United States Government Accountability Office

Report to Congressional Committees

September 2026

CYBERSECURITY

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

GAO-26-108836

GAO Highlights

CYBERSECURITY

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.

Contents

Tables

Figures

Abbreviations

CPAG	Cybersecurity Program Audit Guide
CPG	Cybersecurity Performance Goals
DHS	Department of Homeland Security
FCC	Federal Communications Commission
HHS	Department of Health and Human Services
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
SAMHSA	Substance Abuse and Mental Health Services Administration
VA	Department of Veterans Affairs
VoIP	Voice over Internet Protocol

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

September 17, 2026

The Honorable Bill Cassidy, M.D.
Chair
The Honorable Bernard Sanders
Ranking Member
Committee on Health, Education, Labor, and Pensions
United States Senate

The Honorable Brett Guthrie
Chairman
The Honorable Frank Pallone, Jr.
Ranking Member
Committee on Energy and Commerce
House of Representatives

In 2023, one person in the United States died by suicide every 11 minutes on average, making it the second leading cause of death for those under the age of 45.[1] The Substance Abuse and Mental Health Services Administration (SAMHSA)[2]—an agency within the Department of Health and Human Services (HHS)—oversees the 988 Suicide and Crisis Lifeline (first called the National Suicide Prevention Lifeline), which, as of March 2026, includes around 218 crisis contact centers and has provided free, confidential 24/7 emotional support and crisis counseling nationwide since 2005.[3]

In its first year, the 988 Lifeline answered about 20,000 calls and by 2018 that number grew to 2.2 million calls annually. In January 2026 alone, the

[1]Centers for Disease Control and Prevention, "*Injuries and Violence Are Leading Causes of Death*," accessed May 19, 2026, https://wisqars.cdc.gov/ANIMATED-LEADING-CAUSES/. These data were the most current available at the time of our review.

[2]The Assistant Secretary for Mental Health and Substance Abuse is responsible to the Secretary of the Department of Health and Human Services for managing and directing SAMHSA. As of the date of this report, SAMHSA is being led by a Principal Deputy Assistant Secretary for Mental Health and Substance Abuse.

[3]The National Suicide Prevention Lifeline (1-800-273-8255 (TALK)) has operated since 2005, while the 3-digit dialing number for the 988 Lifeline launched in July 2022.

988 Lifeline handled 428,000 calls, reflecting rapid growth in demand for crisis support.[4]

In December 2022, the 988 Lifeline experienced a ransomware attack that resulted in a nationwide outage lasting several hours. This outage raised public concern about the cybersecurity of 988 Lifeline information systems and exposed a significant vulnerability in its operation.

Subsequently, Congress passed the SUPPORT for Patients and Communities Reauthorization Act of 2025, which requires, among other things, the timely reporting of cybersecurity incidents and vulnerabilities affecting the 988 Lifeline.[5] It also includes a provision for us to review the cybersecurity risks and vulnerabilities of the 988 Lifeline.

Our objectives 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.

We used our Cybersecurity Program Audit Guide (CPAG) to facilitate our methodology.[6] We selected control areas and control objectives from our guide based on their relevance to the availability of 988 Lifeline information and information systems. We then selected National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 revision 5 cybersecurity controls related to the following CPAG components:[7]

- asset and risk management,

[4]The number provided includes only the number of calls the 988 Lifeline handled and does not include the numbers for incoming chat and text.

[5]SUPPORT for Patients and Communities Reauthorization Act of 2025, Pub. L. No. 119-44, 139 Stat. 669 (Dec. 1, 2025).

[6]GAO, *Cybersecurity Program Audit Guide*, GAO-23-104705 (Washington, D.C.: Sept. 28, 2023).

[7]National Institute of Standards and Technology, *Security and Privacy Controls for Information Systems and Organizations*, Special Publication 800-53, revision 5 (Gaithersburg, MD: September 2020). We used NIST publication as guidance and a source of leading cybersecurity best practices to inform our assessment of cybersecurity controls and oversight processes. Because the network administrator and the crisis contact centers are nonfederal entities, NIST guidance did not constitute mandatory requirements.

- identity and access management,
- continuous monitoring and logging,
- incident response, and
- contingency planning and recovery.

To address the first objective, we evaluated SAMHSA's 988 Lifeline cooperative agreement and the network administrator's network agreement with crisis contact centers for inclusion of cybersecurity controls against HHS's public health sector-specific cybersecurity best practices.[8] We also assessed documentation of the oversight roles, responsibilities, and activities of SAMHSA and its network administrator against NIST cybersecurity controls related to the CPAG asset and risk management component.

To address the second objective, we selected a nongeneralizable sample of 10 crisis contact centers and either conducted interviews or received questionnaire responses from them. We selected crisis contact centers of varying size and those that used and did not use the network administrator's Unified Platform.[9] We evaluated the network administrator and selected crisis contact centers' implementation of selected NIST cybersecurity controls related to identity and access management, continuous monitoring and logging, incident response, and contingency planning and recovery.

We interviewed HHS and SAMHSA officials, the network administrator, selected crisis contact centers, as well as other federal agencies such as the Department of Homeland Security (DHS), Department of Veterans Affairs (VA), and the Federal Communications Commission (FCC). These interviews helped corroborate evidence and provided context for each objective. For further details on our objectives, scope, and methodology, please see appendix I.

We conducted this performance audit from December 2025 to September 2026 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to

[8]HHS, *Healthcare and Public Health Sector-Specific Cybersecurity Performance Goals, Strengthening the Cybersecurity of the Healthcare Sector and Keeping Patients Safe and Secure*, (Washington, D.C.: Jan. 24, 2024).

[9]As discussed later in the report, the Unified Platform is a network administrator owned and maintained system that crisis contact centers can use to connect counselors with contacts via voice, text, and chat.

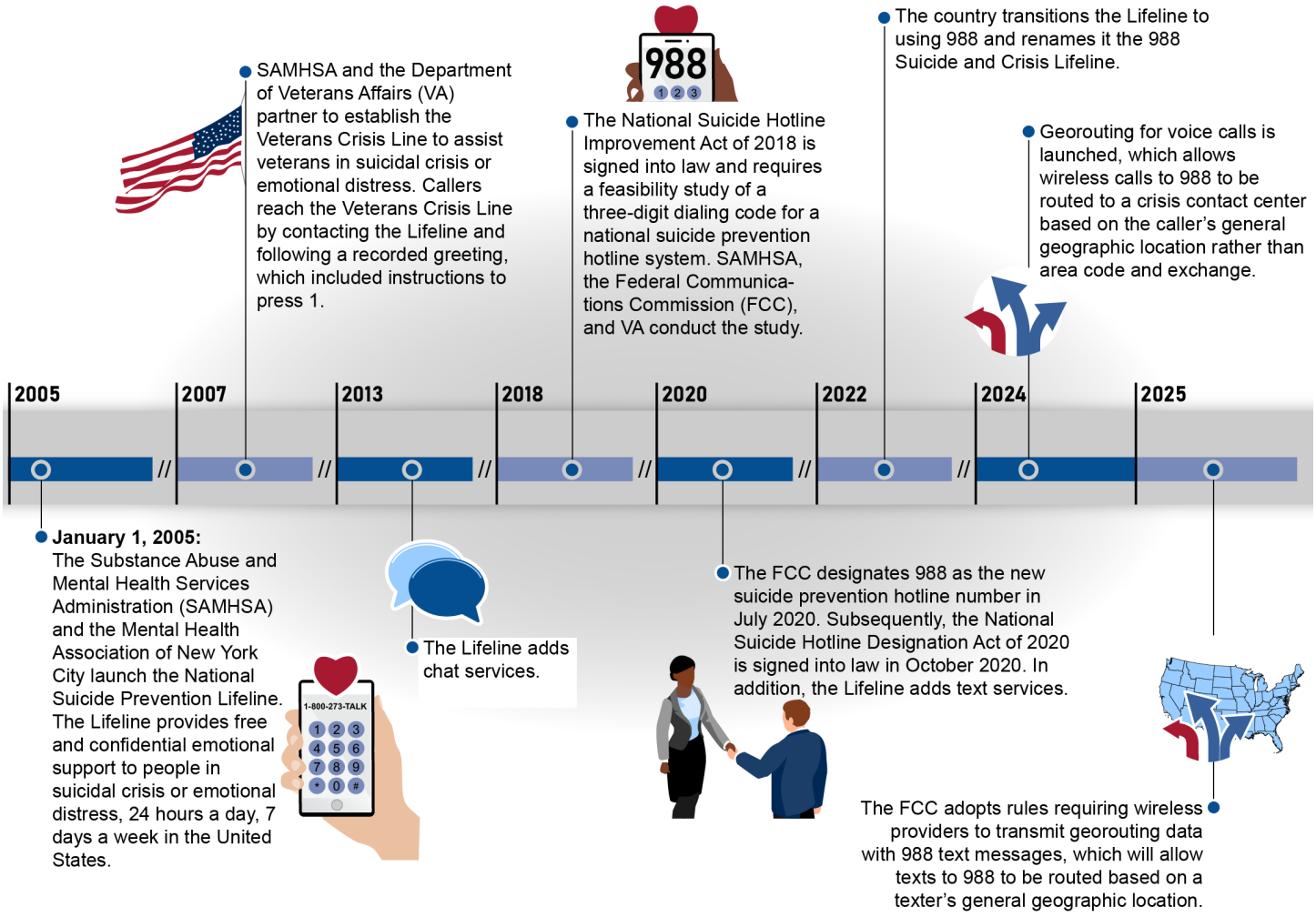
obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

