传染病病原体等物质实行严格的监督管理, 情节严重的;

(四) 违反国务院有关主管部门或者省级人民政府对管制器具、危险化学品、民用爆炸物品决定的管制或者限制交易措施的。

**第八十八条** 防范恐怖袭击重点目标的管理、营运单位违反本法规定, 有下列情形之一的, 由公安机关给予警告, 并责令改正; 拒不改正的, 处十万元以下罚款, 并对其直接负责的主管人员和其他直接责任人员处一万元以下罚款:

(一) 未制定防范和应对处置恐怖活动的预案、措施的;

(二) 未建立反恐怖主义工作专项经费保障制度, 或者未配备防范和处置设备、设施的;

(三) 未落实工作机构或者责任人员的;

(四) 未对重要岗位人员进行安全背景审查, 或者未将有不适合情形的人员调整工作岗位的;

(五) 对公共交通运输工具未依照规定配备安保人员和相应设备、设施的;

(六) 未建立公共安全视频图像信息系统值班监看、信息保存使用、运行维护等管理制度的。

大型活动承办单位以及重点目标的管理单位未依照规定对进入大型活动场所、机场、火车站、码头、城市轨道交通站、公路长途客运站、口岸等重点目标的人员、物品和交通工具进行安全检查的, 公安机关应当责令改正; 拒不改正的, 处十万元以下罚款, 并对其直接负责的主管人员和其他直接责任人员处一万元以下罚款。

**第八十九条** 恐怖活动嫌疑人员违反公安机关责令其遵守的约束措施的，由公安机关给予警告，并责令改正；拒不改正的，处五日以上十五日以下拘留。

**第九十条** 新闻媒体等单位编造、传播虚假恐怖事件信息，报道、传播可能引起模仿的恐怖活动的实施细节，发布恐怖事件中残忍、不人道的场景，或者未经批准，报道、传播现场应对处置的工作人员、人质身份信息和应对处置行动情况的，由公安机关处二十万元以下罚款，并对其直接负责的主管人员和其他直接责任人员，处五日以上十五日以下拘留，可以并处五万元以下罚款。

个人有前款规定行为的，由公安机关处五日以上十五日以下拘留，可以并处一万元以下罚款。

**第九十一条** 拒不配合有关部门开展反恐怖主义安全防范、情报信息、调查、应对处置工作的，由主管部门处二千元以下罚款；造成严重后果的，处五日以上十五日以下拘留，可以并处一万元以下罚款。

单位有前款规定行为的，由主管部门处五万元以下罚款；造成严重后果的，处十万元以下罚款；并对其直接负责的主管人员和其他直接责任人员依照前款规定处罚。

**第九十二条** 阻碍有关部门开展反恐怖主义工作的，由公安机关处五日以上十五日以下拘留，可以并处五万元以下罚款。

单位有前款规定行为的，由公安机关处二十万元以下罚款，并对其直接负责的主管人员和其他直接责任人员依照前款规定处罚。

阻碍人民警察、人民解放军、人民武装警察依法执行职务的，从重处罚。

**第九十三条** 单位违反本法规定，情节严重的，由主管部门责令停止从事相关业务、提供相关服务或者责令停产停业；造成严重后果的，吊销有关证照或者撤销登记。

**第九十四条** 反恐怖主义工作领导机构、有关部门的工作人员在反恐怖主义工作中滥用职权、玩忽职守、徇私舞弊，或者有违反规定泄露国家秘密、商业秘密和个人隐私等行为，构成犯罪的，依法追究刑事责任；尚不构成犯罪的，依法给予处分。

反恐怖主义工作领导机构、有关部门及其工作人员在反恐怖主义工作中滥用职权、玩忽职守、徇私舞弊或者有其他违法违纪行为的，任何单位和个人有权向有关部门检举、控告。有关部门接到检举、控告后，应当及时处理并回复检举、控告人。

**第九十五条** 对依照本法规定查封、扣押、冻结、扣留、收缴的物品、资金等，经审查发现与恐怖主义无关的，应当及时解除有关措施，予以退还。

**第九十六条** 有关单位和个人对依照本法作出的行政处罚和行政强制措施决定不服的，可以依法申请行政复议或者提起行政诉讼。

## 第十章 附 则

**第九十七条** 本法自2016年1月1日起施行。2011年10月29日第十一届全国人民代表大会常务委员会第二十三次会议通过的《全国人民代表大会常务委员会关于加强反恐怖工作有关问题的决定》同时废止。

# EXHIBIT D

**Declaration of David Newman  
Principal Deputy Assistant Attorney General  
National Security Division  
Department of Justice**



---

# Certification of Translation

---



COUNTY OF SUFFOLK  
COMMONWEALTH OF MASSACHUSETTS

July 24, 2024

This is to certify that the attached translation is, to the best of my knowledge and belief, a true and accurate translation from Simplified Chinese into English of the attached document:

- **National Intelligence Law**

Linguistic Systems, Inc. adheres to an ISO-certified quality management system that ensures best practices are always followed in the selection of linguists skilled in both the languages and subject matters necessary for every translation.



Linguistic Systems, Inc.



260 Franklin Street, Suite 230, Boston MA 02110 • Phone 617-528-7400 • Fax 617-528-7490 • [www.linguist.com](http://www.linguist.com)

Certifications: ISO 9001 • ISO 17100 • ISO 18587 • ISO 27001

## National Intelligence Law of the People's Republic of China

(Passed at the 28th meeting of the Standing Committee of the 12th National People's Congress on June 27, 2017. Amended according to the "Decision on Amending Six Laws Including the Law of the People's Republic of China on Frontier Health and Quarantine" passed at the 2nd meeting of the Standing Committee of the 13th National People's Congress on April 27, 2018.)

Browsing Font Size: Large Medium Small Source: National People's Congress of China Website Date: June 12, 2018, 14:48:46

### Table of Contents

Chapter 1: General Provisions

Chapter 2: Powers and Responsibilities of National Intelligence Work Organizations

Chapter 3: Guarantee of National Intelligence Work

Chapter 4: Legal Responsibilities

Chapter 5: Supplementary Provisions

#### Chapter 1: General Provisions

Article 1: This law is formulated to strengthen and ensure national intelligence work, safeguard national security and interests, and is based on the Constitution.

Article 2: National intelligence work adheres to the overall concept of national security, provides intelligence references for major national decisions, supports the prevention and resolution of risks that endanger national security, and maintains national sovereignty, unity, territorial integrity, people's welfare, sustainable economic and social development, and other major national interests.

Article 3: The state establishes a centralized, unified, cooperative, scientifically efficient national intelligence system.

The central national security leadership body exercises unified leadership over national intelligence work, formulates policies for national intelligence work, plans the overall development of national intelligence work, establishes and improves coordination mechanisms for national intelligence work, coordinates national intelligence work in various fields, and researches and decides on major issues in national intelligence work.

The Central Military Commission exercises unified leadership and organization of military intelligence work.

Article 4: National intelligence work shall adhere to the principles of combining open work with



secret work, specialized work with the mass line, and division of responsibilities with cooperation and coordination.

Article 5: The intelligence agencies of national security organs and public security organs, and military intelligence agencies (collectively referred to as national intelligence work agencies) shall, according to the division of responsibilities, cooperate with each other, carry out intelligence work, and conduct intelligence operations.

Relevant state organs shall, according to their respective functions and tasks, closely cooperate with national intelligence work agencies.

Article 6: National intelligence work agencies and their staff shall be loyal to the state and the people, abide by the Constitution and laws, be dedicated to their duties, maintain strict discipline, be honest and clean, selflessly contribute, and resolutely safeguard national security and interests.

Article 7: All organizations and citizens shall legally support, assist, and cooperate with national intelligence work, and keep confidential the national intelligence work secrets they are aware of.

The state protects individuals and organizations that support, assist, and cooperate with national intelligence work.

Article 8: National intelligence work shall be conducted in accordance with the law, respecting and protecting human rights, and safeguarding the legitimate rights and interests of individuals and organizations.

Article 9: The state shall commend and reward individuals and organizations that have made significant contributions to national intelligence work.

## Chapter 2: Powers and Responsibilities of National Intelligence Work Organizations

Article 10: National intelligence work agencies shall, as needed for their work, use necessary methods, means, and channels according to the law to conduct intelligence work both domestically and abroad.

Article 11: National intelligence work agencies shall collect and process intelligence related to actions that harm the national security and interests of the People's Republic of China, which are implemented or directed by, or funded by, foreign institutions, organizations, or individuals,

or colluded with by domestic and foreign institutions, organizations, or individuals. They provide intelligence basis or reference for preventing, stopping, and punishing such actions.

