UC BERKELEY

CENTER FOR LONG-TERM CYBERSECURITY

CLTC WHITE PAPER SERIES

A Path to Long-Term Cyber Resilience for Under-Resourced Organizations

MICHAEL RAZEEQ

CLTC WHITE PAPER SERIES

A Path to Long-Term Cyber Resilience for Under-Resourced Organizations

MICHAEL RAZEEQ

August 2025

CLTC
Center for Long-Term Cybersecurity
UC Berkeley

Contents

Executive Summary

State, local, tribal, and territorial governments ("SLTTs"), small- and medium-sized businesses ("SMBs"), and nonprofits across the United States are often targeted in cyber attacks by nation-states, criminals, and other actors. From a cybersecurity perspective, many of these organizations are under-resourced,[1] even though they may manage critical infrastructure and deliver essential services. They lack the financial resources and human expertise that the federal government and global corporations have to adequately secure infrastructure and deliver services. The societal impacts of cyber attacks on under-resourced organizations — even apart from their financial costs — are significant. Such attacks force schools to close, disrupting education and childcare;[2] they delay vital court proceedings;[3] they threaten the availability of municipal drinking water;[4] and they limit healthcare providers' access to medical records and endanger patients' lives.[5]

Under-resourced organizations can take actions to become more resilient to cybersecurity incidents.[6] One way they can build cyber resilience is to outsource some of their cybersecurity tasks to information technology ("IT") managed service providers ("MSPs"), managed security service providers ("MSSPs"), and other types of IT and security service providers. This report examines the ways in which MSPs, MSSPs, and similar service providers (collectively referred to in this report as "ITSSPs") can improve the long-term cyber resilience of under-resourced organizations. Part 1 provides a description of the research approach taken to complete this report. Part 2 describes the current state of cybersecurity for under-resourced organizations, focusing on those that operate water and wastewater systems. Next, Part 3 examines the roles of different types of ITSSPs and how ITSSPs serve their clients. Part 4 offers recommendations to position more ITSSPs to be able to support under-

1 This report uses the term "under-resourced organizations" to refer to the collection of state, local, tribal, and territorial governments (SLTTs), nonprofits, and small- and medium-size businesses (SMBs) that lack the resources to adequately address their cybersecurity needs.

2 Kara Arundel, "School Ransomware Attacks Are on the Rise. What Can Districts Do?," *K-12 Dive*, October 28, 2024, https://www.k12dive.com/news/school-ransomware-attacks-cybersecurity-funding/730333/.

3 Matt Kapko, "Dallas Courts Still Closed 2 Weeks Post-Ransomware Attack," *Cybersecurity Dive*, May 17, 2023, https://www.cybersecuritydive.com/news/dallas-courts-closed-ransomware/650523/.

4 Thao Nguyen, "EPA Urges Water Utilities to Protect Nation's Drinking Water amid Heightened Cyberattacks," *USA Today*, May 21, 2024, https://www.usatoday.com/story/news/nation/2024/05/21/epa-cyberattacks-community-water-systems/73778706007/.

5 Sean Lyngaas, "'It's Putting Patients' Lives in Danger': Nurses Say Ransomware Attack Is Stressing Hospital Operations," *CNN*, May 29, 2024, https://www.cnn.com/2024/05/29/tech/ransomware-attacks-hospitals-patients-danger.

6 As used in this report, "resilience" refers to the ability of an organization to continue to deliver its intended outcomes despite a cybersecurity incident.

resourced organizations. Lastly, Part 5 concludes with a call to action to carry out these recommendations.

This report recommends demand-side actions for under-resourced organizations and the communities that work with them to improve the awareness and procurement of ITSSP services, such as: (1) expanding the availability of cybersecurity awareness and training; (2) establishing a matching service to help under-resourced organizations find ITSSPs; (3) developing purchasing pools or collaboratives as a way to increase the market power of under-resourced organizations to procure ITSSP services; and (4) working with investors and donors to prioritize cybersecurity as part of their investments or funding. This report also recommends supply-side actions to increase the availability and ability of ITSSPs to support under-resourced organizations, such as: (1) increasing community engagement and outreach by ITSSPs; (2) expanding pro bono and discounted services by ITSSPs for under-resourced organizations; and (3) enhancing information sharing and collaboration among ITSSPs. While the recommendations in this report are intended to be applicable across sectors, this report focuses on the water and wastewater systems ("WWS") sector, because water is a key dependency for many other critical infrastructure and key resource sectors (such as healthcare and public health, emergency services, food and agriculture, and chemicals), and it includes government, nonprofit, and for-profit entities.

Research Approach

This report examined existing research relevant to the topic and utilized semi-structured interviews conducted between December 2024 and April 2025 with individuals from 15 ITSSPs, as well as two state government officials with experience working with IT and information security service providers. Of the ITSSPs interviewed, two explicitly refer to themselves as MSPs and one as an MSSP. The remaining organizations refer to themselves as IT or cybersecurity firms, consultancies, or platforms that provide a combination of services offered by traditional MSPs and MSSPs.

Five of the ITSSPs interviewed have over 100 staff members, while the rest have fewer. Four of the ITSSPs offer IT and information security services as one of several lines of business and generate over $1 billion in annual revenue. Seven of the ITSSPs (all with fewer than 100 staff members) describe themselves as mission-driven organizations that primarily serve other mission-driven organizations and nonprofits. The other ITSSPs interviewed serve a broad range of clients, including SLTTs, nonprofits, and for-profit entities. Although a small number of organizations were interviewed, the information security expertise of the interviewees — and the range of organizations they represent — provided sufficient perspectives to analyze the issues addressed in this report and provide recommendations.[7]

7 Interviewees were existing professional contacts of the researcher or were referred to the researcher by professional contacts. Interviewees also provided suggestions for additional people to interview for this report. The interviews ranged between 30 minutes and one hour each and were primarily conducted via video call. To facilitate an open discussion, interviewees were informed that their organizations would not be identified individually in the report. For that reason, interviews were not recorded.