The 988 Lifeline, managed by HHS's SAMHSA, is the nation's primary 24/7 service for confidential support to individuals in suicidal crisis or emotional distress via call, text, and chat across the U.S. and its territories. It operates through a distributed national network of around 218 local, state, and federally funded independent crisis contact centers staffed by trained crisis counselors. The 988 Lifeline originated in 2005 as the National Suicide Prevention Lifeline, established by SAMHSA and the Mental Health Association of New York City. In 2007, it integrated with VA's Veterans Crisis Line to provide access to veterans in suicidal crisis. In July 2022, following a rulemaking by FCC and enactment of the National Suicide Hotline Designation Act of 2020, 9-8-8 became the nationwide three-digit number for suicide prevention and mental health crisis counseling. Since transitioning to the 988 number, the 988 Lifeline has continued to grow, receiving more than 25 million contacts, 8 million of which took place in 2025 alone.[10] See figure 1 for the history of the 988 Lifeline.

[10]GAO's previously issued reports discuss 988 Lifeline and Veterans Crisis Line operations. See GAO, *Suicide Prevention: Capacity and Federal Assessment of the 988 Lifeline*, GAO-26-108114 (Washington, D.C.: July 1, 2026) and *Veterans Crisis Line: Actions Needed to Better Ensure Effectiveness of Communications with Veterans*, GAO-25-107182 (Washington, D.C.: June 2, 2025).

Figure 1: History of the 988 Lifeline



Sources: GAO analysis of HHS and other documents; GAO (all illustrations). | GAO-26-108836

988 Lifeline Operation and Infrastructure

The 988 Lifeline operates as a federated system of telecommunications, cloud, and crisis contact center platforms managed across federal, state, local, and private-sector partners. SAMHSA provides overall federal oversight and funding, managing program operations and overseeing the network administrator, who coordinates with state and local crisis contact

centers.[11] FCC regulates the 988 Lifeline dialing code and routing of 988 calls and texts by communications services providers. DHS's Cybersecurity and Infrastructure Security Agency supports national cybersecurity resilience and may provide threat information and technical assistance. VA operates the Veterans Crisis Line, which is integrated into the 988 Lifeline. In addition, private telecommunications service providers, Voice over Internet Protocol (VoIP) providers, and cloud providers, along with states and territories, support daily operations. This multi-entity structure creates shared responsibility for cybersecurity.

Five key entities are critical to the 988 Lifeline operation: the network administrator, network provider, communications service providers, crisis contact centers, and states/territories. Each of these organizations plays a specific role.

- Network administrator: Manages vendors, infrastructure, and day-to-day operations.
- Network provider: Receives and routes calls from telecommunication providers.
- Communications service providers: Connects callers to the 988 network.[12]
- Crisis contact centers: Provides counseling services to those in need.
- States/territories: Oversees and manages state/territory 988 response.

The 988 Lifeline uses georouting data to route wireless calls based on the caller's general location, as determined by their service provider.[13] This process identifies the caller's general geographic area without pinpointing the exact location of the cell site or handset associated with the call. Telecommunications and VoIP providers route all 988 calls to the Lifeline's centralized network, which then directs them to the nearest local

[11]SAMHSA does not provide 100 percent of the funding for all 988 services. Many states and territories provide funding to support 988 operations.

[12]FCC's 988 rules apply to telecommunications carriers, interconnected VoIP providers, and providers of one-way VoIP. See 47 CFR § 52.200.

[13]FCC adopted rules to implement georouting for 988 text messages, which will require nationwide providers to comply by April 16, 2027, and non-nationwide providers to comply by October 16, 2028. See *Implementation of the National Suicide Hotline Act of 2018*, WC Docket No. 18-336, Fourth Report and Order, 40 FCC Rcd 5629 (2025).

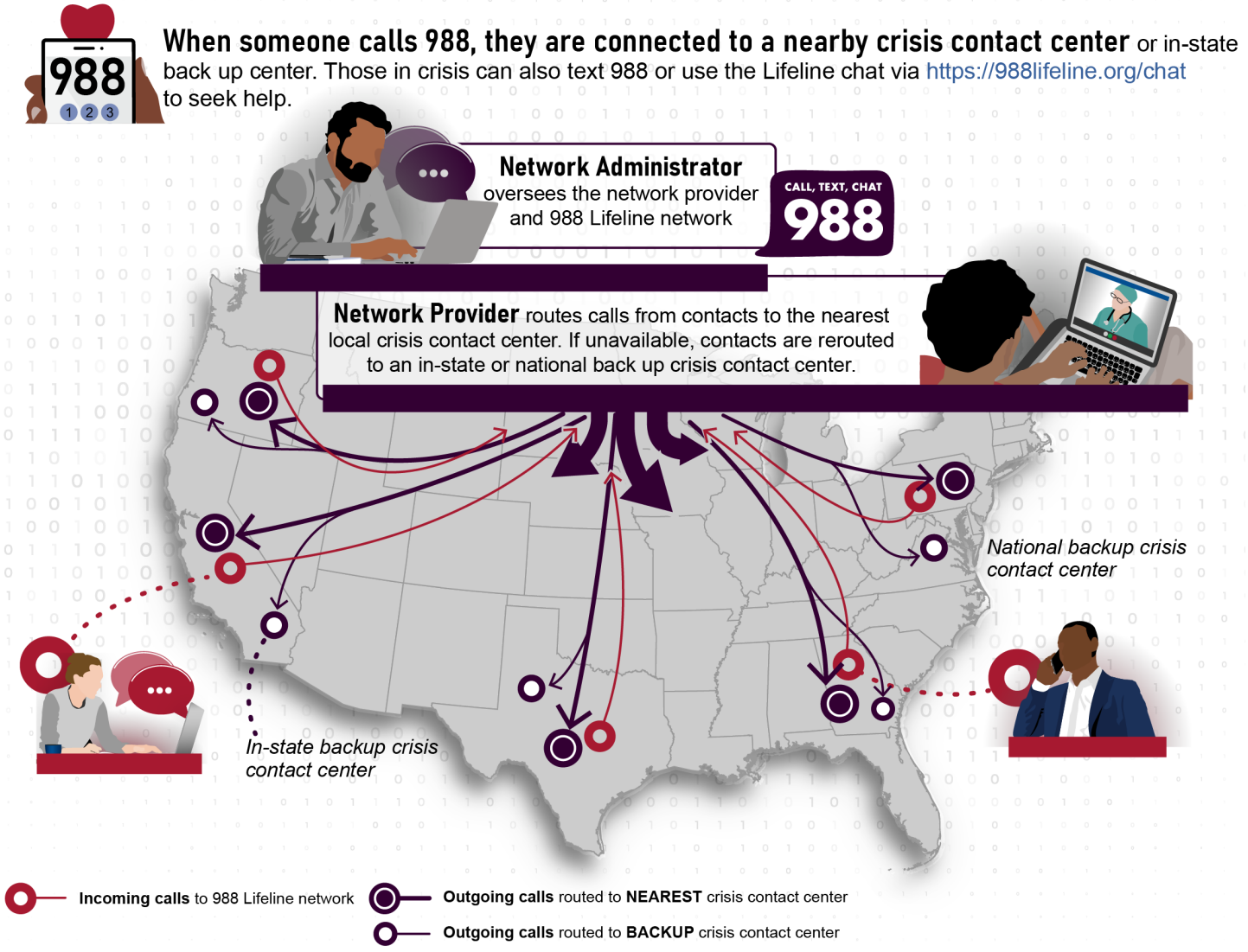
crisis contact center.[14] If the user's local crisis contact center is unavailable, contacts are rerouted to an in-state backup crisis contact center or national backup center (see figure 2).[15]

The 988 Lifeline routes texts to local crisis contact centers based on a contact's phone number and chat based on the zip code provided by the contact when a chat request is submitted. Both chat and text contacts are routed to statewide pools of crisis counselors from the individual's state who answer those texts and chats on the network administrator's Unified Platform.

[14]Calls are georouted using the 988 Lifeline telecommunications network based on georouting data. Chat contacts are routed based on the zip code information the contact provides when initiating the online 988 Lifeline chat service.

[15]Crisis contact centers handle 988 Lifeline contacts via call, text, and/or chat. Some also serve as national backup centers, receiving contacts when local centers or in-state backups are unavailable due to outages or limited counselor capacity.