Article 12: National intelligence work agencies may, according to relevant national regulations, establish cooperative relationships with relevant individuals and organizations and entrust them with related tasks.

Article 13: National intelligence work agencies may, according to relevant national regulations, engage in foreign exchanges and cooperation.

Article 14: In conducting intelligence work according to the law, national intelligence work agencies may request necessary support, assistance, and cooperation from relevant organs, organizations, and citizens.

Article 15: National intelligence work agencies may, according to national regulations and after strict approval procedures, take technical reconnaissance measures and identity protection measures as needed for their work.

Article 16: When performing tasks according to the law, staff of national intelligence work agencies, in accordance with national regulations and with approval, may present appropriate credentials to enter restricted areas and locations, inquire about relevant information from relevant organs, organizations, and individuals, and review or retrieve relevant files, materials, and items.

Article 17: Staff of national intelligence work agencies, when carrying out urgent tasks, may enjoy expedited passage by presenting appropriate credentials.

According to work needs and relevant national regulations, they may prioritize or requisition transportation, communication tools, sites, and buildings from relevant organs, organizations, and individuals. When necessary, they may set up related workspaces and equipment. After completing the tasks, they must promptly return or restore the items to their original state and pay the corresponding fees as required. Compensation is required for any damages caused.

Article 18: National intelligence work agencies may, according to work needs and relevant national regulations, request customs, border inspection, and other relevant agencies to provide inspection exemptions and other conveniences.

Article 19: National intelligence work agencies and their staff must strictly act according to the law, avoid exceeding their authority or abusing their power, refrain from infringing on the legal rights and interests of citizens and organizations, and must not use their positions for personal gain. They must not disclose state secrets, commercial secrets, or personal information.

### Chapter 3: Guarantee of National Intelligence Work

Article 20: National intelligence work agencies and their staff conducting intelligence work according to the law are protected by the law.

Article 21: The state strengthens the construction of national intelligence work agencies, implementing special management and protection for their organizational structure, personnel, staffing, funding, and assets.

The state establishes management systems for the recruitment, selection, assessment, training, treatment, and exit of personnel adapted to the needs of intelligence work.

Article 22: National intelligence work agencies should enhance their capability to carry out intelligence work in line with its needs.

National intelligence work agencies should use scientific and technological means to improve their ability to identify, filter, synthesize, and analyze intelligence information.

Article 23: When the personal safety of staff of national intelligence work agencies or individuals cooperating with them is threatened due to their tasks or cooperation, relevant state departments should take necessary measures to provide protection and rescue.

Article 24: The state will provide proper arrangements for individuals who have made contributions to national intelligence work and require resettlement.

Relevant departments such as public security, civil affairs, finance, health, education, human resources and social security, veteran affairs, and medical insurance, as well as state-owned enterprises and institutions, should assist national intelligence work agencies in providing resettlement services.

Article 25: For individuals who become disabled, suffer casualties, or die due to conducting or supporting, assisting, or cooperating with national intelligence work, corresponding compensations and benefits shall be provided according to relevant national regulations.

Individuals and organizations that suffer property losses due to supporting, assisting, and cooperating with national intelligence work shall receive compensation according to relevant national regulations.

Article 26: National intelligence work agencies should establish and improve strict supervision and security review systems, supervise their staff's adherence to laws and disciplines, and take necessary measures to conduct regular or irregular security reviews according to the law.

Article 27: Any individual or organization has the right to report or accuse national intelligence work agencies and their staff of exceeding their authority, abusing their power, or other illegal and disciplinary violations. Relevant authorities receiving such reports or accusations should promptly investigate and inform the informant or accuser of the results.

No individual or organization may suppress or retaliate against those who lawfully report or accuse national intelligence work agencies and their staff.

National intelligence work agencies should provide convenient channels for individuals and organizations to report, accuse, or provide feedback, and ensure confidentiality for informants and accusers.

#### Chapter 4: Legal Responsibilities

Article 28: Those who obstruct national intelligence work agencies and their staff from conducting intelligence work according to the law in violation of this law may be subject to disciplinary action by the relevant units as suggested by national intelligence work agencies, or warnings or detention for up to fifteen days by national security or public security organs. If a crime is constituted, criminal liability shall be pursued according to the law.

Article 29: Those who disclose state secrets related to national intelligence work may be subject to disciplinary action by the relevant units as suggested by national intelligence work agencies, or warnings or detention for up to fifteen days by national security or public security organs. If a crime is constituted, criminal liability shall be pursued according to the law.

Article 30: Those who impersonate national intelligence work agency staff or other relevant personnel to engage in fraudulent activities, scams, extortion, or similar offenses shall be punished according to the "Law of the People's Republic of China on Public Security Administration." If a crime is constituted, criminal liability shall be pursued according to the law.

Article 31: National intelligence work agencies and their staff who exceed their authority, abuse their power, infringe on the legal rights and interests of citizens and organizations, use their positions for personal gain, or disclose state secrets, commercial secrets, and personal information shall be disciplined according to the law. If a crime is constituted, criminal liability shall be pursued according to the law.

Chapter 5: Supplementary Provisions

Article 32: This law shall come into effect on June 28, 2017.

# 中华人民共和国国家情报法

(2017年6月27日第十二届全国人民代表大会常务委员会第二十八次会议通过 根据2018年4月27日第十三届全国人民代表大会常务委员会第二次会议《关于修改〈中华人民共和国国境卫生检疫法〉等六部法律的决定》修正)

浏览字号: 大 中 小来源: 中国人大网 2018年6月12日 14:48:46

## 目 录

第一章 总 则

第二章 国家情报工作机构职权

第三章 国家情报工作保障

第四章 法律责任

第五章 附 则

## 第一章 总 则

**第一条** 为了加强和保障国家情报工作,维护国家安全和利益,根据宪法,制定本法

。

**第二条** 国家情报工作坚持总体国家安全观,为国家重大决策提供情报参考,为防范和化解危害国家安全的风险提供情报支持,维护国家政权、主权、统一和领土完整、人民福祉、经济社会可持续发展和国家其他重大利益。

**第三条** 国家建立健全集中统一、分工协作、科学高效的国家情报体制。

中央国家安全领导机构对国家情报工作实行统一领导,制定国家情报工作方针政策,规划国家情报工作整体发展,建立健全国家情报工作协调机制,统筹协调各领域国家情报工作,研究决定国家情报工作中的重大事项。

中央军事委员会统一领导和组织军队情报工作。

**第四条** 国家情报工作坚持公开工作与秘密工作相结合、专门工作与群众路线相结合、分工负责与协作配合相结合的原则。

**第五条** 国家安全机关和公安机关情报机构、军队情报机构(以下统称国家情报工作机构)按照职责分工,相互配合,做好情报工作、开展情报行动。

各有关国家机关应当根据各自职能和任务分工，与国家情报工作机构密切配合。

**第六条** 国家情报工作机构及其工作人员应当忠于国家和人民，遵守宪法和法律，忠于职守，纪律严明，清正廉洁，无私奉献，坚决维护国家安全和利益。

**第七条** 任何组织和公民都应当依法支持、协助和配合国家情报工作，保守所知悉的国家情报工作秘密。

国家对支持、协助和配合国家情报工作的个人和组织给予保护。

**第八条** 国家情报工作应当依法进行，尊重和保障人权，维护个人和组织的合法权益。

**第九条** 国家对在国家情报工作中作出重大贡献的个人和组织给予表彰和奖励。

## **第二章 国家情报工作机构职权**

**第十条** 国家情报工作机构根据工作需要，依法使用必要的方式、手段和渠道，在境内外开展情报工作。

**第十一条** 国家情报工作机构应当依法搜集和处理境外机构、组织、个人实施或者指使、资助他人实施的，或者境内外机构、组织、个人相勾结实施的危害中华人民共和国国家安全和利益行为的相关情报，为防范、制止和惩治上述行为提供情报依据或者参考。

**第十二条** 国家情报工作机构可以按照国家有关规定，与有关个人和组织建立合作关系，委托开展相关工作。

**第十三条** 国家情报工作机构可以按照国家有关规定，开展对外交流与合作。

**第十四条** 国家情报工作机构依法开展情报工作，可以要求有关机关、组织和公民提供必要的支持、协助和配合。

**第十五条** 国家情报工作机构根据工作需要，按照国家有关规定，经过严格的批准手续，可以采取技术侦察措施和身份保护措施。

**第十六条** 国家情报工作机构工作人员依法执行任务时，按照国家有关规定，经过批准，出示相应证件，可以进入限制进入的有关区域、场所，可以向有关机关、组织和个人了解、询问有关情况，可以查阅或者调取有关的档案、资料、物品。

**第十七条** 国家情报工作机构工作人员因执行紧急任务需要，经出示相应证件，可以享受通行便利。

国家情报工作机构工作人员根据工作需要，按照国家有关规定，可以优先使用或者依法征用有关机关、组织和个人的交通工具、通信工具、场地和建筑物，必要时，可以设置相关工作场所和设备、设施，任务完成后应当及时归还或者恢复原状，并依照规定支付相应费用；造成损失的，应当补偿。