Under-Resourced Organizations and the Challenges They Face

1. AN OVERVIEW OF UNDER-RESOURCED ORGANIZATIONS IN THE U.S.

As organizations' cyber attack surfaces have continued to expand,[8] it has become increasingly more complicated and expensive to secure those attack surfaces. It has also become increasingly difficult for organizations, in particular under-resourced organizations, to hire staff with sufficient training to defend their networks and systems.[9] Different categorizations of organizations that lack sufficient resources to meet their cybersecurity needs are referred to as "below the cyber poverty line," "under-resourced organizations,"[10] "high-risk communities,"[11] and other designations. This report uses the term "under-resourced organizations" to refer to the collections of SLTTs, SMBs, and nonprofits that lack adequate cybersecurity resources.

Under-resourced organizations may operate critical infrastructure and provide essential services in communities across the U.S. They represent a significant portion of all U.S. organizations and employ a significant number of people. As of 2022, there were over 90,000 local governments in the U.S., including counties, townships, and municipal and special purpose entities.[12] In 2023, there were over 33 million small businesses in the U.S., which collectively employed 46% of the private-sector workforce.[13] And, in 2022, there were nearly 2 million nonprofits operating in the U.S., employing over 10% of all private-sector employees.[14] Those SLTTs, SMBs, and nonprofits range from churches to hospitals to water treatment plants.

8 An "attack surface" encompasses all of the vulnerabilities and points of entry an unauthorized actor could exploit to access an information system or network.

9 John Morris et al., "Cybersecurity as a Service," arXiv, Feb. 22, 2024, 4, https://arxiv.org/abs/2402.13965.

10 Michael Razeeq, "Civilian Cyber Corps: A Model Law for States" (Washington, DC: New America, Sept. 26, 2024), 7, https://www.newamerica.org/future-security/reports/civilian-cyber-corps-a-model-law-for-states/background/.

11 "High-Risk Communities," Cybersecurity & Infrastructure Security Agency (hereinafter, "CISA"), accessed June 15, 2025, https://www.cisa.gov/audiences/high-risk-communities.

12 Federal Reserve Bank of St. Louis, by Amy Smaldone and Mark L.J. Wright, "A Breakdown by Number and Type," *The Regional Economist* (St. Louis, Missouri, 2024), https://www.stlouisfed.org/publications/regional-economist/2024/march/local-governments-us-number-type#:~:text=The%20total%20number%20of%20U.S.,)%20and%20Ohio%20(3%2C939).

13 "The State of Small Business Now," U.S. Chamber of Commerce, April 10, 2023, https://www.uschamber.com/small-business/state-of-small-business-now.

14 "How many nonprofits are there in the US?," USAFacts, November 16, 2023, https://usafacts.org/articles/how-many-nonprofits-are-there-in-the-us/.

2. A FOCUS ON WATER AND WASTEWATER SYSTEM CYBERSECURITY

The water and wastewater sector ("WWS") is one of the most important critical infrastructure and key resource sectors identified by CISA. Over 260 million Americans receive drinking water from utilities owned by local governments, and around 50 million Americans receive drinking water from private utilities owned by a mix of for-profit companies and nonprofits.[15] In the U.S., there are around 170,000 water and wastewater systems, including around 153,000 public water systems and 16,500 treatment facilities.[16] Yet, much of the water and wastewater infrastructure is aging and in need of repair or replacement. According to the U.S. Government Accountability Office, small drinking water systems in the U.S. will require $74.4 billion over the next 20 years for improvements to meet safe drinking water standards.[17]

Water and wastewater infrastructure includes IT and operational technology ("OT") to control operations and operate facilities efficiently.[18] As CISA notes, "the integration of IT/OT systems have created new vectors through which adversaries can exploit vulnerabilities in assets, networks, systems, and devices."[19] Despite the need to upgrade infrastructure and the introduction of new IT and OT risks, WWS operators "often lack the resources and technical capacity to adopt rigorous cybersecurity practices."[20] One assessment of 1,062 drinking water systems identified 97 systems serving around 26.6 million Americans as having critical or high-risk cybersecurity vulnerabilities.[21] Significant disruptions to U.S. water and wastewater infrastructure could cause "irreparable physical damage to drinking water infrastructure" and cost nearly $45 billion a day across the U.S.[22]

15 U.S. Government Accountability Organization (hereinafter, "GAO"), *Private Water Utilities: Action Needed to Enhance Ownership Data* (March 2021), 8, https://www.gao.gov/assets/gao-21-291.pdf.

16 GAO, *Critical Infrastructure Protection, EPA Urgently Needs a Strategy to Address Cybersecurity Risks to Water and Wastewater Systems*, GAO-24-106744 (August 2024), 1, https://www.gao.gov/assets/gao-24-106744.pdf.

17 GAO, *Private Water Utilities: Action Needed to Enhance Ownership Data*, 2.

18 GAO, *Critical Infrastructure Protection*, 6, 17. "Operational technology systems are programmed to provide remote and automated control of pipes, pumps, and other physical elements used to treat, store, distribute, and monitor water for contaminants or other properties, such as water pressure or quality."