Figure 2: Connecting 988 Lifeline Users with Crisis Contact Centers



Sources: GAO analysis of HHS and other documents; GAO (all illustrations); Substance Abuse and Mental Health Services Administration (988 logo). | GAO-26-108836

The individual crisis contact centers vary in terms of the size, contact volume, and available resources. While some crisis contact centers handle fewer than 1,000 voice contacts annually, others respond to over 100,000 contacts from voice, text, and chat during that same period. The number of personnel employed by and resources available to a given

crisis contact center are equally as diverse. For example, some crisis contact centers operate with less than 20 part-time or volunteer staff, while others employ hundreds of full-time employees with dedicated IT staff.

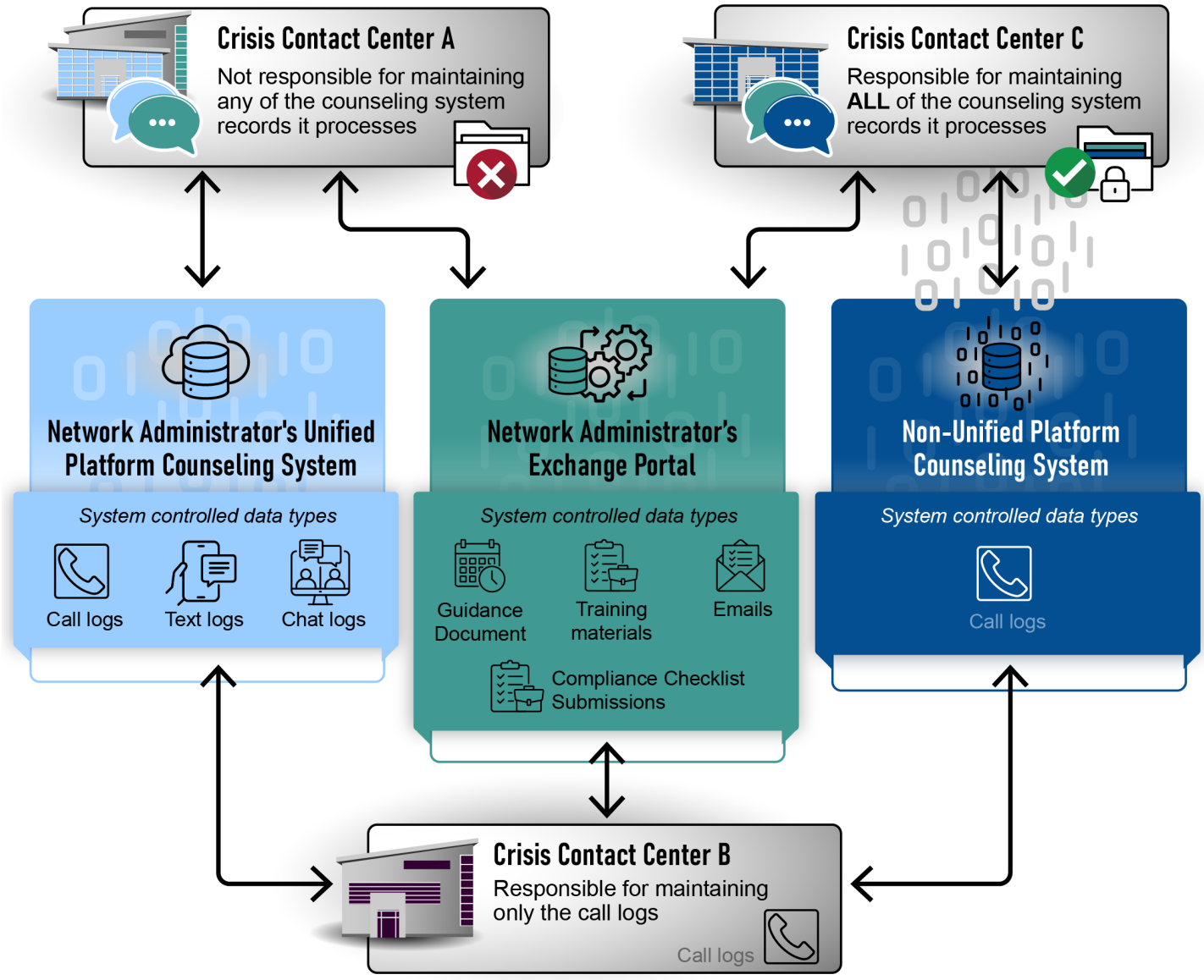
Crisis Contact Centers Rely on a Range of IT Systems to Deliver Services and Maintain Data

The 988 Lifeline is supported through a range of IT systems that provide counseling and administrative functions. The counselors deliver services through one or more IT systems that support call, text, and chat functions and which may interface with other emergency services, such as 911 and other hotlines. In addition to commercial tools, the 988 Lifeline network administrator provides crisis contact centers with free access to the Unified Platform, which is a cloud-based system that integrates call, text, and chat services for administrators and counselors. As of March 2026, 104 crisis contact centers use the Unified Platform for call, text, and/or chat. The other crisis contact centers use their own systems; however, all crisis contact centers are integrated with the 988 Lifeline network infrastructure, which manages and routes contacts across the 988 Lifeline network. The specific IT systems a crisis contact center uses depends on that center's individual needs and considerations. For example, some crisis contact centers that already receive 911 calls chose not to use the Unified Platform because they wanted to use a single IT system to respond to 911 and 988 calls.

While the network administrator sets baseline privacy and security standards for network contact centers through a network agreement, crisis contact centers are independent organizations that decide their own privacy and security policies. Moreover, while many crisis contact centers voluntarily delete their data after 30 days, others reported centers retaining them for over a year. A contact's name is not expressly recorded by crisis contact centers but may be documented in a voice, chat, or text log if volunteered by the contact during a counseling session.

Regardless of what IT systems crisis contact centers use to offer counseling services, they all use the network administrator's exchange portal. This portal is used to communicate with crisis contact centers and facilitate delivery of 988 Lifeline related documentation to the network administrator. In addition, the network administrator uses the exchange portal to provide crisis contact centers 988 Lifeline related guidance and training. See figure 3 for a description of the IT systems used by the 988 Lifeline crisis contact centers and the types of data processed by them.

Figure 3: 988 Lifeline Crisis Contact Centers IT Systems and Data



Crisis contact centers communicate with and exchange documentation with the network administrator using the exchange portal

Sources: GAO analysis of HHS and other documents; Cetacons/stock.adobe.com (icons); GAO (crisis center, check and X icon illustrations). | GAO-26-108836

988 Lifeline Funding and Oversight

The 988 Lifeline network administrator is funded through cooperative agreements between SAMHSA and the network administrator. Cooperative agreements are a type of federal assistance that promotes collaboration between the federal government and the recipient, providing SAMHSA with substantial involvement in the execution of the program. The fiscal year 2021 988 Lifeline network administrator cooperative agreement is a $115 million, 5-year instrument. The fiscal year 2026 cooperative agreement for the 988 Lifeline network administrator was awarded in May 2026, is valued at $255 million per year, and expected to continue through 2031.

Through the cooperative agreements, SAMHSA provides funding, policy direction, and oversight of the network administrator, while the network administrator is responsible for implementation of the 988 Lifeline. In this role, the network administrator manages the vendors, operations, infrastructure, and support for the crisis contact centers.

The network administrator is also responsible for managing crisis contact center access to the 988 Lifeline network. This is managed through an annual network agreement that establishes requirements for crisis contact center participation in the network, including cybersecurity standards.

Federal Requirements and Guidance Support Protecting the 988 Lifeline

NIST has published standards and guidelines that include guidance related to protecting the confidentiality, integrity, and availability of systems and data. These guidelines include NIST SP 800-53 revision 5, which provides information security related guidance for federal information systems in the form of a catalog of security and privacy controls, to include those related to access controls, continuous monitoring, incident response, and contingency planning.[16]

HHS Partially Implemented Oversight Activities of 988 Lifeline Cybersecurity

HHS partially implemented oversight activities of the cybersecurity for the 988 Lifeline. Specifically, HHS defined cybersecurity controls but did not establish them as requirements in the fiscal year 2026 cooperative agreement and the network administrator's current network agreement with crisis contact centers. It also defined oversight roles and responsibilities to monitor the implementation of cybersecurity controls. Further, HHS established processes to monitor cybersecurity control implementation but did not always adhere to them.

[16]National Institute of Standards and Technology, *Security and Privacy Controls for Information Systems and Organizations*, Special Publication 800-53, revision 5 (Gaithersburg, MD: September 2020).