**第十八条** 国家情报工作机构根据工作需要，按照国家有关规定，可以提请海关、出入境边防检查等机关提供免检等便利。

**第十九条** 国家情报工作机构及其工作人员应当严格依法办事，不得超越职权、滥用职权，不得侵犯公民和组织的合法权益，不得利用职务便利为自己或者他人谋取私利，不得泄露国家秘密、商业秘密和个人信息。

### **第三章 国家情报工作保障**

**第二十条** 国家情报工作机构及其工作人员依法开展情报工作，受法律保护。

**第二十一条** 国家加强国家情报工作机构建设，对其机构设置、人员、编制、经费、资产实行特殊管理，给予特殊保障。

国家建立适应情报工作需要的人员录用、选调、考核、培训、待遇、退出等管理制度。

**第二十二条** 国家情报工作机构应当适应情报工作需要，提高开展情报工作的能力。

国家情报工作机构应当运用科学技术手段，提高对情报信息的鉴别、筛选、综合和研判分析水平。

**第二十三条** 国家情报工作机构工作人员因执行任务，或者与国家情报工作机构建立合作关系的人员因协助国家情报工作，其本人或者近亲属人身安全受到威胁时，国家有关部门应当采取必要措施，予以保护、营救。

**第二十四条** 对为国家情报工作作出贡献并需要安置的人员，国家给予妥善安置。



公安、民政、财政、卫生、教育、人力资源社会保障、退役军人事务、医疗保障等有关部门以及国有企业事业单位应当协助国家情报工作机构做好安置工作。

**第二十五条** 对因开展国家情报工作或者支持、协助和配合国家情报工作导致伤残或者牺牲、死亡的人员，按照国家有关规定给予相应的抚恤优待。

个人和组织因支持、协助和配合国家情报工作导致财产损失的，按照国家有关规定给予补偿。

**第二十六条** 国家情报工作机构应当建立健全严格的监督和安全审查制度，对其工作人员遵守法律和纪律等情况进行监督，并依法采取必要措施，定期或者不定期进行安全审查。

**第二十七条** 任何个人和组织对国家情报工作机构及其工作人员超越职权、滥用职权和其他违法违纪行为，有权检举、控告。受理检举、控告的有关机关应当及时查处，并将查处结果告知检举人、控告人。

对依法检举、控告国家情报工作机构及其工作人员的个人和组织，任何个人和组织不得压制和打击报复。

国家情报工作机构应当为个人和组织检举、控告、反映情况提供便利渠道，并为检举人、控告人保密。

#### 第四章 法律 责 任

**第二十八条** 违反本法规定，阻碍国家情报工作机构及其工作人员依法开展情报工作的，由国家情报工作机构建议相关单位给予处分或者由国家安全机关、公安机关处警告或者十五日以下拘留；构成犯罪的，依法追究刑事责任。

**第二十九条** 泄露与国家情报工作有关的国家秘密的，由国家情报工作机构建议相关单位给予处分或者由国家安全机关、公安机关处警告或者十五日以下拘留；构成犯罪的，依法追究刑事责任。

**第三十条** 冒充国家情报工作机构工作人员或者其他相关人员实施招摇撞骗、诈骗、敲诈勒索等行为的，依照《中华人民共和国治安管理处罚法》的规定处罚；构成犯罪的，依法追究刑事责任。

**第三十一条** 国家情报工作机构及其工作人员有超越职权、滥用职权，侵犯公民和组织的合法权益，利用职务便利为自己或者他人谋取私利，泄露国家秘密、商业秘密和个人信息等违法违纪行为的，依法给予处分；构成犯罪的，依法追究刑事责任。

## **第五章 附 则**

**第三十二条** 本法自2017年6月28日起施行。

# EXHIBIT E

**Declaration of David Newman  
Principal Deputy Assistant Attorney General  
National Security Division  
Department of Justice**



---

# Certification of Translation

---



COUNTY OF SUFFOLK  
COMMONWEALTH OF MASSACHUSETTS

July 24, 2024

This is to certify that the attached translation is, to the best of my knowledge and belief, a true and accurate translation from Simplified Chinese into English of the attached document:

- **Counterespionage Law**

Linguistic Systems, Inc. adheres to an ISO-certified quality management system that ensures best practices are always followed in the selection of linguists skilled in both the languages and subject matters necessary for every translation.



Linguistic Systems, Inc.



260 Franklin Street, Suite 230, Boston MA 02110 • Phone 617-528-7400 • Fax 617-528-7490 • [www.linguist.com](http://www.linguist.com)

Certifications: ISO 9001 • ISO 17100 • ISO 18587 • ISO 27001

# Counter-Espionage Law of the People's Republic of China

Date: April 27, 2023 Source: Xinhua News Agency

Font Size: [Default](#) | [Large](#) | [Extra Large](#) | [Print](#)

Xinhua News Agency, Beijing, April 26

## Counter-Espionage Law of the People's Republic of China

(Passed at the 11th Meeting of the Standing Committee of the 12th National People's Congress on November 1, 2014, and revised at the 2nd Meeting of the Standing Committee of the 14th National People's Congress on April 26, 2023)

### Table of Contents

Chapter 1: General Provisions

Chapter 2: Security Precautions

Chapter 3: Investigation and Handling

Chapter 4: Safeguards and Supervision

Chapter 5: Legal Liability

Chapter 6: Supplementary Provisions

### Chapter 1: General Provisions

Article 1 In order to strengthen counter-espionage efforts, prevent, stop, and punish espionage activities, safeguard national security, and protect the interests of the people, this law is formulated in accordance with the Constitution.

Article 2 Counter-espionage work shall adhere to the centralized and unified leadership of the Party Central Committee, uphold the overall national security concept, combine public and secret work, integrate specialized work with the mass line, and adopt a proactive defense, lawful punishment, and a combination of treatment and prevention approach to fortify the national security and public defense line.

Article 3 Counter-espionage work must be carried out in accordance with the law, respecting and safeguarding human rights, and protecting the legal rights and interests of individuals and organizations.

Article 4 Espionage activities referred to in this law include the following behaviors:

(1) Activities that harm the national security of the People's Republic of China, carried out by espionage organizations or their agents, or directed, funded, or colluded in by domestic or foreign institutions, organizations, or individuals;

(2) Joining espionage organizations, accepting tasks from espionage organizations or their agents, or defecting to espionage organizations or their agents;

(3) Activities involving the theft, espionage, purchase, or illegal provision of national secrets, intelligence, and other documents, data, materials, and items related to national security and interests, carried out by foreign institutions, organizations, or individuals other than espionage organizations and their agents, or directed, funded, or colluded in by such entities, or activities aimed at inciting, enticing, coercing, or bribing state employees to betray;

(4) Network attacks, intrusions, interference, control, or destruction targeting government agencies, confidential units, or critical information infrastructure, carried out by espionage organizations or their agents, or directed, funded, or colluded in by domestic or foreign institutions, organizations, or individuals;

(5) Providing enemies with instructions on attack targets;

(6) Engaging in other espionage activities.

Espionage activities carried out by espionage organizations or their agents within the territory of the People's Republic of China, or using Chinese citizens, organizations, or other conditions to engage in espionage activities against a third country that harm the national security of the People's Republic of China, are subject to this law.

Article 5 The state establishes a counter-espionage coordination mechanism to oversee and coordinate major matters in counter-espionage work and to research and resolve significant problems related to counter-espionage.

Article 6 National security agencies are the principal authorities responsible for counter-espionage work.

Relevant departments such as public security, confidentiality, and military departments shall cooperate closely, enhance coordination, and perform their duties in accordance with the law according to their responsibilities.

Article 7 Citizens of the People's Republic of China have the duty to safeguard the nation's security, honor, and interests, and must not engage in activities that harm the national security,

honor, and interests.

All state organs and armed forces, political parties and people's organizations, enterprises and institutions, and other social organizations have the obligation to prevent and stop espionage activities and to safeguard national security.

The national security organs must rely on the support of the people in counter-espionage work, mobilizing and organizing the people to prevent and stop espionage activities.

Article 8 All citizens and organizations shall, according to the law, support and assist in counter-espionage work, and keep confidential any state secrets and counter-espionage work secrets they come to know.

