

HHS Should Strengthen Oversight and Enhance Security Controls for the 988 Suicide and Crisis Lifeline

GAO-26-108836

September 2026

A report to congressional committees

Contact: Jennifer R. Franks, franksj@gao.gov

What GAO Found

The 988 Suicide and Crisis Lifeline (988 Lifeline) is managed on behalf of the Department of Health and Human Services (HHS) by a network administrator who oversees the day-to-day operations and ensures that the nearly 220 local crisis contact centers are compliant with the organization's cybersecurity requirements.

HHS partially implemented oversight activities related to cybersecurity for the 988 Lifeline. Specifically, HHS defined oversight roles and responsibilities to monitor cybersecurity control implementation. However, HHS did not include all key HHS-defined cybersecurity control areas in the 988 Lifeline cooperative agreement with its network administrator or for the network agreement between the administrator and crisis contact centers. In addition, HHS established processes to monitor security control implementation but did not always adhere to them.

Inclusion of Department of Health and Human Services (HHS)-defined Cybersecurity Control Areas in 988 Lifeline Agreements

Control area	Included in cooperative agreement?	Included in network agreement?
Mitigate known vulnerabilities	✓ Yes	✓
Email security	✗ No	✗
Multifactor authentication	✗	✓
Basic cybersecurity training	✗	✓
Strong encryption	✗	✓
Revoke credentials for departing workforce members	✓	✗
Basic incident planning and preparedness	✓	✓
Unique credentials	✗	✓
Separate user and privileged accounts	✗	✗
Vendor cybersecurity requirements	✗	✓

Source: GAO analysis of HHS data; GAO (all icons). | GAO-26-108836

While the network administrator and crisis contact centers fully implemented selected continuous monitoring controls, they have not consistently implemented other selected cybersecurity controls identified in guidance from the National Institute of Standards and Technology. Specifically, the network administrator has not implemented identity and access controls related to updated password guidance and partially implemented controls related to contingency plans. In addition, the crisis contacts centers have partially implemented incident response and contingency planning controls. Without the full implementation of these controls, the 988 Lifeline faces increased risk of cybersecurity incidents, which could result in prolonged service disruptions and potentially prevent individuals in crisis access to timely mental health support.

Why GAO Did This Study

HHS's Substance Abuse and Mental Health Services Administration launched the National Suicide Prevention Lifeline in 2005 to serve individuals in suicidal crisis or emotional distress. In 2022, it was renamed the 988 Suicide and Crisis Lifeline. The uninterrupted operation of the 988 Lifeline is critical to the health and safety of millions of Americans. These services were severely impacted in December 2022 by a cybersecurity attack that compromised critical 988 network infrastructure, leading to a nationwide service disruption lasting several hours. In addition, Congress passed the SUPPORT for Patients and Communities Reauthorization Act of 2025 that, among other things, includes a provision for GAO to report on the 988 Lifeline cybersecurity risks and vulnerabilities.

The objectives for this report were to determine (1) to what extent HHS has provided oversight of cybersecurity controls for the 988 Lifeline and (2) to what extent the 988 Lifeline network administrator and crisis contact centers have implemented selected cybersecurity controls.

To do so, GAO assessed cooperative and network agreements and related cybersecurity documentation and compared them to best practices and selected National Institute of Standards and Technology controls. GAO also interviewed HHS officials, the network administrator, and selected crisis contact centers.

What GAO Recommends

GAO is making 10 recommendations to HHS to update the cooperative and network agreements and to fully implement key cybersecurity controls. HHS concurred with the recommendations.