HHS Defined but Did Not Establish All Cybersecurity Control Areas as Requirements in Agreements

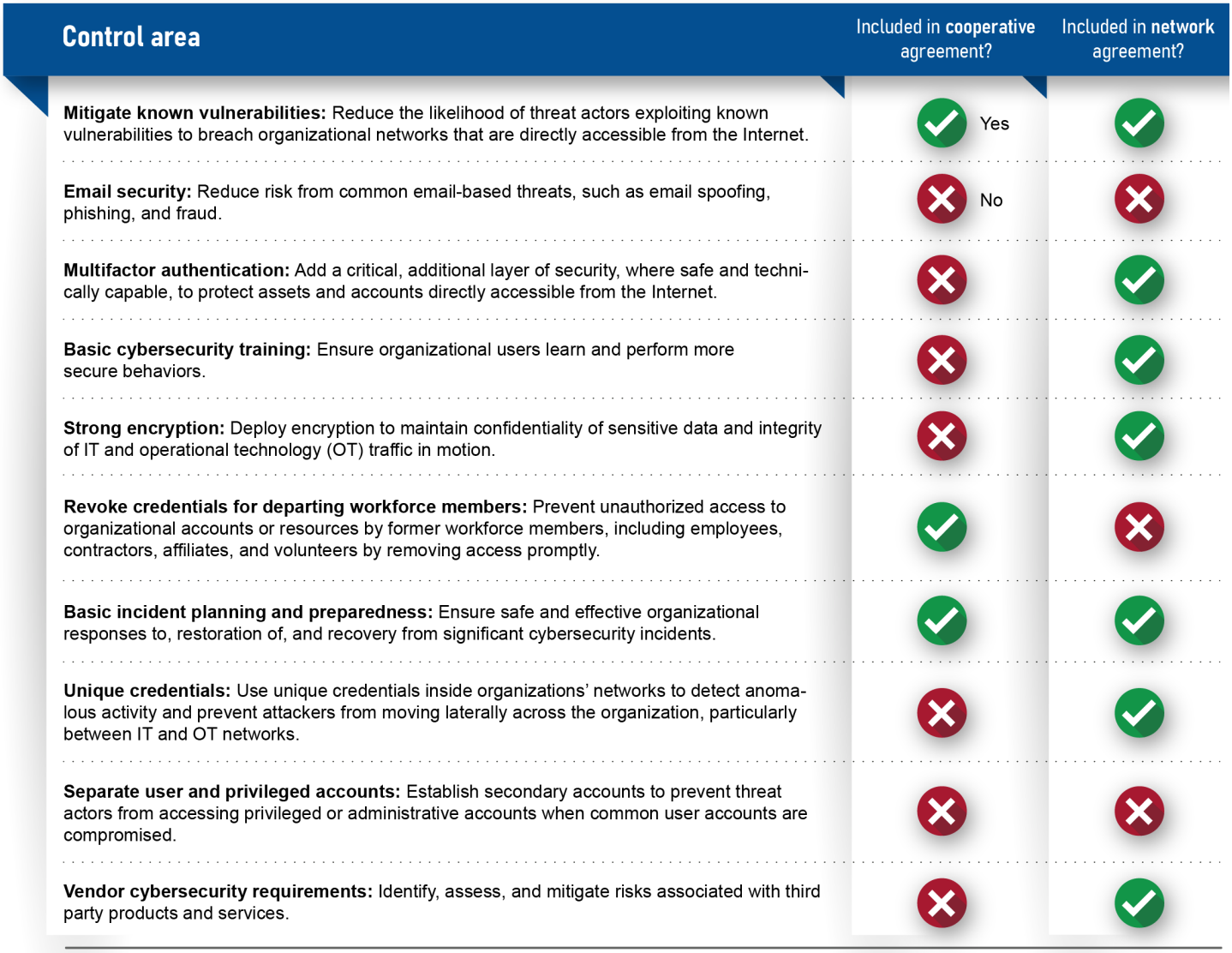
Cybersecurity controls describe the safeguards and protection capabilities appropriate for achieving an organization's particular security objective. NIST SP 800-53 revision 5 cybersecurity guidance states that organizations should require external entities to employ organization-defined controls.

HHS defined key cybersecurity control areas but did not consistently establish them as requirements in the fiscal year 2026 cooperative agreement and for the network administrator's network agreement with crisis contact centers. Specifically, HHS's Healthcare and Public Sector-Specific Cybersecurity Performance Goals (CPG) identifies 10 essential cybersecurity control areas that align with NIST SP 800-53 security controls.[17] These control areas help health care organizations establish baseline safeguards to address common vulnerabilities and strengthen cybersecurity.

However, HHS did not establish all these control areas as requirements in the fiscal year 2026 cooperative agreement and for the network administrator's current network agreement with the crisis contact centers. Specifically, the cooperative agreement included three of the 10 control areas, while the network agreement included seven (see figure 4).

[17]HHS, *Healthcare and Public Health Sector-Specific Cybersecurity Performance Goals, Strengthening the Cybersecurity of the Healthcare Sector and Keeping Patients Safe and Secure*, (Washington, D.C.: Jan. 24, 2024).

Figure 4: The Department of Health and Human Services (HHS) Inclusion of Cybersecurity Performance Goals Control Areas in 988 Lifeline Agreements



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

SAMHSA officials stated that the agency does not have the authority to include all cybersecurity control areas as requirements for nonfederal systems, but that the network administrator can embed them in the network agreement as requirements for crisis contact center participation.

Officials said that they plan to include these cybersecurity controls in future iterations of the cooperative agreement and the administrator's network agreement with crisis contact centers. SAMHSA officials added that the fiscal year 2026 cooperative agreement with the network administrator does not include all the CPGs since the Notice of Funding Opportunity had already been posted and was awarded in May 2026. Officials noted that enforcing cybersecurity requirements for crisis contact centers is a challenge because they participate through a voluntary network agreement with the network administrator. As a result, SAMHSA stated that it can only recommend, rather than require, that crisis contact centers implement the controls, and that responsibility for implementing cybersecurity safeguards rests with the individual crisis contact centers. Nevertheless, including these CPGs in these agreements will help establish clear baseline expectations, promote cybersecurity consistency across participating entities, and strengthen oversight of key safeguards needed to protect system availability and sensitive data.

Without all relevant cybersecurity control areas in the cooperative agreement and the administrator's network agreements with crisis contact centers, HHS will have limited assurance that entities supporting the 988 Lifeline consistently implement appropriate safeguards to reduce the risk of cybersecurity-related disruptions that could affect system availability and individuals' ability to access life-saving resources.

HHS Defined Oversight Roles and Responsibilities in Agreements

Clearly defined roles and responsibilities help organizations in monitoring compliance with requirements. NIST SP 800-53 revision 5 guidance states that organizations should define and document roles and oversight responsibilities for external entities.

HHS defined oversight roles and responsibilities in the 988 Lifeline agreements. As previously mentioned, the cooperative agreement specifies SAMHSA's oversight roles and responsibilities, including assigning project officers to monitor implementation. These officers conducted regular coordination meetings, reviewed and approved project phases before work began or resumed, and reviewed and approved key policies, including the network agreement. They were also responsible for monitoring the performance and progress of call, text, and chat network systems.

In addition, the 988 Lifeline network agreement defined the network administrator's oversight responsibilities for the crisis contact centers. For example, the network agreement stated that the administrator must develop a compliance work plan for each crisis contact center to identify

risks or potential noncompliance. In addition, the administrator was required to conduct comprehensive reviews of every crisis contact centers' deliverables by auditing documentation, such as policies and procedures. By defining oversight roles and responsibilities, HHS has greater assurance that entities understand their cybersecurity responsibilities and expectations.

HHS and the Network Administrator Developed Oversight Processes but Did Not Always Adhere to Them

Organizations monitor external service providers to ensure compliance and reduce risk. NIST SP 800-53 revision 5 guidance states that organizations should employ organization-defined processes, methods, and techniques to monitor whether external entities meet control requirements.

HHS developed two processes to monitor the network administrator's compliance with cybersecurity controls defined in the cooperative agreement. In addition, the network administrator developed two processes to monitor the crisis contact centers' compliance with security controls defined in the network agreement; however, it did not always adhere to them. Specifically,

- HHS biweekly meetings: HHS established bi-weekly technology update meetings with the network administrator to discuss 988 Lifeline cybersecurity issues, including cybersecurity legislation, user authentication, and guidance for crisis contact centers' implementation of security controls.
- Incident reporting procedures: HHS participated in an alerts and communications standard operating procedure (created in June 2022 and last updated in January 2026), that outlines related reporting requirements and required actions the network administrator is to take during and after outages and incidents that affect 988 Lifeline operations.
- Cybersecurity survey: The network administrator requested that crisis contact centers complete an optional cybersecurity survey to assess implementation of controls. As of March 2026, 146 of the 218 crisis contact centers completed the survey. Network administrator officials stated that they plan to require completion of the survey in the next network agreement revision.
- Compliance checklist process: The network administrator required crisis contact centers to submit documentation—such as a business continuity analysis, cybersecurity policy, and incident response policy—to demonstrate compliance with network agreement requirements by November 1, 2024.

However, enforcement of the checklist documentation was inconsistent. Of the 12 crisis contact centers' compliance checklists we received from HHS, none submitted the three security related documents to the administrator before the deadline and seven submitted them after the deadline. The remaining five crisis contact centers have not yet submitted all required documents, as of March 2026.