19 "National Critical Functions - Supply Water and Manage Wastewater," CISA, accessed July 27, 2025, https://www.cisa.gov/national-critical-functions-supply-water-and-manage-wastewater.

20 Michael S. Regan & Jake Sullivan, letter to state governors, The White House, March 18, 2024, 1, https://www.epa.gov/system/files/documents/2024-03/epa-apnsa-letter-to-governors_03182024.pdf.

21 Environmental Protection Agency Office of Inspector General, by Bruno Pigott, *Management Implication Report: Cybersecurity Concerns Related to Drinking Water Systems*, November 13, 2024, 5, https://www.epaoig.gov/sites/default/files/reports/2024-11/full_report_-_25-n-0004t_1.pdf.

22 Ibid., 5.

In addition to managing IT and OT vulnerabilities across complex, geographically distributed operations, WWS organizations must contend with workforce shortages,[23] including limited availability of staff with specialized cybersecurity experience. Many under-resourced organizations that operate water and wastewater systems do not employ cybersecurity staff because they are "uncertain they needed such staff or were unable to provide competitive pay to recruit and retain staff."[24] Instead, they rely on internal staff with little or no cybersecurity expertise or they outsource cybersecurity needs to external service providers.[25]

The threats to U.S. water and wastewater systems are not theoretical. On March 18, 2024, the EPA Administrator and the Assistant to the President for National Security Affairs sent a joint letter to state governors warning that individuals associated with the Iranian government had targeted and disabled a common type of OT used at water facilities. The letter also warned that a group associated with the Chinese government had compromised the IT of multiple drinking water systems to pre-position themselves to disrupt those systems in the event of geopolitical tensions or military conflicts.[26] Between 2006 and 2023, there were 27 publicly disclosed cyber attacks on U.S. water and wastewater facilities.[27] Since 2023, there have been several more cyber attacks on water and wastewater facilities, including a cyber attack that forced a large company — a supplier of drinking water, wastewater, and other services to around 14 million Americans and 18 military facilities across 14 states — to take its systems offline.[28]

23 GAO, *Critical Infrastructure Protection*, 20.

24 Ibid.

25 Ibid.

26 Regan & Sullivan, letter to U.S. state governors, 1.

27 Threat Perspective: United States Water & Wastewater, Dragos, Inc. (June 2023), 2, https://hub.dragos.com/hubfs/Reports/Dragos_Report_CyberThreatPerspective_USWater_Wastewater_Complete.pdf?hsLang=en.

28 Jonathan Greig, "American Water Works Believes No Water, Wastewater Facilities Affected by Cyberattack," *The Record*, Recorded Future, October 7, 2024, https://therecord.media/american-water-works-cyberattack-utility.

MSPs, MSSPs, and Other SPs

1. AN OVERVIEW OF IT AND SECURITY SERVICE PROVIDERS

Many under-resourced organizations choose to outsource IT and information security services to MSPs, MSSPs, and similar service providers (collectively referred to in this report as "ITSSPs"). Outsourcing IT and information security services can allow under-resourced organizations to reduce internal costs and gain access to skilled IT and information security professionals. Outsourcing those services can also allow under-resourced organizations to quickly adapt to evolving external factors, for example by obtaining up-to-date threat and vulnerability information and increasing the manpower available to address those issues. Further, outsourcing enables under-resourced organizations to indirectly share the costs for those services with the service providers' other clients.

There are over 40,000 ITSSPs in the U.S.[29] According to data provided by IT-Harvest, an IT and cybersecurity industry research platform with data about more than 150 ITSSPs, the service providers range from small organizations with fewer than 10 staff to large multinational entities with over 1000 staff. Two-thirds of the service providers listed on the IT-Harvest website have under $1 million in yearly revenue which, combined with the information provided by interviewees for this report, indicates that many service providers are small businesses.

The nomenclature used to describe MSPs, MSSPs, and similar organizations is important because it helps ensure that the under-resourced organizations can identify and engage the appropriate types of service providers. For example, recommendations that focus narrowly on MSSPs risk excluding MSPs and other IT service providers that also provide cybersecurity services. Conversely, recommendations that focus specifically on MSPs risk excluding IT service providers that primarily offer cybersecurity services rather than IT support and, therefore, do not consider themselves MSPs. Some of the organizations interviewed for this report call themselves "MSPs with MSSP features," cybersecurity consultancies, or other labels.

29 Managed Service Providers Association of America, https://mspaa.net/#!map/ord=rnd (noting there are around 43,200 MSPs without counting MSSPs and other types of consultancies).

MSPs typically provide support for a company's IT operations and IT infrastructure management services.[30] Examples of services that MSPs typically provide include: managing IT infrastructure (e.g., network routing and rule and web proxy configurations); managing applications and databases; providing IT help desk support; managing user accounts; and provisioning software (e.g., deployment, maintenance, and upgrades). While MSPs may provide some cybersecurity services, they may not offer the depth of security services that MSSPs offer.

MSSPs provide cybersecurity services and typically maintain or directly outsource a 24/7 security operations center (SOC).[31] They typically do not offer the range of IT services that MSPs provide. Examples of services that MSSPs provide include: governance and strategy advice; personnel security monitoring; training; vulnerability and risk assessments; penetration testing; information system or device monitoring and alerts (typically through a security information and event management (SIEM) tool); identity and access management; support; incident response support; business continuity and disaster recovery support; and system patching and updates.[32]

MSPs, MSSPs, and similar service providers can collectively be referred to as IT and information security service providers, or ITSSPs. The services provided by ITSSPs vary, so terms like MSP and MSSP might not always be clear, especially for under-resourced organizations with limited knowledge of the IT and cybersecurity industries. Table 1 provides examples of the types of services those organizations provide. In practice, these distinctions are not mutually exclusive and services may vary or overlap across ITSSPs.

