United States Senate
COMMITTEE ON HEALTH, EDUCATION, LABOR, AND PENSIONS
WASHINGTON, DC 20510–6300

October 10, 2025

VIA ELECTRONIC TRANSMISSION

Chuck Robbins
Chair and Chief Executive Officer
Cisco
3098 Olsen Drive
San Jose, CA 95128

Dear Mr. Robbins,

Cybersecurity incidents pose a substantial threat to the American economy and the consumer. In 2024, the Federal Bureau of Investigation (FBI) estimated that cyber crimes resulted in over $16 billion in losses.[1] The Senate Committee on Health, Education, Labor, and Pensions (HELP) is conducting an investigation of these challenges and an assessment of initiatives underway to respond.

As cyber incidents continue to increase, it is essential that the public and private sector take steps to safeguard the information of millions of patients, students, and employees across America. These efforts also are critical to protect our national security interests.

The emergency directive issued by the Cybersecurity and Infrastructure Security Agency (CISA) on September 25 directed federal agencies to disconnect certain Cisco devices from federal systems in just one day in response to evidence of an active cybersecurity threat.[2] Recent reports indicate at least one federal agency has already been breached as a result of this vulnerability. This incident highlights the growing threat of sophisticated attacks from hostile actors, such as China, Russia, and Iran.

As the largest provider of network infrastructure in the world, Cisco holds a unique position in delivering tools not only to the federal government, but virtually all businesses. These tools

[1] *FBI Releases Annual Internet Crime Report*, Federal Bureau of Investigation (Apr. 23, 2025), https://www.fbi.gov/news/press-releases/fbi-releases-annual-internet-crime-report#:~:text=The%20Federal%20Bureau%20of%20Investigation's,increase%20in%20losses%20from%202023.
[2] *CISA Issues Emergency Directive Requiring Federal Agencies to Identify and Mitigate Cisco Zero-Day Vulnerabilities*, Cybersecurity and Infrastructure Security Agency (Sept. 25, 2025), https://www.cisa.gov/news-events/news/cisa-issues-emergency-directive-requiring-federal-agencies-identify-and-mitigate-cisco-zero-day.

connect consumers and businesses to care services, educational tools, and platforms businesses need to operate. Any vulnerability in Cisco's systems would jeopardize this access for millions of Americans.

As Cisco works with the federal government to patch any cybersecurity vulnerabilities, it must work with these stakeholders to ensure their systems are protected as well. To that end, I request answers to the following questions by **October 27, 2025**:

1. Has Cisco identified any specific threats to individual customers? If so, how is it communicating next steps or security patches?

2. How is Cisco proactively communicating with customers as Cisco identifies more about the potential threat?

3. Is Cisco currently recommending that individual customers disconnect or upgrade end-of-support devices as CISA directed federal agencies do on September 25?[3]

4. How is Cisco engaging with specific federal agencies, including the Departments of Education, Labor, and Health and Human Services to provide sector-specific services or assistance to impacted entities?

5. Estimates are that 45% of companies in the United States do not employ a Chief Information Security Officer (CISO).[4] How is Cisco working to communicate with individual customers, specifically health care providers, schools, and small businesses, to ensure they have current information about ways to address any cybersecurity vulnerabilities?

Sincerely,

Bill Cassidy, M.D.

Bill Cassidy, M.D.
Chairman
U.S. Senate Committee on Health,
Education, Labor, and Pensions

[3] *Id*.
[4] Daniel Hein, *45 Percent of Companies Don't Have a Chief Information Security Officer*, Solutions Review (Nov. 22, 2021), https://solutionsreview.com/security-information-event-management/45-percent-of-companies-dont-have-a-chief-information-security-officer/#:~:text=TechTarget%20defines%20a%20CISO%20as,effectively%20defend%20against%20cyber%20threats.