SAMHSA officials stated that participation in the network agreement is voluntary for crisis contact centers. Officials added that the network agreement has limited enforcement mechanisms because HHS's primary recourse for noncompliance, such as failing to submit required compliance documentation, is to remove a crisis contact center from the 988 Lifeline network. According to SAMHSA, crisis contact centers are independent organizations and responsibility for implementing and managing cybersecurity safeguards primarily rests with the individual crisis contact centers. Until HHS and the network administrator ensure submissions of the compliance checklist process and related documentation, the department will have limited assurance that entities supporting the 988 Lifeline consistently established, documented, and implemented security controls to protect the availability of systems and sensitive mental health information from unauthorized access.

Network Administrator and Sampled Crisis Contact Centers Have Partially Implemented Selected Cybersecurity Controls

The network administrator and sampled crisis contact centers have partially implemented selected NIST cybersecurity controls aligned with four CPAG control components. Specifically, the:

- network administrator fully implemented one and not implemented one selected identity and access management controls,
- network administrator and crisis contact centers fully implemented one selected continuous monitoring and logging control,
- network administrator fully implemented four selected incident response controls and the crisis contact centers partially implemented four selected incident response controls, and
- network administrator fully implemented two and partially implemented one selected contingency planning and recovery controls and the crisis contact centers fully implemented one and partially implemented two contingency planning and recovery controls.

See table 1 below for a summary of the entities' implementation of the selected CPAG components and NIST controls.

Table 1: Network Administrator and Sampled Crisis Contact Centers Efforts to Implement Selected Cybersecurity Program Audit Guide (CPAG) Components and National Institute of Standards and Technology (NIST) Controls for the 988 Lifeline

CPAG components and NIST controls	Network administrator	Crisis contact centers
Identity and access management		
Require multifactor authentication	●	n/a
Implement updated password guidance	○	n/a
Continuous monitoring and logging		
Develop monitoring systems	●	●
Incident response		
Develop an incident response policy	●	◑
Develop an incident response plan	●	◑
Conduct incident response training and testing	●	◑
Establish incident reporting procedures and report incidents	●	◑
Contingency planning and recovery		
Develop a contingency planning policy	●	◑
Develop contingency plans	◑	●
Conduct contingency plan training and testing	●	◑

Legend: ●=Fully implemented ◑=Partially implemented ○=Not implemented

Source: GAO analysis of agency documentation. | GAO-26-108836

The Administrator Partially Implemented Identity and Access Management Controls

Identity and access management, to include assessing identification and authentication mechanisms, involves and detecting inappropriate access to computer resources (data, equipment, and facilities). According to NIST SP 800-53 revision 5, identification and authentication controls help prevent unauthorized users or processes from accessing systems.

- Require multifactor authentication: Multifactor authentication strengthens security by requiring users to verify their identity using more than just a username and password.[18] The Office of Management and Budget also calls for agencies to (1) implement application layer phishing-resistant multifactor authentication for all agency users and (2) offer application layer phishing-resistant multifactor authentication to all public users.[19]

[18]NIST SP 800-53 guidance states that users should provide two or more authentication factors from different categories: something they know (such as a password or PIN), something they have (such as a smart card or security key), or something they are (such as a fingerprint or facial recognition).

[19]Office of Management and Budget, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*, M-22-09 (Washington, D.C.: Jan. 26, 2022).

- Implement updated password guidance: NIST Special Publication 800-63B-4 recommends that agencies eliminate routine password rotation and complex character requirements, and instead encouraged the use of longer, more secure passphrases.[20]

The network administrator fully implemented one and did not implement one of the selected identity and access management controls for systems supporting the 988 Lifeline (see table 2).[21] A discussion of each control follows the table.

Table 2: Network Administrator Efforts to Implement Selected Identity and Access Management Related National Institute of Standards and Technology (NIST) Controls for Systems Supporting the 988 Lifeline

NIST controls	Network administrator
Require multifactor authentication	●
Implement updated password guidance	○

Legend: ●=Fully implemented ◑=Partially implemented ○=Not implemented

Source: GAO analysis of agency documentation. | GAO-26-108836

Require multifactor authentication: The network administrator has implemented multifactor authentication for systems that interface with crisis contact centers. Specifically, it required two-factor authentication for both the Unified Platform and the network administrator's exchange portal.

Implement updated password guidance: The network administrator has not updated its password guidance and continues to require routine password changes and the use of composition rules (e.g., special characters) for both the Unified Platform and exchange portal. SAMHSA officials acknowledged that the network administrator is responsible for updating the Unified Platform and exchange portal password requirements that all crisis contact centers adhere to when logging in to those two systems.

[20]National Institute of Standards and Technology, *Digital Identity Guidelines: Authentication and Authenticator Management*, Special Publication 800-63B-4, (Gaithersburg, MD: July 2025).

[21]We did not evaluate crisis contact centers' implementation of identity and access management related controls due to the fact the network administrator has sole responsibility for implementing multifactor authentication and password policies for the Unified Platform and exchange portal.

SAMHSA officials stated that the current cooperative agreement did not require NIST compliance and that NIST password guidance constitutes a recommendation rather than a requirement. SAMHSA officials added that it does not have the authority to mandate a NIST-specific password for nonfederal systems. The network administrator stated that it did not mandate its implementation because password requirements are under crisis contact center-level responsibility and the centers' password policies cover "reasonable cybersecurity." The network administrator is enforcing multifactor authentication and a 12-character minimum password—exceeding the 8-character minimum recommended by NIST when multifactor authentication is enforced. SAMHSA noted that the network administrator is currently assessing whether to cease mandatory rotation per new guidance. Although SAMHSA stated that it does not have the authority to mandate compliance with NIST guidance for nonfederal systems, NIST Special Publication 800-63B-4 represents widely accepted cybersecurity leading practices used to strengthen identity and access management. By not aligning with the current guidance, HHS reduces assurance that participating entities are implementing consistent and effective password management which could lead to compromised passwords and unauthorized access to sensitive mental health information.[22]

The Administrator and Sampled Crisis Contact Centers Fully Implemented Continuous Monitoring

Continuous monitoring provides ongoing awareness of cybersecurity vulnerabilities and threats to an organization's systems and network. According to NIST SP 800-53 revision 5, it is achieved through monitoring capabilities that detect, alert, and analyze security events for anomalies or unusual activity. Monitoring systems detect attacks, identify compromises, and flag unauthorized connections and improper system use using defined techniques and methods.

The network administrator and crisis contact centers fully implemented the selected control for continuous monitoring (see table 3). A discussion of the control follows the table.

[22]Password rotation increases the risk from phishing attacks by exploiting user fatigue and mimicking password reset emails. Phishing attacks are increasing in frequency and are associated with several incidents reported by crisis contact centers we interviewed.

Table 3: Network Administrator and Crisis Contact Centers Efforts to Implement Selected Continuous Monitoring Related National Institute of Standards and Technology (NIST) Control for Systems Supporting the 988 Lifeline

NIST control	Network administrator	Crisis contact centers
Develop monitoring systems	●	●

Legend: ●=Fully implemented ◑=Partially implemented ○=Not implemented

Source: GAO analysis of agency documentation. | GAO-26-108836

Develop monitoring systems: The network administrator reported monitoring the system to detect attacks and potential indicators of compromise. Specifically, it implemented monitoring capabilities, including real-time alerts through Software-as-a-Service platform vendors.[23] Crisis contact center officials stated they either relied on these service providers or implemented their own monitoring tools. In addition, all nine crisis contact centers that provided feedback reported having alerting mechanisms to identify service disruptions or cybersecurity incidents and stated they actively monitor systems and networks to analyze detected events and anomalies.[24] The administrator also holds weekly meetings with vendors to discuss anomalies.

In addition, the network administrator implemented an identity access management platform to support functions such as multifactor authentication, single sign-on, role-based access control, and least privilege. The administrator further stated it has a 988 Lifeline technical and operations team that monitors the network 24/7. By implementing continuous monitoring, the network administrator and crisis contact centers strengthen their ability to detect unauthorized access across the 988 Lifeline and enhance overall system security.

The Administrator Fully Implemented and Sampled Crisis Contact Centers Partially Implemented Incident Response

Incident response involves organizations developing and implementing actions to take when a cybersecurity incident occurs. According to NIST SP 800-53 revision 5, an incident is an adverse event or occurrence that actually or imminently jeopardizes, without lawful authority, the confidentiality, integrity, or availability of information or an information system.

[23]Software-as-a-Service is a cloud-based software model that allows users to access applications through an internet-connected device's interface such as a web browser.

[24]One of the 10 sampled/selected crisis contact centers did not respond to this question.

- Develop an incident response policy: This policy governs an organization's incident response program and should include, among other things, the policy's purpose, scope, roles, responsibilities, and management commitment.
- Develop an incident response plan: This plan documents a predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyberattack against an organization's systems.
- Conduct incident response training and testing: Regular training and testing ensure personnel have sufficient knowledge, skills, and abilities to complete their assigned incident response and recovery responsibilities.
- Establish incident reporting procedures and report incidents: These procedures and reporting ensure organizations can understand, manage, and mitigate the impact of an incident in a timely manner.

