

Protecting Biotechnology, Biomanufacturing, and Biological Data as Critical Infrastructure

Overview

The **Protecting Biotechnology and Biomanufacturing as Critical Infrastructure Act** would require the Cybersecurity and Infrastructure Security Agency (CISA) to protect biotechnology and biomanufacturing infrastructure by establishing coverage mechanisms for cross-sector infrastructure that do not neatly fall within the current Critical Infrastructure Sectors designations.

The **Protecting Biological Data as Critical Infrastructure Act** would require CISA to protect genetic and other sensitive biometric data to ensure coverage with the proper cybersecurity controls.

Background

The National Security Commission on Emerging Biotechnology (NSCEB) assessed in April 2025 that malicious actors will increasingly target the biotechnology sector's infrastructure and data. Already, they have carried out numerous cyberattacks on critical infrastructure in biotechnology, such as hospitals and agricultural facilities. Despite its growing significance to national security and the economy, the federal government does not adequately protect biotechnology infrastructure or sensitive biological data.

Biotechnology infrastructure cuts across several of the Critical Infrastructure Sectors designated by the Department of Homeland Security (DHS)'s CISA—including the health, agricultural, and industrial sectors—but is not explicitly recognized or comprehensively protected under current policy. Similarly, biological data, which are critical to research breakthroughs and often contain sensitive personal information, are not currently treated as a strategic national resource. Piecemeal federal government efforts are underway, but they do not fully address the changing landscape and major vulnerabilities remain.

DHS must treat biotechnology infrastructure and sensitive biological data as critical infrastructure for national security purposes by adopting the following amendments to the Homeland Security Act of 2002: Protecting Biotechnology and Biomanufacturing as Critical Infrastructure Act and Protecting Biological Data as Critical Infrastructure Act. Failure to do so leaves the United States vulnerable to biotechnology-related cyberattacks and exploitation by adversaries such as China.

Protecting Biotechnology and Biomanufacturing Act

HOUSE

Sponsor:
Rep. Ro Khanna
(D-CA-17)

Original Co-Sponsor:
Rep. Stephanie Bice
(R-OK-05)
Rep. Scott Peters
(D-CA-50)

SENATE

Original Co-Sponsor:
Sen. Maggie Hassan
(D-NH)

Original Co-Sponsor:
Sen. Todd Young
(R-IN)

Protecting Biological Data Act

HOUSE

Sponsor:
Rep. Ro Khanna
(D-CA-17)

Original Co-Sponsor:
Rep. Stephanie Bice
(R-OK-05)

Rep. Scott Peters
(D-CA-50)

SENATE

Original Co-Sponsor:
Sen. Todd Young
(R-IN)

Original Co-Sponsor:
Sen. Maggie Hassan
(D-NH)

Congress established the National Security Commission on Emerging Biotechnology (NSCEB) to assess biotechnology's national security impact and recommend strategies to ensure American leadership.

Read the NSCEB's April 2025 report at <https://www.biotech.senate.gov/final-report>

Legislative Details

Protecting Biotechnology and Biomanufacturing as Critical Infrastructure Act

This amendment directs the DHS to develop and execute a work plan within 45 days to ensure that biotechnology and biomanufacturing is protected as critical infrastructure, without adding a new sector. This work plan would include following components:

01 Stakeholder Identification

Identify key biotechnology infrastructure stakeholders.

02 Outreach Plan

Inform stakeholders of their inclusion in pre-existing critical infrastructure sectors, where applicable, and ensure they are in relevant consortia and Coordinating Councils.

03 Strategic Plan Update

Create an action plan to update the National Infrastructure Protection Plan (NIPP) by 2026, incorporating biotechnology sector equities and input.

04 Implementation Report

Submit a final report to Congress within one year of plan execution.

05 Follow-Up Evaluation

DHS would then conduct a follow-up evaluation within 2 years of updating the national strategic plan. DHS should note if there are critical biotechnology areas that remain unprotected.

Protecting Biological Data as Critical Infrastructure Act

This amendment directs CISA to conduct:

01 Classification of Genetic Data Systems

Designate systems handling genomic sequences and sensitive biometric data as critical infrastructure.

02 Collaboration

Mandate collaboration between CISA and biotechnology stakeholders to 1) create security protocols, including joint exercises and data-sharing mechanisms, and 2) synchronize security concerns across sectors, including biosecurity stakeholders.

03 CISA Staffing Increase

Increase personnel to manage new responsibilities related to securing genomic and biometric data.

04 Federal Training Programs

Implement training to address security challenges and ethical considerations tied to the protection of genetic and biometric data.

05 National Cybersecurity Strategy Integration

Incorporate genetic and biometric data security into the strategy to ensure responsiveness to evolving threats.

Interested in co-sponsoring this bill?

Please contact:

ideas@biotech.senate.gov

