A BILL TO REGULATE FOREIGN-OWNED DIGITAL APPLICATIONS TO PROTECT U.S. NATIONAL SECURITY

BE IT ENACTED BY THE CONGRESS HERE ASSEMBLED THAT:

SECTION 1. The United States shall hereby regulate digital applications with foreign ownership or foreign-influenced data practices in order to protect national security, user privacy, and critical infrastructure.

A. A regulatory body known as the Digital Application Security Review Board (DASRB) shall be established under the U.S. Department of Commerce.

B. The DASRB shall consist of:

1. A representative from the Department of Commerce (Chair)
2. A representative from CISA
3. A representative from the FTC
4. A representative from the DOJ National Security Division
5. Two cybersecurity experts appointed by the Secretary of Commerce

C. The DASRB shall convene quarterly or upon emergency request by any two board members.

SECTION 2. AUTHORITY OF THE DASRB

A. The DASRB shall review digital applications available to U.S. users that exhibit foreign ownership, foreign data access, or foreign influence.

B. The DASRB shall classify applications into one of three categories:

1. Low Risk – No significant national security or data privacy vulnerabilities found.
2. Moderate Risk – Identifiable concerns requiring user transparency and enhanced monitoring.
3. High Risk – Clear or substantial threats to U.S. national security, government systems, or consumer data.

C. The DASRB shall have full investigatory power to:

1. Request documentation regarding data practices and foreign partnerships
2. Conduct audits and technical testing
3. Issue binding rulings on an app's risk classification

SECTION 3. HIGH-RISK APPLICATION RESTRICTIONS

A. Applications designated as High Risk by a two-thirds DASRB vote shall be removed from all U.S. digital marketplaces within 30 days of determination.

B. High-risk applications shall be blocked from operating on U.S. servers or networks.

C. Developers of removed applications may reapply for U.S. market access after 18 months, contingent upon demonstrated mitigation of identified threats.

SECTION 4. MODERATE-RISK APPLICATION REQUIREMENTS

A. Moderate-risk applications may remain available but must implement a government-issued warning displayed to users at download and at first launch:

"This application has been designated a moderate security risk by the United States Digital Application Security Review Board."

B. Moderate-risk applications must submit quarterly security and data-access reports to the DASRB.

C. Failure to comply with reporting requirements may result in elevation to high-risk status.

SECTION 5. DEFINITIONS

A. "Foreign Ownership" shall be defined as any direct or indirect ownership stake of 10% or more held by a foreign entity.

B. "Foreign Influence" shall be defined as the ability of a foreign government or corporation to access user data, alter algorithms, or influence platform governance.

C. "Digital Application" shall refer to any mobile, web-based, or software platform that collects or processes user data.

SECTION 6. ENFORCEMENT AND PENALTIES

A. The Federal Trade Commission and the Department of Commerce shall enforce this legislation.

B. Noncompliance shall result in:

1. Civil fines up to $50 million per violation,
2. Mandatory removal from U.S. digital marketplaces for repeated violations.

SECTION 7. FUNDING

A. Foreign Digital Services Compliance Fee:

Any application with foreign ownership or influence operating in the United States shall pay an annual compliance fee ranging from $50,000 to $500,000 determined by:

1. number of active U.S. users,
2. volume of data collected, and
3. level of foreign ownership or access.

B. Risk-Based Surcharges:

Applications designated as Moderate Risk shall pay an additional 5% surcharge on their annual compliance fee.

Applications under appeal for High-Risk classification shall pay a temporary 8% surcharge until the appeal is resolved.

C. Data Security Impact Fund:

All compliance fees, surcharges, and civil penalties shall be deposited into the Data Security

D. Impact Fund (DSIF), which shall exclusively support DASRB operations, cybersecurity audits, and threat analysis.

Annual Report:
The DASRB shall submit an annual public report to Congress summarizing collected funds, expenditures, and recommendations for future budget adjustments based on emerging digital-security needs.

SECTION 8. IMPLEMENTATION AND TIMELINE

A. The DASRB shall be operational in November 2026.
B. App risk assessments shall begin no later than 18 months after enactment.
C. All conflicting laws are hereby declared null and void.