In addition, the SUPPORT for Patients and Communities Reauthorization Act of 2025 and network agreement require that crisis contact centers report incidents and vulnerabilities to the network administrator.

The network administrator fully implemented four selected incident response controls. The crisis contact centers partially implemented four selected incident response controls (see table 4). A discussion of each control follows the table.

Table 4: Network Administrator and Crisis Contact Centers Efforts to Implement Selected Incident Response Related National Institute of Standards and Technology (NIST) Controls for Systems Supporting the 988 Lifeline

NIST controls	Network administrator	Crisis contact centers
Develop an incident response policy	●	◑
Develop an incident response plan	●	◑
Conduct incident response training and testing	●	◑
Establish incident reporting procedures and report incidents	●	◑

Legend: ●=Fully implemented ◑=Partially implemented ○=Not implemented

Source: GAO analysis of agency documentation. | GAO-26-108836

Develop an incident response policy: The network administrator established an incident management policy that defines its purpose, scope, responsibilities, and management commitment. The policy was signed and approved within the past 12 months and references a supporting procedure document—the incident response plan. In addition,

four of the 10 crisis contact centers reported having an incident response policy. However, one reported it did not and five did not comment.

Develop an incident response plan: The network administrator had a current incident response plan that provided a structured approach for handling cybersecurity incidents. The plan outlined key components including the purpose, scope, audience, and governance, incident response team, incident response process, the reporting process, and security incident metrics. In addition, nine of the 10 crisis contact centers reported having an incident response plan. However, one reported it did not.

Conduct incident response training and testing: In 2025, the network administrator conducted a cybersecurity tabletop exercise to test its incident response plan and standard operating procedures. In January 2026, it hosted a cybersecurity incident reporting training session focused on workflow and incident tracking, and it required personnel to complete annual security awareness training. However, only three of the 10 crisis contact centers we interviewed reported conducting incident response training and testing.

Establish incident reporting procedures and report incidents: The network administrator maintained a cybersecurity incident and vulnerability reporting capability through a module accessible within the network administrator's exchange portal. Reported data was routed through defined incident and vulnerability reporting workflows. The crisis contact centers we interviewed reported experiencing five incidents since December 2022. However, one crisis contact center we interviewed stated it was not aware it had to report incidents to SAMHSA and three of 10 crisis contact centers indicated that it was not clear what constitutes an incident and/or vulnerability that should be reported.[25] For example, one of the crisis contact centers we interviewed stated it would be helpful to establish incident and vulnerability thresholds and another stated it would be helpful if it was provided examples of each.

Some of the crisis contact center officials stated that they lacked experience developing incident response policies, plans, and training and testing and that these controls were not always implemented because they were not required by the current network agreement. SAMHSA

[25]Cybersecurity vulnerabilities and incidents are a common occurrence and vary significantly in severity and impact.

officials stated that the network administrator will provide training, guidance, and support as needed. Based on the current network agreement, crisis contact centers attested to maintaining cybersecurity policies and plans during the most recent compliance review cycle. SAMHSA officials added that enforcement at this time could only be removing the crisis contact centers from the 988 Lifeline, which they stated would weaken the 988 Lifeline and impact state crisis services. In addition, during our review, SAMHSA and the network administrator developed and provided recently issued cybersecurity reporting guidance to clarify what constitutes an incident or vulnerability. This guidance included examples and described the thresholds for distinguishing between vulnerabilities and incidents. Since the guidance was recently issued, we did not follow-up with SAMHSA and crisis contact centers to evaluate the impact of the new guidance on crisis contact center incident reporting. As a result, we are not making a recommendation related to the incident reporting procedures and report incidents control.

Nevertheless, until the crisis contact centers fully implement all of the remaining selected controls related to incident response, they face increased risk their incident response capabilities will be insufficient to effectively detect, contain, eradicate, and recover from cybersecurity incidents, leaving organizations vulnerable to further damages, extended downtime, and uncontained threats.

The Administrator and Sampled Crisis Contact Centers Partially Implemented Contingency Planning

According to NIST SP 800-53 revision 5, contingency planning is essential for achieving continuity of operations for organizational mission and business functions. Contingency planning addresses system restoration and implementation of alternative mission or business processes when systems are compromised or breached.

- Develop a contingency planning policy: This policy outlines the organization's contingency planning requirements and ensures that personnel fully understands how to carry it out.
- Develop contingency plans: These plans are essential to ensure that, in the event of unexpected disruptions, critical operations can continue or be quickly restored, while safeguarding information resources. A disaster recovery plan should be included in the contingency plan and address disruptions affecting the primary facility. The disaster recovery plan should identify alternate processing and storage locations and define the procedures for transferring, restoring, and resuming system operations and backup information at an alternate off-site location. In addition, the cooperative agreement requires the network administrator to develop a business continuity

analysis and a comprehensive disaster recovery plan that covers all system components and network partners.

- Conduct contingency plan training and testing: Regular training and testing are necessary to ensure that personnel know their roles and to provide management with confidence that recovery plans will work as intended.

The network administrator fully implemented two and partially implemented one selected contingency planning and recovery control. The crisis contact centers fully implemented one and partially implemented two selected contingency planning and recovery controls (see table 5). A discussion of each control follows the table.

Table 5: Network Administrator and Crisis Contact Centers Efforts to Implement Selected Contingency Planning Related National Institute of Standards and Technology (NIST) Controls for Systems Supporting the 988 Lifeline

NIST controls	Network administrator	Crisis contact centers
Develop a contingency planning policy	●	◑
Develop contingency plans	◑	●
Conduct contingency plan training and testing	●	◑

Legend: ●=Fully implemented ◑=Partially implemented ○=Not implemented

Source: GAO analysis of agency documentation. | GAO-26-108836

Develop a contingency planning policy: The network administrator developed a contingency planning policy that identifies the purpose, scope, roles, responsibilities, and procedures. The policy has been updated twice, most recently within the past 12 months. In addition, three of the 10 crisis contact centers reported having a contingency planning policy. However, two reported they did not and five did not comment.

Develop contingency plans: The network administrator has developed and implemented a contingency plan that incorporates elements identified in NIST SP 800-53 guidance. The plan included a business continuity analysis, which was updated twice in 2025, and serves as the organization-wide contingency plan, while also directing designated department staff to develop contingency plans tailored to their specific department's needs. In addition, the network administrator has taken steps to promote the implementation of contingency planning by its vendors, including establishing contract requirements for vendors to develop and maintain disaster recovery plans. Although the network administrator stated it has not reviewed the vendor's contingency plans, it has conducted vendor risk assessments that included evaluating availability and contingency planning. According to SAMHSA officials,

vendors do not provide this information due to its sensitive nature. As an alternative, the network administrator reviews service organization controls 2 reports when available.[26]

However, the network administrator did not include key elements of a disaster recovery plan in the contingency plan. Specifically, the contingency plan did not address facility-level information system planning or define off-site recovery procedures. All 10 crisis contact centers we interviewed reported developing a contingency plan.

Conduct contingency plan training and testing: The network administrator conducted contingency plan training and testing in November 2025 through a table-top exercise. In addition, it has taken steps to promote vendor testing by requiring, through contract language, that vendors periodically test their disaster recovery plans. In addition, the network administrator has performed vendor risk assessments that included evaluating availability and contingency planning. However, only five of the 10 crisis contact centers we interviewed reported conducting contingency plan training and testing.

The crisis contact centers did not always include the two controls related to contingency planning policy training and testing because they were not required by the current network agreement. SAMHSA officials stated that the network administrator plans to address these gaps through webinar-based contingency planning training for all crisis contact centers, including a demonstration of a tabletop exercise. SAMHSA also noted it will work with the network administrator to support crisis contact centers in developing contingency planning policies. SAMHSA officials added that enforcement at this time could only be removing the crisis contact centers from the 988 Lifeline.

Until the network administrator and crisis contact centers fully implement the three controls related to contingency planning, there is an increased risk contingency plans will not function as intended, preventing timely restoration of system services and potentially leading to significant operational disruptions, financial losses, and reputational damage.

Conclusions

Effective oversight of cybersecurity programs and control implementation by HHS is critical to maintaining the availability of 988 Lifeline services

[26]A service organization controls 2 report is issued by an independent auditor who evaluates an organization's implementation of controls impacting the security, availability, processing integrity, confidentiality, and privacy of the systems and data they maintain.

and to protecting the sensitive data those systems process and store. SAMHSA and the network administrator partially implemented selected NIST controls related to asset and risk management. For example, they did not consistently include HHS's essential cybersecurity control areas in the cooperative agreement or the network administrator's network agreements with crisis contact centers and they did not fully implement monitoring processes. Without clear cybersecurity requirements and reliable compliance monitoring, SAMHSA and the network administrator do not have the guidance and information necessary to ensure effective oversight of the 988 Lifeline.