Article 9 The state shall protect individuals and organizations that support and assist in counter-espionage work.

Individuals and organizations that report espionage activities or make significant contributions to counter-espionage work shall be honored and rewarded according to relevant national regulations.

Article 10 Espionage activities that are conducted or directed by foreign institutions, organizations, or individuals, or that are funded by them, or that involve domestic institutions, organizations, or individuals colluding with foreign entities, which harm the national security of the People's Republic of China, must be pursued under the law.

Article 11 National security agencies and their staff must act strictly according to the law in their work and shall not exceed their authority, abuse their power, or infringe upon the legitimate rights and interests of individuals and organizations.

Information about individuals and organizations obtained by national security agencies and their staff in the performance of counter-espionage duties may only be used for counter-espionage purposes. Such information that constitutes state secrets, work secrets, commercial secrets, or personal privacy and personal information must be kept confidential.

## Chapter 2 Security Prevention

Article 12 State organs, people's organizations, enterprises, institutions, and other social organizations shall bear the primary responsibility for the counter-espionage security prevention work within their units. They must implement counter-espionage security measures, educate their personnel about safeguarding national security, and mobilize and organize their personnel to prevent and stop espionage activities.

Local people's governments at all levels and relevant industry supervisory departments shall manage counter-espionage security prevention work within their administrative regions and industries according to their responsibilities.

National security agencies shall coordinate, guide, and supervise the counter-espionage security prevention work in accordance with the law.

Article 13 People's governments at all levels and relevant departments shall organize counter-espionage security prevention publicity and education activities, incorporating counter-espionage security prevention knowledge into education, training, and legal publicity content, to enhance national counter-espionage security awareness and national security literacy.

News, broadcasting, television, culture, and internet information service units should conduct targeted counter-espionage publicity and education for society.

National security agencies shall guide relevant units in conducting counter-espionage publicity and education activities based on the counter-espionage security prevention situation to improve awareness and capability.

Article 14 No individual or organization may unlawfully obtain or possess documents, data, materials, or items that are classified as state secrets.

Article 15 No individual or organization may unlawfully produce, sell, possess, or use specialized espionage equipment required for espionage activities. Specialized espionage equipment shall be confirmed by the national security supervisory department of the State Council in accordance with relevant national regulations.

Article 16 Any citizen or organization that discovers espionage activities should promptly report them to national security agencies. If reports are made to other state organs or organizations, those relevant state organs or organizations must immediately transfer the reports to national security agencies for handling.

National security agencies shall publicly disclose the contact details for reporting, such as telephone numbers, mailboxes, and online platforms, and handle the reports in a timely manner according to the law while keeping the identity of the informants confidential.



Article 17 The state shall establish a management system for key counter-espionage security prevention units.

Key counter-espionage security prevention units shall establish a counter-espionage security prevention work system, fulfill the requirements for counter-espionage security prevention work, and designate internal functional departments and personnel responsible for counter-espionage security prevention duties.

Article 18 Key counter-espionage security prevention units shall strengthen the education and management of staff regarding counter-espionage security prevention. They must supervise and inspect the fulfillment of counter-espionage security prevention obligations by personnel during their declassification period after leaving their positions or resigning.

Article 19 Key counter-espionage security prevention units shall enhance daily security prevention management of sensitive matters, locations, carriers, etc., and implement counter-espionage physical security measures such as isolation reinforcement, closed management, and setting up alerts.

Article 20 Key counter-espionage security prevention units shall, in accordance with the requirements and standards for counter-espionage technical prevention, take corresponding technical measures and other necessary actions to strengthen counter-espionage technical prevention for critical departments, network facilities, and information systems.

Article 21 For new construction, renovation, or expansion projects within the security control areas surrounding important national agencies, national defense and military-industrial units, and other significant confidential units and military facilities, the national security agency shall implement the construction project permits related to national security matters.

Local governments at or above the county level shall fully consider national security factors and designated security control areas when preparing national economic and social development plans, land use and spatial planning, and consult with national security agencies.

The designation of security control areas shall balance development and security, adhering to the principles of scientific rationality and necessity. It shall be jointly determined by national se-

curity agencies, along with departments such as development and reform, natural resources, housing and urban-rural development, confidentiality, national defense technology industry, and relevant military departments. This designation shall be reported to the people's governments of provinces, autonomous regions, and municipalities directly under the central government for approval and dynamic adjustment.

The specific implementation measures for construction project permits involving national security matters shall be formulated by the national security authority of the State Council in coordination with relevant departments.

Article 22 Based on the needs of counter-espionage work, national security agencies may, in conjunction with relevant departments, establish counter-espionage technical prevention standards, guide relevant units in implementing counter-espionage technical prevention measures, and, with strict approval procedures, conduct counter-espionage technical prevention inspections and tests on units with potential risks.

### Chapter 3 Investigation and Disposal

Article 23 The national security agency shall exercise the powers specified by this Law and other relevant laws in counter-espionage work.

Article 24 When performing counter-espionage duties in accordance with the law, personnel from the national security agency shall present their work credentials as required. They may verify the identity of Chinese citizens or foreign individuals, inquire about relevant situations from concerned individuals and organizations, and inspect the belongings of individuals suspected of espionage activities if their identity is unclear.

Article 25 When performing counter-espionage duties in accordance with the law, personnel from the national security agency, with the approval of the head of the national security agency at the municipal level or above, and presenting their work credentials, may inspect the electronic devices, facilities, and relevant procedures and tools of concerned individuals and organizations. If during the inspection, circumstances that endanger national security are found, the national security agency shall order corrective measures to be taken immediately. If there is a refusal to rectify or if national security hazards remain after correction, the agency may seal or seize the items.

For electronic devices, facilities, and relevant procedures and tools that are sealed or seized according to the previous paragraph, the national security agency shall promptly lift the seal or return the seized items after the situation endangering national security is resolved.

Article 26 When performing counter-espionage duties according to the law, personnel from the national security agency, with the approval of the head of the national security agency at the municipal level or above, may review and obtain relevant documents, data, materials, and items in accordance with national regulations. Concerned individuals and organizations are required to cooperate. The scope and extent of the review and retrieval must not exceed what is necessary for performing counter-espionage duties.

Article 27 If there is a need to summon individuals who violate this Law for investigation, a summons certificate must be used with the approval of the head of the case-handling department of the national security agency. For individuals discovered on-site violating this Law, personnel from the national security agency may verbally summon them by presenting their work credentials, but this must be noted in the interrogation record. The reason and basis for the summons must be explained to the summoned individual. Individuals who refuse to accept the summons without justifiable reasons or evade the summons may be forcibly summoned.

The national security agency shall conduct the inquiry at a designated location within the city or county where the summoned individual resides or at their residence.

The national security agency must promptly question and verify information from the summoned individual. The inquiry and verification time must not exceed eight hours. If the situation is complex and may involve administrative detention or criminal suspicion, the time must not exceed twenty-four hours. The national security agency must provide necessary food and rest time for the summoned individual. Continuous summoning is strictly prohibited.

Except in cases where notification is not possible or may hinder the investigation, the national security agency must promptly inform the family of the summoned individual of the reason for the summons. Once the situation preventing notification is resolved, the family should be immediately informed.

Article 28 When the national security agency investigates espionage activities, it may, with the approval of the head of the national security agency at the municipal level or above, legally

inspect the person, belongings, and places suspected of espionage activities.

If an inspection of a female body is required, it must be conducted by female personnel.

Article 29 When the national security agency investigates espionage activities, it may, with the approval of the head of the national security agency at the municipal level or above, check the relevant property information of individuals suspected of espionage.

Article 30 When investigating espionage activities, the national security agency may, with the approval of the head of the national security agency at the municipal level or above, legally seal, seize, or freeze locations, facilities, or property suspected of being used for espionage activities. Locations, facilities, or property unrelated to the espionage activities under investigation may not be sealed, seized, or frozen.

Article 31 When national security agency personnel carry out measures such as reviewing, retrieving, summoning, inspecting, querying, sealing, seizing, or freezing during counter-espionage work, at least two personnel must be involved. They must present work credentials and relevant legal documents in accordance with regulations, and relevant personnel must sign and stamp on written materials such as records.

Important evidence collection work such as inspections, sealing, and seizing must be recorded by audio and video throughout the process, with records kept for future reference.

Article 32 When the national security agency is investigating and collecting evidence related to espionage activities, relevant individuals and organizations must provide truthful information and cannot refuse.

Article 33 For Chinese citizens who, after leaving the country, may pose a threat to national security or cause significant damage to national interests, the State Council's national security department may decide to restrict their departure from the country for a certain period and notify immigration authorities.