2. HOW ITSSPs SERVE UNDER-RESOURCED ORGANIZATIONS

Understanding how ITSSPs and their clients find each other is an important first step toward identifying ways to further increase ITSSP coverage of WWS organizations. All of the interviewees reported that their ITSSPs primarily grow their client bases through inbound leads — i.e., clients find them through word of mouth and, to a lesser extent, online search. For all of the ITSSPs interviewed, but especially for those with fewer than 100 staff members, word of mouth was identified as the primary way that new clients learn about ITSSPs' services. As a result, whom the employees of an organization (or their contacts) know is a constraint

30 Nick Hayes, "MSP vs. MSSP: Understanding the Difference," *CrowdStrike*, June 16, 2023, https://www.crowdstrike.com/en-us/cybersecurity-101/managed-security/msp-vs-mssp/.

31 Ibid.

32 Morris et al., "Cybersecurity as a Service," 4.

Table 1: IT and Security Service Providers

Managed Service Provider (MSP)	Cybersecurity Consultancy	Managed Security Service Provider (MSSP)
• Assistance to set up and/or manage IT infrastructure (e.g., servers, routers and access points, and cloud services) • Management operations software • Identity and access management services • Help desk services and technical support • Reporting, auditing, and compliance • Some baseline security, including vulnerability and patch management services • Network operations center (NOC) • IT and data governance advice	• Identity and access management services • Threat detection and intelligence and event alerting • Incident response services • Reporting, auditing, compliance, risk assessments, and penetration testing • Vulnerability and patch management services • Cybersecurity strategy and governance advice	• Management of security software (e.g., endpoint detection and response and data loss prevention tools) • Threat detection and intelligence and event alerting • Incident response services • Reporting, auditing, compliance, risk assessments, and penetration testing • Vulnerability and patch management services • Security operations center (SOC) • Cybersecurity strategy and governance advice • Cybersecurity education and training

on how that organization will learn about ITSSPs and which ITSSPs they are likely to contact. That constraint would need to be addressed in order to expand ITSSP coverage for WWS organizations.

In addition to inbound leads, the interviewees reported that their ITSSPs engage with prospective clients through various other means. All of the ITSSPs meet prospective clients through industry and community events.[33] For larger ITSSPs, these events did not seem to be as important for client development as they are for smaller ITSSPs. Some of the ITSSPs offer webinars and publish newsletters and reports, although these are more often than not used to engage with existing clients or organizations otherwise within the ITSSPs' networks. A few of the ITSSPs interviewed provide pro bono services to under-resourced organizations and encourage their staff to participate in pro bono activities.

ITSSPs serve organizations across a broad range of industries and sectors. For example, an ITSSP might provide services to both a community health center and a rural water treatment plant. None of the interviewees reported limitations regarding the industries or sectors they could serve. Those clients have some common cybersecurity needs, such as setting up strong

33 This report does not consider online advertising conducted by ITSSPs, because online search results would not immediately provide a comprehensive listing of ITSSPs or a reliable way for potential beneficiaries to understand the services their organizations need (which is likely why many potential beneficiaries rely on word of mouth to learn about ITSSPs).

passwords or multi-factor authentication. However, ITSSPs' clients can also have needs specific to their industry, technology stack, and cybersecurity maturity level.[34]

Some interviewees reported challenges their organizations might face when serving clients with significant OT environments. Organizations that operate water and wastewater systems, for example, have specific needs because of the industrial control system ("ICS") and OT environments they operate, which can include programmable logic controllers ("PLCs"), supervisory control and data acquisition ("SCADA") systems, and human-machine interfaces ("HMIs"), in addition to traditional IT systems. OT interacts with and can detect or cause direct changes in physical systems, such as pipes, pumps, valves, and tanks.

For that reason, ITSSPs that work with WWS organizations must have expertise in both IT and OT operations and cybersecurity, so they tend to be specialized ITSSPs, like Dragos Inc. or I&C Secure, Inc. A 2023 report from Dragos notes that two of the five most pervasive threats to water and wastewater systems include vulnerable ICS/OT controllers and the ability of adversaries to access ICS/OT environments through exposed assets (the other three threats identified in the report could still allow access to ICS/OT environments).[35] A report from October 2024 found that 400 web-based HMIs for U.S. water facilities were exposed online, 40 of which were "fully unauthenticated and controllable by anyone with a browser." With some exceptions,[36] executing attacks on ICS/OT environments generally requires specialized knowledge of signal processing, control principles, the physics of process behavior, the mechanics and failure conditions of equipment, and more.[37] Specialized knowledge is also required to defend those systems against cyber attacks.

Other factors can dictate which clients work with which ITSSPs. Some interviewees noted that their organizations tailor their services to the specific needs of their clients. Interviewees at smaller ITSSPs that primarily serve nonprofits noted the importance of alignment of a client's

34 For purposes of this report, cybersecurity maturity level is used to refer to the overall capabilities across an organization's IT and information security programs. The implementation tiers of the NIST Cybersecurity Framework (Partial, Risk-Informed, Repeatable, and Adaptive) provide a useful guide that can serve as a proxy for an organization's cybersecurity maturity level. National Institute of Standards & Technology, *The NIST Cybersecurity Framework (CSF) 2.0*, NIST CSWP 29, Feb. 26, 2024, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf.