Gaps in the implementation of controls by both the network administrator and crisis contact centers increase the risk of prolonged disruption to the 988 Lifeline services and limits access to critical crisis support for individuals experiencing suicidal distress. For example, shortcomings in identity and access management controls could lead to unauthorized access to sensitive mental health information. Also, gaps in incident response controls increase the risk that crisis contact centers will fail to detect, contain, eradicate, and recover from cybersecurity incidents. Furthermore, contingency planning capabilities that have not been fully implemented may fail during an actual disruption, increasing the risk of extended outages to 988 Lifeline services.

Recommendations for Executive Action

We are making the following 10 recommendations to HHS:

The Secretary of HHS should direct the Assistant Secretary for Mental Health and Substance Abuse to incorporate the seven missing cybersecurity control areas from HHS's CPG in the 988 Lifeline cooperative agreement. (Recommendation 1)

The Secretary of HHS should direct the Assistant Secretary for Mental Health and Substance Abuse to work with the network administrator to incorporate the three missing cybersecurity control areas from HHS's CPG in the 988 Lifeline network administrator's network agreement with the crisis contact centers. (Recommendation 2)

The Secretary of HHS should direct the Assistant Secretary for Mental Health and Substance Abuse to work with the network administrator to ensure full implementation of the 988 Lifeline network agreement compliance checklist process. (Recommendation 3)

The Secretary of HHS should direct the Assistant Secretary for Mental Health and Substance Abuse to work with the network administrator to implement the current NIST password guidance. (Recommendation 4)

The Secretary of HHS should direct the Assistant Secretary for Mental Health and Substance Abuse to work with the network administrator to establish requirements for crisis contact centers' development of incident response planning policies and monitor the implementation of such policies. (Recommendation 5)

The Secretary of HHS should direct the Assistant Secretary for Mental Health and Substance Abuse to work with the network administrator to establish requirements for crisis contact centers' development of incident response plans and monitor the implementation of such plans. (Recommendation 6)

The Secretary of HHS should direct the Assistant Secretary for Mental Health and Substance Abuse to work with the network administrator to establish requirements for crisis contact centers' development of incident response training and testing and monitor implementation of such training and testing. (Recommendation 7)

The Secretary of HHS should direct the Assistant Secretary for Mental Health and Substance Abuse to work with the network administrator to establish requirements for crisis contact centers' development of contingency planning policies and monitor the implementation of such policies. (Recommendation 8)

The Secretary of HHS should direct the Assistant Secretary for Mental Health and Substance Abuse to ensure that the network administrator includes key elements of a disaster recovery plan in the contingency plan. (Recommendation 9)

The Secretary of HHS should direct the Assistant Secretary for Mental Health and Substance Abuse to work with the network administrator to establish requirements for crisis contact centers' development of contingency plan training and testing and monitor the implementation of such training and testing. (Recommendation 10)

Agency Comments and Our Evaluation

We provided a draft of this report to HHS, VA, FCC, and DHS for their review and comments. HHS, the agency to which we made recommendations, provided written comments which are reprinted in appendix II. HHS concurred with all 10 of our recommendations and

stated that it recognized the importance of making the 988 Suicide and Crisis Lifeline more secure. HHS noted that its authority to mandate specific cybersecurity controls may be constrained by the organizational independence of the states, territories, and local entities that operate the crisis contact centers. As such, the implementation of best practices and standards would depend on the cooperation of these independent entities. HHS also provided technical comments, which we have incorporated as appropriate.

In HHS's technical comments, it stated that figure 4 should be revised by changing the red X to a green check mark for the “separate user and privileged accounts” CPG control area under "included in network agreement." HHS stated that the current network agreement addresses this control area through the Center Operations Policy, which states, “named accounts shall be provided for all access to the 988 Lifeline administrator systems and account credentials should not be shared between center staff.”

We disagree that the cited Center Operations Policy meets the intent of the CPG control area for “separate user and privileged accounts.” The Center Operations Policy requires individual user accounts and prohibits credential sharing. In contrast, the CPG control area requires users with privileged or administrative accounts to use separate standard user accounts for routine activities, consistent with the principle of least privilege.

Of the three agencies to which we did not make recommendations, VA provided written comments, reprinted in appendix III, in which it concurred with our findings and recommendations to HHS. FCC provided technical comments, which we have incorporated as appropriate. In addition, DHS did not have any comments on the report.

We are sending copies of this report to the appropriate congressional committees, the Secretary of Health and Human Services, the Inspector General of Health and Human Services, the Secretary of Homeland Security, the Secretary of Veterans Affairs, the Chaiman of the Federal Communications Commission, and other interested parties. In addition, the report is available at no charge on the GAO website at https://www.gao.gov.

If you or your staff should have any questions about this report, please contact me at franksj@gao.gov. Contact points for our Offices of Congressional Relations and Media Relations may be found on the last

page of this report. GAO staff who made key contributions to this report are listed in appendix IV.

//SIGNED//

Jennifer R. Franks
Acting Chief Technology Officer
Director, Center for Enhanced Cybersecurity
Information Technology and Cybersecurity

Appendix I: Objectives, Scope, and Methodology

Our objectives were to determine (1) to what extent the Department of Health and Human Services (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.

We used our Cybersecurity Program Audit Guide (CPAG) to facilitate our methodology.[1] We selected control areas and control objectives from our guide based on their relevance to the availability of 988 Lifeline information and information systems. We then selected related National Institute of Standards and Technology (NIST) Special Publication 800-53 revision 5 cybersecurity controls.[2] NIST guidance includes multiple related controls and enhancements within each control area. Our review examined selected NIST controls but did not evaluate all related controls and control enhancements. We evaluated the Substance Abuse and Mental Health Services Administration (SAMHSA), the network administrator, and selected crisis contact centers' implementation of selected NIST cybersecurity controls related to the following CPAG components:

- asset and risk management: policies and procedures related to external parties;
- identity and access management: multifactor authentication and password policies;
- continuous monitoring and logging: monitoring systems;
- incident response: policies, plans, training, testing, and reporting; and
- contingency planning and recovery: policies, plans, training and testing.

To address both objectives, we gained an understanding of the operating environment by analyzing network diagrams, 988 Lifeline agreements, and cybersecurity policy. We also interviewed SAMHSA and network administrator officials to identify SAMHSA, the network administrator, and crisis contact centers' cybersecurity responsibilities.

[1]GAO, *Cybersecurity Program Audit Guide*, GAO-23-104705 (Washington, D.C.: Sept. 28, 2023).

[2]We used the NIST publication as guidance and a source of leading cybersecurity best practices to inform our assessment of cybersecurity controls and oversight processes. Because the network administrator and the crisis contact centers are nonfederal entities, the NIST publication alone did not constitute mandatory requirements.

To address the first objective, we evaluated SAMHSA's cooperative agreement and the network administrator's network agreement security control requirements against NIST Special Publication 800-53 revision 5 control guidance. Specifically, we assessed whether the agreements included organization-defined controls from HHS's Public Health Sector-Specific Cybersecurity Performance Goals.[3] We also evaluated the cooperative and network agreements and related policies inclusion of cybersecurity oversight roles and responsibilities against NIST guidance. In addition, we evaluated evidence of SAMHSA and the network administrator's implementation of cybersecurity oversight activities against NIST cybersecurity controls related to the CPAG asset and risk management component. Specifically, we reviewed three documented examples of IT and cybersecurity meetings between SAMHSA and the network administrator. Also, we assessed a 988 Lifeline outage reporting procedure for network administrator roles and responsibilities. We further examined results of the network administrator's cybersecurity survey of the 988 Lifeline crisis contact centers. Moreover, we analyzed 12 network agreement compliance checklists from randomly selected crisis contact centers. We analyzed the checklists for the submission and approval of three cybersecurity-related documents.

To address the second objective, we selected a nongeneralizable sample of 10 out of 218 crisis contact centers and either conducted interviews or received questionnaire responses from them. We took steps to select crisis contact centers of varying size and those that used and did not use the network administrator's Unified Platform. To determine this selection, we requested a list of all the crisis contact centers that included contact volume for calendar year 2025. We then sorted the crisis contact centers based on their use of the Unified Platform and call volume.

We took steps in sorting the list to protect against selection bias and then began our selection at the beginning of the list working down. We selected 60 crisis contact centers in total. We then emailed the selected crisis contact centers as necessary in order to get the desired number of participants. To increase response opportunities and maintain flexibility given the short evidence collection period, we allowed selected crisis contact centers to participate by virtual interview or written answers to our semi-structured questions. Participation was voluntary. Ten crisis contact centers participated either by interviews or provided written responses to

[3]HHS, *Healthcare and Public Health Sector-Specific Cybersecurity Performance Goals, Strengthening the Cybersecurity of the Healthcare Sector and Keeping Patients Safe and Secure*, (Washington, D.C.: Jan. 24, 2024).

our semi-structured questions. Specifically, we interviewed seven crisis contact centers and three provided written responses. The characteristics of the 10 selected crisis contact centers that responded to our initial outreach to 60 centers could differ from centers as a whole; differing on both descriptive characteristics and/or volition to respond.