For individuals suspected of espionage activities, national security agencies at the provincial level or above may notify immigration authorities to prohibit their departure from the country.

Article 34 For foreign individuals who may engage in activities harmful to the national security of the People's Republic of China after entering the country, the State Council's national security department may notify immigration authorities to prohibit their entry.

Article 35 Immigration authorities shall execute the decision of the national security agency regarding the prohibition of entry or exit in accordance with national regulations. If the reasons for the prohibition of entry or exit no longer apply, the national security agency must promptly revoke the decision and notify immigration authorities.

Article 36 When the national security agency discovers network information content or risks such as network attacks related to espionage activities, it shall, in accordance with the responsibilities set out in the Cybersecurity Law of the People's Republic of China, promptly notify the relevant departments for legal handling. The relevant departments may direct telecommunications operators and internet service providers to take timely measures such as patching vulnerabilities, strengthening network defenses, stopping transmission, removing programs and content, suspending related services, delisting relevant applications, and closing related websites, as well as preserving relevant records. In urgent situations where failure to act immediately would severely harm national security, the national security agency may order the relevant entities to patch vulnerabilities, stop related transmissions, and suspend relevant services, and report to the relevant departments.

If the relevant measures have been taken and the information content or risks have been resolved, the national security agency and relevant departments should promptly make decisions to restore relevant transmissions and services.

Article 37 For the needs of counter-espionage work, the national security agency, in accordance with national regulations and following strict approval procedures, may take technical reconnaissance measures and identity protection measures.

Article 38 In cases of violations of this law that involve criminal suspicions and require determination of whether relevant matters are state secrets or intelligence and assessment of harmful consequences, the national confidentiality departments or confidentiality departments at the provincial, autonomous region, or municipal level shall conduct the assessment and organize evaluations within a certain period in accordance with procedures.

Article 39 If, upon investigation, the national security agency finds that espionage activities involve criminal offenses, it shall initiate an investigation in accordance with the Criminal Procedure Law of the People's Republic of China.

#### Chapter 4: Safeguards and Supervision

Article 40: National security agency staff performing their duties in accordance with the law are protected by law.

Article 41: In the investigation of espionage activities by national security agencies, postal, courier, and other logistics operators, as well as telecommunications operators and internet service providers, must provide necessary support and assistance.

Article 42: National security agency staff, when performing urgent tasks, are entitled to priority access to public transportation and preferential passage, upon presenting their work credentials.

Article 43: When performing duties according to the law, national security agency staff may, upon presenting their work credentials, enter relevant locations and units. According to national regulations, with approval and upon presenting their work credentials, they may enter restricted areas, locations, and units.

Article 44: For counter-espionage work, national security agencies may, in accordance with national regulations, have priority use or requisition vehicles, communication tools, premises, and buildings from state organs, people's organizations, enterprises, and other social organizations as well as individuals. If necessary, they may set up related work sites and facilities. After the task is completed, these should be promptly returned or restored to their original condition, and the corresponding costs should be paid as required. Compensation should be provided for any losses incurred.

Article 45: For counter-espionage needs, national security agencies may, in accordance with national regulations, request customs, immigration control, and other inspection authorities to facilitate customs clearance for relevant personnel and exempt certain documents and equipment from inspection. Relevant inspection authorities shall provide assistance in accordance with the law.

Article 46: When national security agency staff or individuals assisting with counter-espionage tasks face threats to their personal safety, either themselves or their close relatives, national security agencies shall, in conjunction with relevant departments, take necessary measures to provide protection and rescue.

Individuals facing danger to their personal safety due to supporting or assisting counter-espionage work may request protection from national security agencies. The agencies shall, in conjunction with relevant departments, take protective measures as required by law.

Individuals and organizations that suffer property losses due to supporting or assisting counter-espionage work shall be compensated according to national regulations.

Article 47: Personnel who have made contributions to counter-espionage work and need resettlement shall be properly resettled by the state.

Departments such as public security, civil affairs, finance, health, education, human resources and social security, veterans' affairs, medical insurance, immigration management, and state-owned enterprises and institutions should assist national security agencies with resettlement work.

Article 48: Personnel who become disabled, or who die, due to counter-espionage work or supporting and assisting such work shall receive corresponding compensation and preferential treatment according to national regulations.

Article 49: The state encourages technological innovation in the field of counter-espionage and aims to leverage technology in counter-espionage work.

Article 50: National security agencies should strengthen the development and professional training of their counter-espionage personnel to enhance their capabilities.

Staff in national security agencies should receive planned political, theoretical, and professional training. Training should link theory to practice, be tailored to needs, and focus on practical results to improve professional skills.

Article 51: National security agencies should strictly implement internal supervision and security review systems. They should oversee their staff's adherence to laws and discipline, and

take necessary measures, conducting regular or irregular security reviews as required by law.

Article 52: Any individual or organization has the right to report or file complaints about abuse of power, exceeding of authority, or other illegal actions by national security agencies and their staff to higher national security agencies, supervisory authorities, people's procuratorates, or other relevant departments.

The national security agency, supervisory authority, or people's procuratorate receiving the report or complaint should promptly investigate the facts, handle the matter according to the law, and inform the whistleblower or complainant of the outcome.

No individual or organization shall suppress or retaliate against those who support or assist national security agencies or who lawfully report or complain.

#### Chapter 5: Legal Responsibilities

Article 53: Those who engage in espionage activities and constitute a crime shall be held criminally responsible according to the law.

Article 54: Individuals who engage in espionage activities but do not constitute a crime may be given a warning or administrative detention of up to fifteen days by the national security agency. They may also face a fine of up to 50,000 yuan, or, if the illegal gains exceed 50,000 yuan, a fine of up to five times the illegal gains, and may be subject to disciplinary action by relevant departments according to the law.

Those who knowingly provide information, funds, materials, labor, technology, or venues to support or assist others in engaging in espionage activities, or who harbor or shield such individuals, but do not constitute a crime, are subject to the same penalties as above.

If an organization engages in the behaviors described in the previous two paragraphs, it will receive a warning from the national security agency and may be fined up to 500,000 yuan. If the illegal gains exceed 500,000 yuan, the fine may be up to five times the illegal gains. Additionally, the directly responsible managers and other directly responsible personnel will be punished according to the provisions of the first paragraph.

The national security agency, based on the illegal circumstances and consequences of relevant units and personnel, may recommend that relevant supervising departments order the suspension of related business, services, or production, revoke relevant licenses, or cancel registrations.



The relevant supervising departments should promptly report the administrative actions to the national security agency.

Article 55 : Those who engage in espionage activities and show repentance or significant achievements in the process may receive lighter, reduced, or exempted penalties. Those who make major contributions will be rewarded.

Article 56: If state organs, people's organizations, enterprises, institutions, and other social organizations fail to fulfill their counter-espionage security prevention obligations as required by this law, the national security agency can order them to make corrections. If they do not correct the issue as required, the national security agency may interview the relevant responsible persons and, if necessary, report the interview results to the unit's superior department. If harmful consequences or negative impacts arise, the national security agency can issue a warning or public criticism. In severe cases, responsible leaders and directly responsible personnel may be disciplined by relevant departments according to the law.

Article 57: For violations of Article 21 of this law regarding new, rebuilt, or expanded construction projects, the national security agency shall order corrections and issue a warning. If the corrections are refused or the situation is severe, the agency may order the suspension of construction or use, temporarily withhold or revoke permits, or recommend that the relevant supervising department handle the matter according to the law.

Article 58: Violations of Article 41 of this law shall result in the national security agency ordering corrections, issuing a warning or public criticism. If corrections are refused or the situation is severe, the relevant supervising department shall impose penalties according to relevant laws and regulations.

Article 59: Violations of this law involving refusal to cooperate with data retrieval will be penalized by the national security agency according to the relevant provisions of the Cybersecurity Law of the People's Republic of China.

Article 60: Violations of this law involving any of the following behaviors will be subject to criminal liability if they constitute a crime; if they do not constitute a crime, the national security agency may issue a warning or impose administrative detention of up to ten days, and may also impose a fine of up to 30,000 yuan:

- (1) Revealing national secrets related to counter-espionage work;
- (2) Refusing to provide information when aware that others are involved in espionage crimes, during an investigation by national security agencies into relevant situations and evidence collection;
- (3) Deliberately obstructing national security agencies in the lawful execution of their tasks;
- (4) Hiding, transferring, selling, or destroying property that has been lawfully sealed, seized, or frozen by national security agencies;
- (5) Concealing, transferring, purchasing, selling, or otherwise hiding property known to be involved in espionage activities;
- (6) Retaliating against individuals or organizations that lawfully support or assist national security agencies.