35 Dragos, Inc., "Threat Perspective: United States Water & Wastewater," 2.

36 HMIs are one exception. They "provide access to an ICS network" and offer "the context and visibility needed to determine whether a system is genuinely part of critical infrastructure. These interfaces act as literal viewports into live industrial processes." "Turning Off the (Information) Flow: Working with the EPA to Secure Hundreds of Exposed Water HMIs," Censys (June 5, 2025), https://censys.com/blog/turning-off-the-information-flow-working-with-the-epa-to-secure-hundreds-of-exposed-water-hmis.

37 Marina Krotofil, *Industrial Control Systems: Engineering Foundations and Cyber-Physical Attack Lifecycle*, Technical Whitepaper, (May 2023), 31, https://github.com/marmusha/cyber-physical-security/raw/main/Industrial-Control-Systems-Engineering-Foundations-and-Cyber-Physical-Attack-Lifecycle.pdf.

mission to their selection of an ITSSP. One reported advising nonprofit clients on physical security needs in response to increasing questions about those issues. Some ITSSPs, especially larger ones, might not have the same flexibility to tailor their services to specific client sectors. In addition, some ITSSPs — particularly those that offer more incident response services or operate a SOC — require a certain number of employees per client or per device. In all of those cases, ITSSPs must be able to hire and retain sufficient personnel to be able to appropriately manage their clients' needs.

Therefore, though they are subject to some limitations, many ITSSPs can serve clients across industries and sectors. Clients that operate ICS/OT environments may require support from specialized service providers that many ITSSPs are not equipped to provide. In addition, factors like mission-alignment can affect which clients and ITSSPs are compatible. Overall, this suggests that ITSSPs should be able to help reduce the number of under-resourced organizations that lack adequate IT and information security support.

Recommendations to Increase ITSSP Coverage of Under-Resourced Organizations

In the short term, cyber volunteer organizations are providing a much-needed lifeline to some under-resourced organizations, including those that operate water and wastewater systems. For example, DEF CON's Project Franklin utilizes the talents of volunteer hackers to help WWS organizations remediate technology vulnerabilities and improve their cyber resilience.[38] However, there are too few cyber volunteer organizations in the U.S. to serve the number of under-resourced organizations in need of their services. Moreover, without dedicated funding and coordination, scaling cyber volunteer organizations to sufficiently serve under-resourced organizations would likely require several years.

ITSSPs provide an option for a longer-term solution. Because IT and security services are their core business, and they do not rely on volunteers to provide those services, ITSSPs do not have the same constraints as cyber volunteer organizations. There are some drawbacks of under-resourced organizations overrelying on ITSSPs, such as the costs, the moral hazard of outsourcing responsibility for this critical business function and, in some cases, the requirement to use ITSSP-supported technologies. However, the benefit to under-resourced organizations of rapidly increasing their cyber resilience far outweighs those drawbacks.

The fact that more WWS organizations do not utilize ITSSPs can be attributed to several factors, some of which were identified by interviewees. On the demand side — i.e., organizations in need of ITSSP services — key factors include costs, a lack of understanding about cybersecurity risks and the services ITSSPs provide, and difficulty identifying competent ITSSPs. On the supply side — i.e., ITSSPs offering services — challenges include insufficient marketing by ITSSPs to the relevant market segments, inadequate means of differentiating their services from those of their competitors, and a lack of information sharing. The remainder of this section provides demand- and supply-side recommendations to improve WWS (and other under-resourced) organizations' access to ITSSP services.

38 "Waterbury Joins DEF CON Franklin Program to Strengthen Cybersecurity for Water Systems," *Industrial Cyber*, Feb. 3, 2025, https://industrialcyber.co/news/waterbury-joins-def-con-franklin-program-to-strengthen-cybersecurity-for-water-systems/.

1. DEMAND-SIDE: RECOMMENDATIONS TO INCREASE AWARENESS AND PROCUREMENT OF ITSSP SERVICES

1. ITSSPs and independent third-parties must increase information security awareness and education for under-resourced organizations.

A WWS organization that does not work with an ITSSP may not realize it needs ITSSP services or even understand what ITSSPs do. Contextualizing the need for and benefits of ITSSP services is, therefore, an essential first step. Some interviewees, particularly those whose ITSSPs serve nonprofit clients, identified the importance of helping clients understand the criticality of cybersecurity in carrying out their missions. Interviewees from ITSSPs that primarily serve for-profit companies did not identify a need to make the case for their services in the same way. Those interviewees noted instead that for-profit clients generally are aware of the services they need before they engage the ITSSP. By the time for-profit entities seek ITSSP services, someone within the client organization has typically already made the business case to justify investments in additional IT and cybersecurity measures and obtained approval for the engagement.

Cybersecurity education and training tailored to subgroups of under-resourced organizations can help to highlight the importance of information security in the context of their missions. The Take9 initiative by Craig Newmark Philanthropies — a large-scale cybersecurity public service campaign — provides an example of what such efforts could entail.[39] Such initiatives can be driven by independent organizations or by individual ITSSPs. In addition, outreach by ITSSPs through forums like news articles, conference talks, and webinars can also help to educate prospective clients about IT and cybersecurity risks and how ITSSPs can help address them. Of the ITSSPs interviewed, most engage in some or all of those activities to reach potential clients.

With respect to SLTTs in particular, state governments already maintain relationships with local government entities that could be used to facilitate education and awareness initiatives. Considering there are nearly two million nonprofits in the U.S. and over 33 million SMBs, similar outreach may prove more challenging, but industry groups may have more success in that area. Despite the challenges, continued education and awareness initiatives are essential to improving demand for ITSSP services from under-resourced organizations.