The 10 crisis contact centers that participated were in various categories of size in terms of contacts serviced and staffing levels. In addition, one crisis contact center we selected utilized only the Unified Platform for voice, text, and/or chat, six used a combination of the Unified Platform and their own IT system for voice, text, and/or chat and three exclusively used their own IT system(s) for voice, text, and/or chat.[4]

To address identity and access management, we evaluated the network administrator's implementation of multifactor authentication and password policies for two key information systems, the Unified Platform and exchange portal, compared to NIST guidance. Specifically, we reviewed authentication settings and policies to determine whether users with access to the Unified Platform and exchange portal were required to use multifactor authentication and rotate passwords on a routine basis. In addition, we reviewed password policies associated with both IT systems.

To address continuous monitoring and logging, we evaluated the system monitoring tools the network administrator and crisis contact centers used to detect system activity compared to NIST guidance. Specifically, we requested evidence showing the monitoring capabilities such as log activity, unauthorized connections, and anomalous activity conducted by the network administrator and interviewed crisis contact centers to determine what tools were implemented. In addition, we verified that system collects data to detect attack indicators in real-time and deploys alerts for identified threats.

To address incident response, we evaluated the network administrator's and crisis contact centers' implementation of incident response policies, plans, testing, training, and reporting compared to NIST guidance. Specifically, we interviewed crisis contact centers to determine whether they have developed incident response policies and plans, engaged in incident response training and testing, and the extent to which they have

[4]Not all crisis contact centers provided voice, text, and chat counseling services.

experienced and reported cybersecurity incidents to the network administrator and SAMHSA.

To address contingency planning and recovery, we evaluated the network administrator's and crisis contact centers' implementation of contingency planning policies, plans, testing, and training compared to NIST guidance. Specifically, we interviewed crisis contact centers to determine whether they have developed contingency planning policies and plans and engaged in contingency planning training and testing.

We interviewed HHS and SAMHSA officials, the network administrator, selected crisis contact centers, as well as other federal agencies such as the Department of Homeland Security, Department of Veterans Affairs, and the Federal Communications Commission. These interviews helped corroborate evidence and provided context for each objective.

We conducted this performance audit from December 2025 to September 2026 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: Comments from the Department of Health and Human Services

DEPARTMENT OF HEALTH & HUMAN SERVICES
OFFICE OF THE SECRETARY

Assistant Secretary for Legislation
Washington, DC 20201

July 20, 2026

Jennfer R. Franks
Director
Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street NW
Washington, DC 20548

Dear Ms. Franks:

Attached are comments on the U.S. Government Accountability Office's (GAO) report entitled, **"Cybersecurity: HHS Should Strengthen Oversight and Enhance Security Controls for the 988 Suicide and Crisis Lifeline"** (GAO-26-108836).

The Department appreciates the opportunity to review this report prior to publication.

Sincerely,

Gary Andres
Assistant Secretary for Legislation

Attachment

GENERAL COMMENTS FROM THE DEPARTMENT OF HEALTH & HUMAN SERVICES ON THE U.S. GOVERNMENT ACCOUNTABILITY OFFICE'S DRAFT REPORT TITLED - CYBERSECURITY: HHS SHOULD STRENGTHEN OVERSIGHT AND ENHANCE SECURITY CONTROLS FOR THE 988 SUICIDE CRISIS LIFELINE (GAO-26-108836)

The Department of Health and Human Services (HHS) appreciates the opportunity to review and comment on the Government Accountability Office (GAO) draft report.

SAMHSA Overarching Comment

The Substance Abuse and Mental Health Services Administration (SAMHSA) has undertaken numerous initiatives to ensure robust security controls are in place for the 988 Suicide and Crisis Lifeline. These efforts reflect SAMHSA's dedication to protecting the integrity and confidentiality of this critical service. SAMHSA supports the recommendations provided by the Government Accountability Office (GAO), recognizing the importance of making the 988 Suicide and Crisis Lifeline even more secure. The agency shares the GAO's commitment to continuous improvement, aiming to enhance security measures and safeguard this invaluable resource. However, its authority to mandate specific cybersecurity controls may be constrained by the organizational independence of states, territories, and local entities that operate these centers. As a result, SAMHSA can recommend best practices and standards, but the implementation of such requirements often depends on the cooperation and governance structures of these independent organizations.

Appendix III: Comments from the Department of Veterans Affairs

DEPARTMENT OF VETERANS AFFAIRS
Office of Congressional and Legislative Affairs
Washington, DC 20420

July 10, 2026

Ms. Jennifer R. Franks
Director, Center for Enhanced Security
Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Ms. Franks:

The Department of Veterans Affairs (VA) has reviewed the Government Accountability Office (GAO) draft report: ***CYBERSECURITY: HHS Should Strengthen Oversight and Enhance Security Controls for the 988 Suicide and Crisis Lifeline*** (GAO-26-108836).

VA concurs with GAO's findings and recommendations to the Department of Health and Human Services (HHS). VA affirms its commitment to the resilience and continuity of crisis services for Veterans and to the sustained coordination with Federal partners in support of a secure and uninterrupted 988 Lifeline network.

VA operates the Veterans Crisis Line (VCL) under the Department's established Federal cybersecurity framework, which is governed by Federal Information Security Modernization Act requirements, VA Handbook 6500 *Risk Management Framework for VA Information Systems VA Information Security Program*, and the risk management framework defined in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37. As a Federal information system, VCL adheres to mandatory NIST SP 800-53 Revision 5 control requirements, which are the same standards GAO recommends HHS extend to its non-Federal network participants. Specifically:

- **Identity and Access Management:** VCL systems enforce phishing-resistant multifactor authentication and current NIST SP 800-63B password guidance, consistent with Office of Management and Budget M-22-09 Federal Zero Trust Strategy.
- **Continuous Monitoring:** VCL operates under VA's enterprise continuous diagnostics and monitoring program, with 24/7 security operations coverage by VA's Security Operations Center.
- **Incident Response:** VA maintains a tested, enterprise incident response program that includes VCL-specific procedures, trained personnel, and defined reporting thresholds aligned with Federal incident reporting requirements.
- **Contingency Planning:** VA maintains and annually tests VCL contingency and disaster recovery plans, which include off-site recovery procedures consistent

with NIST SP 800-53, Contingency Planning (CP) 2, CP-7, and CP-9 requirements.

The controls in place limit VA's exposure to the cybersecurity gaps identified in GAO's report, which primarily affect non-Federal crisis contact centers operating under voluntary network agreements with the Substance Abuse and Mental Health Services Administration (SAMHSA).

VA recognizes that any disruption to the 988 Lifeline network directly impacts Veterans' access to life-saving crisis support. The December 2022 ransomware attack, which caused a Nationwide 988 service outage lasting several hours, is a stark reminder that cybersecurity failures in the network are not abstract risks; they are critical risks for the Veterans VA serves.

For this reason, VA strongly supports GAO's recommendations and HHS's efforts to close the identified gaps in cybersecurity oversight, agreement requirements, and control implementation across the 988 networks. Strengthening incident response, contingency planning, and access management across all participating crisis contact centers will reduce the risk of future disruptions that could prevent Veterans from reaching VCL in critical moments.

VA is committed to sustained coordination with SAMHSA, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency, and other Federal partners to advance the shared goal of a resilient, secure, and continuously available crisis services network. VA will continue to make VCL and Office of Information and Technology officials available to support GAO, HHS, and other oversight and implementation activities related to the 988 Lifeline as appropriate and stands ready to share applicable practices and lessons learned from VA's own cybersecurity program where they may benefit the broader network.

Sincerely,

Donald Bergin
Assistant Secretary for
Congressional and Legislative Affairs

Appendix IV: GAO Contact and Staff Acknowledgments

GAO Contact

Jennifer R. Franks, franksj@gao.gov

Staff Acknowledgments

In addition to the contact named above, West Coile, Saar Dagani, Tammi Kalugdan, Duc Ngo (Assistant Directors), Brandon Sanders (Analyst-in-Charge), Christopher Businsky, Rebecca Eyler, Shane Homick, Sherwyn Hunte, Anh-Thi Le, Koushik Nalluru, and Walter Vance made key contributions to this report.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. You can also subscribe to GAO's email updates to receive notification of newly posted products.

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, https://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on X, LinkedIn, Instagram, and YouTube.
Subscribe to our Email Updates. Listen to our Podcasts.
Visit GAO on the web at https://www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: https://www.gao.gov/about/what-gao-does/fraudnet

Automated answering system: (800) 424-5454

Media Relations

Sarah Kaczmarek, Managing Director, Media@gao.gov

Congressional Relations

David A. Powner, Acting Managing Director, CongRel@gao.gov

General Inquiries

https://www.gao.gov/about/contact-us