Article 61 If the illegal acquisition, possession of documents, data, materials, or items classified as national secrets, as well as the illegal production, sale, possession, or use of specialized espionage equipment, does not constitute a crime, the national security agency may issue a warning or impose administrative detention of up to ten days.

Article 62 The national security agency must properly safeguard property that has been sealed, seized, or frozen in accordance with this law and handle it as follows:

(1) If criminal activity is suspected, handle it according to the provisions of the Criminal Procedure Law of the People's Republic of China and other relevant laws.

(2) If the activity does not constitute a crime but there are illegal facts, items that should be confiscated by law must be confiscated, and those that should be destroyed by law must be destroyed.

(3) If there are no illegal facts or the items are unrelated to the case, the seal, seizure, or freeze must be lifted and the relevant property should be promptly returned. If losses are caused, compensation must be provided according to the law.

Article 63 If the property involved in the case meets any of the following conditions, it

should be recovered, confiscated, or measures should be taken to eliminate the risks according to the law:

- (1) Property obtained through illegal means and its proceeds, and property used for carrying out espionage activities.
- (2) Documents, data, materials, and items that are classified as state secrets and obtained or held illegally.
- (3) Specialized espionage equipment that is produced, sold, held, or used illegally.

Article 64 All benefits obtained by the perpetrator and their close relatives or other relevant personnel from espionage organizations and their agents are to be confiscated or seized by the national security organs according to the law.

Article 65 Fines collected and property confiscated by national security organs are to be submitted to the national treasury.

Article 66 For foreigners who violate this law, the State Council's national security authority can decide to deport them within a specified period and impose a restriction on their re-entry. If they do not leave within the specified period, they may be forcibly expelled.

For foreigners who violate this law and are expelled, they are prohibited from re-entering for ten years from the date of expulsion. The decision of the State Council's national security authority is final.

Article 67: Before making an administrative penalty decision, the national security organs shall inform the concerned party of the proposed administrative penalty content, facts, reasons, and legal basis, as well as the party's rights to make statements, defenses, and request a hearing in accordance with the Administrative Penalty Law of the People's Republic of China.

Article 68: If the concerned party disagrees with the administrative penalty decision, administrative enforcement decision, or administrative licensing decision, they may apply for reconsideration within sixty days from the date of receiving the decision. If they disagree with the reconsideration decision, they may file a lawsuit with the People's Court within fifteen days from the date of receiving the reconsideration decision.

Article 69: National security personnel who abuse their powers, neglect their duties, engage

in favoritism, or commit illegal detention, torture, coercion, violent evidence collection, or unauthorized disclosure of national secrets, work secrets, commercial secrets, personal privacy, or personal information shall be subject to disciplinary action according to the law. If their actions constitute a crime, they shall be held criminally responsible in accordance with the law.

#### Chapter 6 Supplementary Provisions

Article 70: The national security organs shall perform their duties related to the prevention, suppression, and punishment of espionage activities and other activities that endanger national security in accordance with laws, administrative regulations, and relevant national provisions. Relevant provisions of this law shall apply.

The public security organs shall apply relevant provisions of this law when discovering and punishing activities that endanger national security in the course of performing their duties in accordance with the law.

Article 71 This law shall come into effect on July 1, 2023.

# 中华人民共和国反间谍法

2023-04-27 08:22 来源： 新华社

字号：默认 大 超大 | 打印 |

新华社北京4月26日电

## 中华人民共和国反间谍法

(2014年11月1日第十二届全国人民代表大会常务委员会第十一次会议通过 2023年4月26日第十四届全国人民代表大会常务委员会第二次会议修订)

### 目录

第一章 总则

第二章 安全防范

第三章 调查处置

第四章 保障与监督

第五章 法律责任

第六章 附则

第一章 总则

第一条 为了加强反间谍工作，防范、制止和惩治间谍行为，维护国家安全，保护人民利益，根据宪法，制定本法。

第二条 反间谍工作坚持党中央集中统一领导，坚持总体国家安全观，坚持公开工作与秘密工作相结合、专门工作与群众路线相结合，坚持积极防御、依法惩治、标本兼治，筑牢国家安全人民防线。

第三条 反间谍工作应当依法进行，尊重和保障人权，保障个人和组织的合法权益。

第四条 本法所称间谍行为，是指下列行为：

(一) 间谍组织及其代理人实施或者指使、资助他人实施，或者境内外机构、组织、个人与其相勾结实施的危害中华人民共和国国家安全的活动；

(二) 参加间谍组织或者接受间谍组织及其代理人的任务，或者投靠间谍组织及其代理人；

(三) 间谍组织及其代理人以外的其他境外机构、组织、个人实施或者指使、资助他人实施，或者境内机构、组织、个人与其相勾结实施的窃取、刺探、收买、非法提供国家秘密、情报以及其他关系国家安全和利益的文件、数据、资料、物品，或者策动、引诱、胁迫、收买国家工作人员叛变的活动；

(四) 间谍组织及其代理人实施或者指使、资助他人实施，或者境内外机构、组织、个人与其相勾结实施针对国家机关、涉密单位或者关键信息基础设施等的网络攻击、侵入、干扰、控制、破坏等活动；

(五) 为敌人指示攻击目标；

(六) 进行其他间谍活动。

间谍组织及其代理人在中华人民共和国领域内，或者利用中华人民共和国的公民、组织或者其他条件，从事针对第三国的间谍活动，危害中华人民共和国国家安全的，适用本法。

第五条 国家建立反间谍工作协调机制，统筹协调反间谍工作中的重大事项，研究、解决反间谍工作中的重大问题。

第六条 国家安全机关是反间谍工作的主管机关。

公安、保密等有关部门和军队有关部门按照职责分工，密切配合，加强协调，依法做好有关工作。

第七条 中华人民共和国公民有维护国家的安全、荣誉和利益的义务，不得有危害国家的安全、荣誉和利益的行为。

一切国家机关和武装力量、各政党和各人民团体、企业事业组织和其他社会组织，都有防范、制止间谍行为，维护国家安全的义务。

国家安全机关在反间谍工作中必须依靠人民的支持，动员、组织人民防范、制止间谍行为。

第八条 任何公民和组织都应当依法支持、协助反间谍工作，保守所知悉的国家秘密和反间谍工作秘密。

第九条 国家对支持、协助反间谍工作的个人和组织给予保护。

对举报间谍行为或者在反间谍工作中做出重大贡献的个人和组织，按照国家有关规定给予表彰和奖励。

第十条 境外机构、组织、个人实施或者指使、资助他人实施的，或者境内机构、组织、个人与境外机构、组织、个人相勾结实施的危害中华人民共和国国家安全的间谍行为，都必须受到法律追究。

第十一条 国家安全机关及其工作人员在工作中，应当严格依法办事，不得超越职权、滥用职权，不得侵犯个人和组织的合法权益。

国家安全机关及其工作人员依法履行反间谍工作职责获取的个人和组织的信息，只能用于反间谍工作。对属于国家秘密、工作秘密、商业秘密和个人隐私、个人信息的，应当保密。

## 第二章 安全防范

第十二条 国家机关、人民团体、企业事业组织和其他社会组织承担本单位反间谍安全防范工作的主体责任，落实反间谍安全防范措施，对本单位的人员进行维护国家安全的教育，动员、组织本单位的人员防范、制止间谍行为。

地方各级人民政府、相关行业主管部门按照职责分工，管理本行政区域、本行业有关反间谍安全防范工作。

国家安全机关依法协调指导、监督检查反间谍安全防范工作。

第十三条 各级人民政府和有关部门应当组织开展反间谍安全防范宣传教育，将反间谍安全防范知识纳入教育、培训、普法宣传内容，增强全民反间谍安全防范意识和国家安全素养。

新闻、广播、电视、文化、互联网信息服务等单位，应当面向社会有针对性地开展反间谍宣传教育。

国家安全机关应当根据反间谍安全防范形势，指导有关单位开展反间谍宣传教育活动，提高防范意识和能力。

第十四条 任何个人和组织都不得非法获取、持有属于国家秘密的文件、数据、资料、物品。

第十五条 任何个人和组织都不得非法生产、销售、持有、使用间谍活动特殊需要的专用间谍器材。专用间谍器材由国务院国家安全主管部门依照国家有关规定确认。

第十六条 任何公民和组织发现间谍行为，应当及时向国家安全机关举报；向公安机关等其他国家机关、组织举报的，相关国家机关、组织应当立即移送国家安全机关处理。

国家安全机关应当将受理举报的电话、信箱、网络平台等向社会公开，依法及时处理举报信息，并为举报人保密。

第十七条 国家建立反间谍安全防范重点单位管理制度。

反间谍安全防范重点单位应当建立反间谍安全防范工作制度，履行反间谍安全防范工作要求，明确内设职能部门和人员承担反间谍安全防范职责。

第十八条 反间谍安全防范重点单位应当加强对工作人员反间谍安全防范的教育和管理，对离岗离职人员脱密期内履行反间谍安全防范义务的情况进行监督检查。

第十九条 反间谍安全防范重点单位应当加强对涉密事项、场所、载体等的日常安全防范管理，采取隔离加固、封闭管理、设置警戒等反间谍物理防范措施。



第二十条 反间谍安全防范重点单位应当按照反间谍技术防范的要求和标准，采取相应的技术措施和其他必要措施，加强对要害部门部位、网络设施、信息系统的反间谍技术防范。

第二十一条 在重要国家机关、国防军工单位和其他重要涉密单位以及重要军事设施的周边安全控制区域内新建、改建、扩建建设项目的，由国家安全机关实施涉及国家安全事项的建设项目许可。