39 Take9 is "a large-scale cybersecurity public service campaign aimed at helping Americans protect themselves against growing cyber threats . . . [and promoting] the awareness, knowledge, and practical tools needed to build personal resilience, contributing to community and national resilience against cyber threats." Amira Dhalla & Sasha Cohen O'Connell, "Take 9 Seconds for a Safer World: Launching a National Public Service Cybersecurity Campaign," *Aspen Institute*, October 2, 2024, https://www.aspeninstitute.org/blog-posts/take-9-for-a-safer-world/. See also https://pausetake9.org/.

2. A cybersecurity nonprofit should build a matching service for ITSSPs.

Many interviewees reported that their clients primarily find ITSSPs through word of mouth. That indicates there is a lack of comprehensive or trustworthy sources for prospective clients to obtain information about ITSSPs. Interviewees also reported that the skill levels of ITSSPs — and consequently, the quality of the services clients receive — can vary widely. There are no uniform qualifications or baseline skill sets for the industry. In other words, whether an under-resourced organization finds an ITSSP, let alone one that can sufficiently meet the organization's needs, is largely the result of who knows whom.

A director of ITSSPs, with information such as their services and the types of industries and clients they serve, would help to address that knowledge gap. Such a service could even be run on a for-profit basis to cover operating costs. It could function similarly to Zocdoc, a platform that uses information provided by individuals to match them with a list of medical professionals who can meet their needs.[40] Individuals trust that Zocdoc's recommended medical care providers will accept their insurance and will meet the criteria they specified. In addition, Zocdoc allows individuals to read reviews of the medical professionals posted by previous patients, which can help them to differentiate among medical professionals. A similar directory of ITSSPs and the services they offer could provide functionality to match under-resourced organizations with ITSSPs.

Similar solutions already exist that could be expanded or referenced to fully meet the needs of under-resourced organizations. For example, the Managed Service Provider Association of America (MSPAA), maintains a database and search functionality intended to help match SMBs with MSPs.[41] MSPAA is a membership-based organization, and it is not clear that other types of ITSSPs (MSSPs and cybersecurity consultancies) are likely to become members or be included in the existing database. None of the ITSSPs (including MSPs) that participated in this research appeared in a search of the MSPAA database. As another example, in June 2025, the University of California, Berkeley's Center for Long-Term Cybersecurity and the CyberPeace Institute launched a directory and matching service for cyber volunteers, which can serve as a model.[42]

40 Zocdoc, https://www.zocdoc.com/.

41 About Us, Managed Service Provider Association of America, https://mspaa.net/about-us/.

42 "Cyber Resilience Corps," UC Berkeley Center for Long-Term Cybersecurity, last modified March 31, 2025, https://cltc.berkeley.edu/program/cyber-resilience-corps/. In 2024, CISA took steps to create such a service for cyber volunteer organizations when it launched the Cyber Volunteer Resource Center as part of the agency's under-resourced organizations portal. However, that resource has not yet been fully developed and lacks comprehensive materials for cyber volunteers. "Cyber Volunteer Resource Center," CISA, last accessed July 27, 2025, https://www.cisa.gov/audiences/high-risk-communities/cybervolunteerresourcecenter.

That matching service addresses a critical cybersecurity need for nonprofits, but it is not intended to replace the long-term IT and cybersecurity support that an ITSSP would provide.

A trusted intermediary must create and maintain any directory or matching service for ITSSPs, as Zocdoc, MSPAA, and UC Berkeley and the CyberPeace Institute have done with their platforms. That intermediary must also bear ongoing costs to maintain and improve the platform. While the cyber volunteer portal is free,[43] Zocdoc earns revenue primarily through fees charged to medical providers for each appointment booked through its platform,[44] and MSPAA collects membership fees. An ITSSP matching service could generate enough revenue to offset some of its operating costs. Ultimately, under-resourced organizations may view an independent nonprofit as more trustworthy than a for-profit company and, therefore, a nonprofit may be best suited to creating and operating a matching service for ITSSPs.

3. Under-resourced organizations and industry groups should form purchasing pools or collaboratives.

Some interviewees reported that purchasing pools (or collaboratives) could be an attractive option for under-resourced organizations to procure ITSSP services. A purchasing pool would allow multiple buyers to submit joint bids for services from an ITSSP. Several interviewees commented that it can be difficult for ITSSPs (especially larger ITSSPs) to make a profit from small businesses (or even small municipalities), because of the level of (sometimes bespoke) support those organizations require. Purchasing pools can help remedy that situation by allowing prospective clients to approach the ITSSP and procure services in a more cost-effective manner. Purchasing pools can reduce the administrative burden on under-resourced organizations and prevent ITSSPs from having to manage multiple responses to requests for services and negotiations.

This recommendation is likely more attractive for SLTTs than for private entities. For purchasing pools to be most effective, the clients must have similar technology within their organizations so that the ITSSP will not be required to create bespoke solutions for each client. A state could require or incentivize municipalities to utilize common technology. For example, in 2023,

43 CyberPeace Institute, cybervolunteers.us.

44 "Zocdoc's Turnaround: From an Unsustainable Path to Profitable Growth," Zocdoc, October 15, 2020, https://www.zocdoc.com/about/news/zocdocs-turnaround-from-an-unsustainable-path-to-profitable-growth/.

the State of Florida procured cybersecurity services through a state department on behalf of municipalities and saved taxpayers around $11 million.[45]

While it may be difficult for a group of independent nonprofits or SMBs to align on the same technology stack, this could be done in various ways. For example, donors and investors could recommend a standard set of technologies for the organizations they fund. Industry groups in which those organizations participate, such as WaterISAC or the National Rural Water Association, could also recommend certain technologies to members in exchange for the benefit of participating in the purchasing pool. In all cases, purchasing pools can offer under-resourced organizations and ITSSPs the benefits of scale, including reduced cost.

