United States Senate

COMMITTEE ON HEALTH, EDUCATION, LABOR, AND PENSIONS

WASHINGTON, DC 20510–6300

October 27, 2025

VIA ELECTRONIC TRANSMISSION

François Locoh-Donou
President, Chief Executive Officer and Director
F5
801 5th Avenue
Seattle, WA 98104

Dear Mr. Locoh-Donou,

Cybersecurity incidents pose a substantial safety and financial threat to the American economy and the consumer. In 2024, organizations around the world faced an average of 1,876 cyber attacks per week, a record high.[1] Despite these growing threats, 35% of smaller organizations believe their cybersecurity infrastructure is not sufficient.[2] 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 sectors 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 October 15, the second directive in under a month, directed federal agencies to review the security of F5 hardware and software and identify any potential security vulnerabilities.[3] This was in response to, "A nation-state affiliated cyber threat actor [that] has compromised F5's systems and exfiltrated files."[4] Recent reports indicate that threat actors gained unauthorized

[1] Check Point Team, *A Closer Look at Q3 2024: 75% Surge in Cyber Attacks Worldwide*, Check Point (Oct. 18, 2024), https://blog.checkpoint.com/research/a-closer-look-at-q3-2024-75-surge-in-cyber-attacks-worldwide/.
[2] Kirsty Paine and Luna Rohland, *Why cyber resilience must be measured, not assumed*, World Economic Forum (Oct. 17, 2025), https://www.weforum.org/stories/2025/10/cyber-resilience-measuring-prevention/.
[3] *ED 26-01: Mitigate Vulnerabilities in F5 Devices*, Cybersecurity and Infrastructure Security Agency (Oct. 15, 2025), https://www.cisa.gov/news-events/directives/ed-26-01-mitigate-vulnerabilities-f5-devices.
[4] *Id*.

access to F5's systems as early as 2023.[5] The second potential breach of a critical network tool connecting public and private entities to essential tools highlights the significant threat of cybersecurity attacks, particularly from hostile actors, such as China, Russia, and Iran.

F5 is widely used by business, including by 85% of the Fortune 500 companies in the United States.[6] F5 has publicly stated that, "A highly sophisticated nation-state threat actor maintained long-term, persistent access to, and downloaded files from, certain F5 systems."[7] This significant breach raises questions about what customer data may have been exfiltrated, but also how to ensure F5 customers can reconnect to F5 systems.

As F5 works with the federal government to patch any cybersecurity vulnerabilities, it must work with customers to ensure their systems are protected as well. To that end, I request answers to the following questions by November 12, 2025:

1. Has F5 identified any specific threats to individual customers? If so, how is it communicating next steps or security patches?
    a. F5 has stated that, "We have not seen any new unauthorized activity, and we believe our containment efforts have been successful."[8] At what point did F5 detect unauthorized activity on its systems and what immediate steps did it take to mitigate this breach?
    b. How is F5 monitoring to ensure additional data from either F5's systems or customer information was not exfiltrated?

2. How is F5 proactively communicating with customers as F5 identifies more about the potential threat?

3. How is F5 working with customers to ensure that they can safely reconnect to F5's systems?

4. Is F5 currently recommending that individual customers follow CISA's October 15 emergency directive, including hardening and updating F5's BIO-IP hardware and software products?[9] If so, how is F5 working with customers to successfully apply these updates?

---

[5] Jake Bleiberg et al., *Hackers Had Been Lurking in Cyber Firm F5 Systems Since 2023*, Bloomberg (Oct. 18, 2025), https://www.bloomberg.com/news/articles/2025-10-18/hackers-had-been-lurking-in-cyber-firm-f5-systems-since-2023.
[6] *Customer Stories and Case Studies*, F5 (Oct. 18, 2025), https://www.f5.com/case-studies.
[7] *K000154696: F5 Security Incident*, F5 (Oct. 17, 2025), https://my.f5.com/manage/s/article/K000154696.
[8] *Id*.
[9] *See Note 3*.

5. How is F5 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?

6. Estimates are that 45% of companies in the United States do not employ a Chief Information Security Officer (CISO).[10] How is F5 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

---

[10] 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-havea-chief-information-securityofficer/#:~:text=TechTarget%20defines%20a%20CISO%20as,effectively%20defend%20against%20cyber%20threats.