县级以上地方各级人民政府编制国民经济和社会发展规划、国土空间规划等有关规划，应当充分考虑国家安全因素和划定的安全控制区域，征求国家安全机关的意见。

安全控制区域的划定应当统筹发展和安全，坚持科学合理、确有必要的原则，由国家安全机关会同发展改革、自然资源、住房城乡建设、保密、国防科技工业等部门以及军队有关部门共同划定，报省、自治区、直辖市人民政府批准并动态调整。

涉及国家安全事项的建设项目许可的具体实施办法，由国务院国家安全主管部门会同有关部门制定。

第二十二条 国家安全机关根据反间谍工作需要，可以会同有关部门制定反间谍技术防范标准，指导有关单位落实反间谍技术防范措施，对存在隐患的单位，经过严格的批准手续，可以进行反间谍技术防范检查和检测。

### 第三章 调查处置

第二十三条 国家安全机关在反间谍工作中依法行使本法和有关法律规定的职权。

第二十四条 国家安全机关工作人员依法执行反间谍工作任务时，依照规定出示工作证件，可以查验中国公民或者境外人员的身份证明，向有关个人和组织问询有关情况，对身份不明、有间谍行为嫌疑的人员，可以查看其随带物品。

第二十五条 国家安全机关工作人员依法执行反间谍工作任务时，经设区的市级以上国家安全机关负责人批准，出示工作证件，可以查验有关个人和组织的电子设备、设施及

有关程序、工具。查验中发现存在危害国家安全情形的，国家安全机关应当责令其采取措施立即整改。拒绝整改或者整改后仍存在危害国家安全隐患的，可以予以查封、扣押。

对依照前款规定查封、扣押的电子设备、设施及有关程序、工具，在危害国家安全的情形消除后，国家安全机关应当及时解除查封、扣押。

第二十六条 国家安全机关工作人员依法执行反间谍工作任务时，根据国家有关规定，经设区的市级以上国家安全机关负责人批准，可以查阅、调取有关的文件、数据、资料、物品，有关个人和组织应当予以配合。查阅、调取不得超出执行反间谍工作任务所需的范围和限度。

第二十七条 需要传唤违反本法的人员接受调查的，经国家安全机关办案部门负责人批准，使用传唤证传唤。对现场发现的违反本法的人员，国家安全机关工作人员依照规定出示工作证件，可以口头传唤，但应当在询问笔录中注明。传唤的原因和依据应当告知被传唤人。对无正当理由拒不接受传唤或者逃避传唤的人，可以强制传唤。

国家安全机关应当在被传唤人所在市、县内的指定地点或者其住所进行询问。

国家安全机关对被传唤人应当及时询问查证。询问查证的时间不得超过八小时；情况复杂，可能适用行政拘留或者涉嫌犯罪的，询问查证的时间不得超过二十四小时。国家安全机关应当为被传唤人提供必要的饮食和休息时间。严禁连续传唤。

除无法通知或者可能妨碍调查的情形以外，国家安全机关应当及时将传唤的原因通知被传唤人家属。在上述情形消失后，应当立即通知被传唤人家属。

第二十八条 国家安全机关调查间谍行为，经设区的市级以上国家安全机关负责人批准，可以依法对涉嫌间谍行为的人身、物品、场所进行检查。

检查女性身体的，应当由女性工作人员进行。

第二十九条 国家安全机关调查间谍行为，经设区的市级以上国家安全机关负责人批准，可以查询涉嫌间谍行为人员的相关财产信息。

第三十条 国家安全机关调查间谍行为，经设区的市级以上国家安全机关负责人批准，可以对涉嫌用于间谍行为的场所、设施或者财物依法查封、扣押、冻结；不得查封、扣押、冻结与被调查的间谍行为无关的场所、设施或者财物。

第三十一条 国家安全机关工作人员在反间谍工作中采取查阅、调取、传唤、检查、查询、查封、扣押、冻结等措施，应当由二人以上进行，依照有关规定出示工作证件及相关法律文书，并由相关人员在有关笔录等书面材料上签名、盖章。

国家安全机关工作人员进行检查、查封、扣押等重要取证工作，应当对全过程进行录音录像，留存备查。

第三十二条 在国家安全机关调查了解有关间谍行为的情况、收集有关证据时，有关个人和组织应当如实提供，不得拒绝。

第三十三条 对出境后可能对国家安全造成危害，或者对国家利益造成重大损失的中国公民，国务院国家安全主管部门可以决定其在一定期限内不准出境，并通知移民管理机构。

对涉嫌间谍行为人员，省级以上国家安全机关可以通知移民管理机构不准其出境。

第三十四条 对入境后可能进行危害中华人民共和国国家安全活动的境外人员，国务院国家安全主管部门可以通知移民管理机构不准其入境。

第三十五条 对国家安全机关通知不准出境或者不准入境的人员，移民管理机构应当按照国家有关规定执行；不准出境、入境情形消失的，国家安全机关应当及时撤销不准出境、入境决定，并通知移民管理机构。

第三十六条 国家安全机关发现涉及间谍行为的网络信息内容或者网络攻击等风险，应当依照《中华人民共和国网络安全法》规定的职责分工，及时通报有关部门，由其依法处置或者责令电信业务经营者、互联网服务提供者及时采取修复漏洞、加固网络防护、停止传输、消除程序和内容、暂停相关服务、下架相关应用、关闭相关网站等措施，保存相

关记录。情况紧急，不立即采取措施将对国家安全造成严重危害的，由国家安全机关责令有关单位修复漏洞、停止相关传输、暂停相关服务，并通报有关部门。

经采取相关措施，上述信息内容或者风险已经消除的，国家安全机关和有关部门应当及时作出恢复相关传输和服务的决定。

第三十七条 国家安全机关因反间谍工作需要，根据国家有关规定，经过严格的批准手续，可以采取技术侦察措施和身份保护措施。

第三十八条 对违反本法规定，涉嫌犯罪，需要对有关事项是否属于国家秘密或者情报进行鉴定以及需要对危害后果进行评估的，由国家保密部门或者省、自治区、直辖市保密部门按照程序在一定期限内进行鉴定和组织评估。

第三十九条 国家安全机关经调查，发现间谍行为涉嫌犯罪的，应当依照《中华人民共和国刑事诉讼法》的规定立案侦查。

#### 第四章 保障与监督

第四十条 国家安全机关工作人员依法履行职责，受法律保护。

第四十一条 国家安全机关依法调查间谍行为，邮政、快递等物流运营单位和电信业务经营者、互联网服务提供者应当提供必要的支持和协助。

第四十二条 国家安全机关工作人员因执行紧急任务需要，经出示工作证件，享有优先乘坐公共交通工具、优先通行等通行便利。

第四十三条 国家安全机关工作人员依法执行任务时，依照规定出示工作证件，可以进入有关场所、单位；根据国家有关规定，经过批准，出示工作证件，可以进入限制进入的有关地区、场所、单位。

第四十四条 国家安全机关因反间谍工作需要，根据国家有关规定，可以优先使用或者依法征用国家机关、人民团体、企业事业组织和其他社会组织以及个人的交通工具、通信工具、场地和建筑物等，必要时可以设置相关工作场所和设施设备，任务完成后应当及时归还或者恢复原状，并依照规定支付相应费用；造成损失的，应当给予补偿。

第四十五条 国家安全机关因反间谍工作需要，根据国家有关规定，可以提请海关、移民管理等检查机关对有关人员提供通关便利，对有关资料、器材等予以免检。有关检查机关应当依法予以协助。

第四十六条 国家安全机关工作人员因执行任务，或者个人因协助执行反间谍工作任务，本人或者其近亲属的人身安全受到威胁时，国家安全机关应当会同有关部门依法采取必要措施，予以保护、营救。