4. Investors and donors should dedicate funding to information security.

Investors have an important role to play in improving the demand-side of the market for ITSSP services, especially since they have a direct financial interest in the success of the organizations they fund. Today, almost all organizations depend on information and information systems to successfully carry out their missions. A significant cyber attack can prevent an organization from achieving its mission or significantly impair a company's ability to continue to operate, as happened with the genetic data testing company, 23andMe, following a 2023 data breach.[46]

To mitigate some risk to their investment, more investors should conduct due diligence regarding the cybersecurity practices of companies in their portfolios and ensure the companies dedicate funding to IT and cybersecurity needs. In addition, investors can partner with ITSSPs that can provide services to organizations across their investment portfolio (effectively creating a purchasing pool or shared services model). For example, an investor could negotiate a discounted rate at which an ITSSP would serve the investor's portfolio companies, allowing the portfolio companies to take advantage of the discounted rate and avoid the administrative and financial costs of finding similar services. Doing so will help ensure that funding intended to support an organization's core mission is not later diverted to shore up cybersecurity gaps following a crisis. State and local governments could also offer tax incentives to investors who dedicate funds to IT and cybersecurity because, on the whole, those investments will benefit

45 "Department of Management Services Strengthens State Workforce, Bolsters Cybersecurity, Delivers Savings for Floridians," Florida Department of Management Services, December 28, 2023, https://www.dms.myflorida.com/agency_administration/communications/dms_news_releases/department_of_management_services_strengthens_state_workforce_bolsters_cybersecurity_delivers_savings_for_floridians.

46 Maura Webber Sadovi, "23andMe CRO Details Data Breach's Role in Bankruptcy," *CFO Dive*, March 25, 2025, https://www.cfodive.com/news/23andme-cro-details-data-breach-role-bankruptcy/743485/.

the public at large by reducing the costs of cybersecurity incidents and enabling continuity of essential services.

Similarly, nonprofit donors can make funds contingent on their grantees demonstrating that they have taken or will take certain baseline cybersecurity measures. Many donors already require grantees to meet certain requirements to apply for or receive funds. This could be addressed as part of a grant application, as a requirement to receive funds, or as part of required reporting related to a grant. The CyberPeace Institute works with donors to do that, among other things, through their CyberPeace Builders program.[47] Donors can also form relationships with ITSSPs that could save the grantees the administrative burden of finding security service providers on their own, and potentially obtain preferential pricing for their grantees.

With both investors and donors, there could be some drawbacks depending on the approach they take. For example, the ITSSP that an investor recommends may not be the best option for a company, based on its technology stack, preferences, or other factors. With respect to nonprofits, many grantees must already comply with significant grant application and reporting requirements, and imposing additional requirements can risk increasing their administrative burden (and costs) to obtain a grant — costs that will not go toward the nonprofit's core mission. Additionally, both investors and donors may not have the cybersecurity knowledge or receive adequate advice to make informed recommendations. Despite those potential drawbacks, investor and donor support present viable options to help expand ITSSP coverage of nonprofit and for-profit entities. This recommendation is less directly applicable to SLTTs, because they do not receive investor or donor funds in the way for-profit and nonprofit organizations do.

2. SUPPLY-SIDE: RECOMMENDATIONS TO INCREASE AVAILABILITY OF AND ACCESS TO ITSSP SERVICES

1. ITSSPs and industry groups must increase their community engagement.

All interviewees from ITSSPs and other security service providers reported that their organizations engage with the under-resourced organizations they serve through conferences, webinars, newsletters, reports, and other means. Continuing to increase ITSSP community engagement, especially in events targeted toward under-resourced organizations, will help to further increase awareness about the ITSSPs' services among prospective clients. While that may be

47 "Cyber Peace Builders," CyberPeace Institute, last accessed July 27, 2025, https://cpb.ngo/foundations.

difficult for thousands of ITSSPs to manage independently, conference and event organizers should seek to connect ITSSPs with under-resourced organizations. Conferences and events, such as those hosted by organizations like the National Governors Association (for states), TechSoup (for nonprofits), and local chambers of commerce (for SMBs), should dedicate programming and space for ITSSPs and prospective clients to network and learn about each others' services and needs.

For example, on June 11, 2025, the Cyber Civil Defense Summit, a conference hosted by UC Berkeley's Center for Long-Term Cybersecurity in Washington, D.C., included sessions focused on water and wastewater systems that brought together MSSPs, government, and industry groups representing WWS organizations. A common theme was the need for more outreach to water and wastewater systems organizations. One panelist noted that most rural water organizations do not follow cybersecurity groups on professional sites or social media, so it is up to the interested organizations to meet the WWS organizations where they are. That could mean contacting them directly, partnering with WaterISAC or the National Rural Water Association, or raising awareness about the resources available to WWS organizations through the Circuit Rider Program, a national program designed to provide technical assistance to rural water systems in the U.S. that are experiencing day-to-day operational, financial, or managerial issues.[48]

2. ITSSPs should expand pro bono and discounted services for under-resourced organizations.

ITSSPs could also raise awareness and serve more under-resourced organizations by providing pro bono and discounted services, such as helping to develop an information security roadmap or strategy, or addressing time-bound needs, such as creating an incident response plan.[49] While providing free or low-cost services may not address the long-term cybersecurity needs of under-resourced organizations, it can provide a lower-cost way to gain exposure and build understanding of the value ITSSPs offer. Some, but not all, interviewees reported that their organizations provide pro bono services to prospective SLTT or nonprofit clients. However, based on the interviews conducted, too few ITSSPs have systematic programs to provide pro bono services. Many ITSSPs have pricing models that would allow for discounted services either based on the type, size, or complexity of the prospective client.

While this recommendation will be useful to help expand the reach of ITSSPs, it may be limited in effect compared with some of the other proposed solutions. For example, the number of

48 "Circuit Rider Program," National Rural Water Association, https://nrwa.org/circuit-rider-program/, last accessed July 27, 2025.
49 "Cyber Security for Good," RipRap Security, last accessed July 27, 2025, https://www.riprapsecurity.com/cyber-security-for-good.

hours of pro bono services or the volume of discounts ITSSPs can offer must be limited so that their businesses can remain profitable. In addition, it is less likely that ITSSPs will provide free or discounted services to prospective for-profit clients (although discounts might be offered to SMBs). Further, at least one interviewee whose ITSSP offers pro bono services noted that some nonprofits that were offered pro bono services failed to utilize those services, for example by not attending meetings or implementing recommendations.

Despite the potential drawbacks, this recommendation could prove valuable, especially if coordinated through independent organizations. For example, industry groups like WaterISAC and the National Rural Water Association could sign up ITSSPs that may be willing to offer free or discounted services to their members. They could also promote existing programs to their members, such as the Dragos Community Defense Program, which makes free resources available to U.S. and Canadian water, electric, and natural gas utilities with less than $100 million in revenue.[50] In addition, cyber insurers, which maintain ITSSPs on approved vendor lists for their insureds to utilize, could encourage their approved vendors to commit to providing a minimum amount of pro bono or discounted services to under-resourced organizations.

3. ITSSPs must enhance collaboration and information-sharing to better serve under-resourced organizations.

Based on the interviews conducted, information sharing and collaboration between ITSSPs is too limited. Although these companies are competitors, improving collaboration and information sharing between ITSSPs could help them better serve their clients. For example, if a broad group of ITSSPs learn about a certain type of malware targeting water treatment plants — and develop effective methods to mitigate the risk of successful deployment of that malware — it will benefit all of the ITSSPs and the WWS organizations that rely on them.

In many cases, information sharing is carried out through Information Sharing and Analysis Centers ("ISACs"),[51] as well as through Information Sharing and Analysis Organizations ("ISAOs"), which serve a similar purpose.[52] Of the existing organizations, the Information Technology-Information Sharing and Analysis Center ("IT-ISAC") seems best placed to help improve information sharing among ITSSPs, but one or more ITSSPs could also form a dedicated group. An ISAC or ISAO could also make public a comprehensive membership directory

50 "Dragos Community Defense Program," Dragos, Inc., last accessed July 27, 2025, https://www.dragos.com/community/community-defense-program/.

51 "Member ISACs," National Council of ISACs, last accessed July 27, 2025, https://www.nationalisacs.org/members.

52 "About," ISAO Standards Organization, last accessed July 27, 2025, https://www.isao.org/about/.

to facilitate the ability of under-resourced organizations to identify and engage service providers. Other organizations, like MSPAA or The Tech Tribe — an online, membership-based community designed to help MSPs' businesses grow — could serve a similar function.[53]

Enhanced information sharing among service providers will not directly expand the number of under-resourced organizations that utilize ITSSPs. However, it can improve the knowledge and expertise of ITSSPs and, in turn, enhance their ability to more effectively serve under-resourced organizations. It could also lead ITSSPs to more frequently operate from the same playbook when addressing common issues, or even to standardize some of their service offerings for under-resourced organizations.

53 The Tech Tribe, https://thetechtribe.com/.

Conclusion

Under-resourced organizations operate critical infrastructure and provide essential services. The WWS sector provides a lens into how important those services can be for communities across the U.S. Safeguarding physical and digital assets of those organizations is essential for them to be able to continue to operate. Yet, too many under-resourced organizations have not adopted adequate cybersecurity measures to safeguard their assets and lack the resources to better secure them. ITSSPs deliver services designed to safeguard their clients' information and information systems and can help under-resourced organizations improve their long-term cyber resilience. However, not enough under-resourced organizations and ITSSPs work together today. No single recommendation in this report will remedy that, but in aggregate, implementation of these recommendations will help improve the cyber resilience of under-resourced organizations. This report should serve as a call to action for the stakeholders referenced to take steps to help secure under-resourced organizations and, by extension, to secure U.S. critical infrastructure.

About the Author

Michael Razeeq is a data governance, strategy, and privacy attorney with experience working for global financial services, media, and energy companies, and a multinational law firm. He is a Non-Resident Fellow, Public Interest Cybersecurity with UC Berkeley's Center for Long-Term Cybersecurity (CLTC), as well as a 2024 New America #SharetheMicinCyber Fellow.

Acknowledgments

The author would like to thank the UC Berkeley Center for Long-Term Cybersecurity and the following individuals for their valuable feedback on this report: Steve Sharer, RipRap Security; Lance Larson, San Diego State University; and Mark Schreiber, Brian Long, and Katelyn Ringrose, McDermott, Will & Emery, LLP.


CLTC
Center for Long-Term
Cybersecurity
UC Berkeley