个人因支持、协助反间谍工作，本人或者其近亲属的人身安全面临危险的，可以向国家安全机关请求予以保护。国家安全机关应当会同有关部门依法采取保护措施。

个人和组织因支持、协助反间谍工作导致财产损失的，根据国家有关规定给予补偿。

第四十七条 对为反间谍工作做出贡献并需要安置的人员，国家给予妥善安置。

公安、民政、财政、卫生健康、教育、人力资源和社会保障、退役军人事务、医疗保障、移民管理等有关部门以及国有企业事业单位应当协助国家安全机关做好安置工作。

第四十八条 对因开展反间谍工作或者支持、协助反间谍工作导致伤残或者牺牲、死亡的人员，根据国家有关规定给予相应的抚恤优待。

第四十九条 国家鼓励反间谍领域科技创新，发挥科技在反间谍工作中的作用。

第五十条 国家安全机关应当加强反间谍专业力量人才队伍建设和专业训练，提升反间谍工作能力。

对国家安全机关工作人员应当有计划地进行政治、理论和业务培训。培训应当坚持理论联系实际、按需施教、讲求实效，提高专业能力。

第五十一条 国家安全机关应当严格执行内部监督和安全审查制度，对其工作人员遵守法律和纪律等情况进行监督，并依法采取必要措施，定期或者不定期进行安全审查。

第五十二条 任何个人和组织对国家安全机关及其工作人员超越职权、滥用职权和其他违法行为，都有权向上级国家安全机关或者监察机关、人民检察院等有关部门检举、控

告。受理检举、控告的国家安全机关或者监察机关、人民检察院等有关部门应当及时查清事实，依法处理，并将处理结果及时告知检举人、控告人。

对支持、协助国家安全机关工作或者依法检举、控告的个人和组织，任何个人和组织不得压制和打击报复。

## 第五章 法律责任

第五十三条 实施间谍行为，构成犯罪的，依法追究刑事责任。

第五十四条 个人实施间谍行为，尚不构成犯罪的，由国家安全机关予以警告或者处十五日以下行政拘留，单处或者并处五万元以下罚款，违法所得在五万元以上的，单处或者并处违法所得一倍以上五倍以下罚款，并可以由有关部门依法予以处分。

明知他人实施间谍行为，为其提供信息、资金、物资、劳务、技术、场所等支持、协助，或者窝藏、包庇，尚不构成犯罪的，依照前款的规定处罚。

单位有前两款行为的，由国家安全机关予以警告，单处或者并处五十万元以下罚款，违法所得在五十万元以上的，单处或者并处违法所得一倍以上五倍以下罚款，并对直接负责的主管人员和其他直接责任人员，依照第一款的规定处罚。

国家安全机关根据相关单位、人员违法情节和后果，可以建议有关主管部门依法责令停止从事相关业务、提供相关服务或者责令停产停业、吊销有关证照、撤销登记。有关主管部门应当将作出行政处理的情况及时反馈国家安全机关。

第五十五条 实施间谍行为，有自首或者立功表现的，可以从轻、减轻或者免除处罚；有重大立功表现的，给予奖励。

在境外受胁迫或者受诱骗参加间谍组织、敌对组织，从事危害中华人民共和国国家安全的活动，及时向中华人民共和国驻外机构如实说明情况，或者入境后直接或者通过所在单位及时向国家安全机关如实说明情况，并有悔改表现的，可以不予追究。

第五十六条 国家机关、人民团体、企业事业组织和其他社会组织未按照本法规定履行反间谍安全防范义务的，国家安全机关可以责令改正；未按照要求改正的，国家安全机

关可以约谈相关负责人，必要时可以将约谈情况通报该单位上级主管部门；产生危害后果或者不良影响的，国家安全机关可以予以警告、通报批评；情节严重的，对负有责任的领导人员和直接责任人员，由有关部门依法予以处分。

第五十七条 违反本法第二十一条规定新建、改建、扩建建设项目的，由国家安全机关责令改正，予以警告；拒不改正或者情节严重的，责令停止建设或者使用、暂扣或者吊销许可证件，或者建议有关主管部门依法予以处理。

第五十八条 违反本法第四十一条规定的，由国家安全机关责令改正，予以警告或者通报批评；拒不改正或者情节严重的，由有关主管部门依照相关法律法规予以处罚。

第五十九条 违反本法规定，拒不配合数据调取的，由国家安全机关依照《中华人民共和国数据安全法》的有关规定予以处罚。

第六十条 违反本法规定，有下列行为之一，构成犯罪的，依法追究刑事责任；尚不构成犯罪的，由国家安全机关予以警告或者处十日以下行政拘留，可以并处三万元以下罚款：

- （一）泄露有关反间谍工作的国家秘密；
- （二）明知他人有间谍犯罪行为，在国家安全机关向其调查有关情况、收集有关证据时，拒绝提供；
- （三）故意阻碍国家安全机关依法执行任务；
- （四）隐藏、转移、变卖、损毁国家安全机关依法查封、扣押、冻结的财物；
- （五）明知是间谍行为的涉案财物而窝藏、转移、收购、代为销售或者以其他方法掩饰、隐瞒；
- （六）对依法支持、协助国家安全机关工作的个人和组织进行打击报复。

第六十一条 非法获取、持有属于国家秘密的文件、数据、资料、物品，以及非法生产、销售、持有、使用专用间谍器材，尚不构成犯罪的，由国家安全机关予以警告或者处十日以下行政拘留。

第六十二条 国家安全机关对依照本法查封、扣押、冻结的财物，应当妥善保管，并按照下列情形分别处理：

（一）涉嫌犯罪的，依照《中华人民共和国刑事诉讼法》等有关法律的规定处理；

（二）尚不构成犯罪，有违法事实的，对依法应当没收的予以没收，依法应当销毁的予以销毁；

（三）没有违法事实的，或者与案件无关的，应当解除查封、扣押、冻结，并及时返还相关财物；造成损失的，应当依法予以赔偿。

第六十三条 涉案财物符合下列情形之一的，应当依法予以追缴、没收，或者采取措施消除隐患：

（一）违法所得的财物及其孳息、收益，供实施间谍行为所用的本人财物；

（二）非法获取、持有的属于国家秘密的文件、数据、资料、物品；

（三）非法生产、销售、持有、使用的专用间谍器材。

第六十四条 行为人及其近亲属或者其他相关人员，因行为人实施间谍行为从间谍组织及其代理人获取的所有利益，由国家安全机关依法采取追缴、没收等措施。

第六十五条 国家安全机关依法收缴的罚款以及没收的财物，一律上缴国库。

第六十六条 境外人员违反本法的，国务院国家安全主管部门可以决定限期出境，并决定其不准入境的期限。未在规定期限内离境的，可以遣送出境。

对违反本法的境外人员，国务院国家安全主管部门决定驱逐出境的，自被驱逐出境之日起十年内不准入境，国务院国家安全主管部门的处罚决定为最终决定。



第六十七条 国家安全机关作出行政处罚决定之前，应当告知当事人拟作出的行政处罚内容及事实、理由、依据，以及当事人依法享有的陈述、申辩、要求听证等权利，并依照《中华人民共和国行政处罚法》的有关规定实施。

第六十八条 当事人对行政处罚决定、行政强制措施决定、行政许可决定不服的，可以自收到决定书之日起六十日内，依法申请复议；对复议决定不服的，可以自收到复议决定书之日起十五日内，依法向人民法院提起诉讼。

第六十九条 国家安全机关工作人员滥用职权、玩忽职守、徇私舞弊，或者有非法拘禁、刑讯逼供、暴力取证、违反规定泄露国家秘密、工作秘密、商业秘密和个人隐私、个人信息等行为，依法予以处分，构成犯罪的，依法追究刑事责任。

## 第六章 附则

第七十条 国家安全机关依照法律、行政法规和国家有关规定，履行防范、制止和惩治间谍行为以外的危害国家安全行为的职责，适用本法的有关规定。

公安机关在依法履行职责过程中发现、惩治危害国家安全的行为，适用本法的有关规定。

第七十一条 本法自2023年7月1日起施行。

### CERTIFICATE OF SERVICE

I hereby certify that on July 26, 2024, I filed the unredacted, classified version of this appendix by causing an original and three copies to be lodged with the Department of Justice Classified Information Security Officer. I further certify that on July 26, 2024, I electronically filed the public, unclassified version of this appendix with the Clerk of the Court for the United States Court of Appeals for the District of Columbia Circuit by using the appellate CM/ECF system. Service on all parties will be accomplished by the appellate CM/ECF system.

*/s/ Sean R. Janda*

---

Sean R. Janda