Testimony of Joshua Corman[1]

"Research-Driven Resilience:
Applying Science to Secure U.S. Water Systems from Cyber Threats"

Subcommittee on Environment
Committee on Science, Space, and Technology
May 21, 2026

Chairman Franklin, Ranking Member Amo, thank you for the opportunity to testify before you today. I am Joshua Corman, Executive in Residence for Public Safety and Resilience at the Institute for Security and Technology and the principal investigator for the UnDisruptable27 project.[2] I have spent the bulk of my career trying to reduce our dependence on undependable technology, especially in life-safety sectors *"where bits and bytes meet flesh and blood."* Today's hearing is a key opportunity to examine how the United States' research and development ecosystem can support one of the most foundational elements of our critical infrastructure: water and wastewater systems.

To put it succinctly, these systems are highly vulnerable, yet they are foundational to key functions of our society. In other words, through our over-dependence on undependable technology, we have created the conditions such that the actions of any single outlier can have a profound and asymmetric impact on human life, public safety, economic stability, and national security. We have not yet paid the price for our failure to design securely, but the threat environment is rapidly worsening. Government is not the only answer, but it is an important *part* of the answer, including with respect to the research and development ecosystem. To meaningfully reduce our risk, we will need to embrace novel research approaches.

To understand just how vulnerable our systems are, consider the fact that most water systems use operational technology that was never designed to be connected to the internet. The industrial control systems that control pumps can have software or firmware that is difficult to patch. They often lack core architectural design elements that would allow for secure configuration. And the workforce that operates these utilities is often equipped with minimal cybersecurity training and lacks access to the tools and services that could help.

Fortunately, what we have not yet seen is threat actors taking advantage of water system vulnerabilities *at scale*. Other sectors of the economy (e.g., healthcare delivery) have been

---

[1] I would like to thank Nicholas Leiserson and Sophia Mauro for their assistance in the preparation of this testimony. No AI assistance was used in developing this testimony.
[2] https://securityandtechnology.org/undisruptable27/

ravaged by ransomware and widespread data theft, but water has, to date, largely avoided being in the crosshairs.

Unfortunately, that is changing, and unlike previous adversaries who sought data or money, our foes now seek to disrupt and destroy lifeline critical functions. People's Republic of China's army units have hacked U.S. water facilities. Whether to directly impede military mobilization or cause civilian panic during crisis or conflict, these military units are taking advantage of the vulnerability of our water infrastructure to hold us at risk. Pro-Iranian government hackers are also targeting U.S. companies as part of the ongoing conflict, and they have a history of hitting water targets. What's more, advances in large language model capabilities also risk exposing water systems to new types of threat actors. Despite concerns about a coming AI-driven cybersecurity crisis due to a rapid increase in the number of identified, and weaponized, vulnerabilities in code, zero industrial control system vendors were included in Project Glasswing, Anthropic's early access program.

In the face of this rapidly rising risk, I created UnDisruptable27 (U27). U27 is an applied research project intended to answer the question: before a potential 2027 hybrid conflict, with the time and resources we have, are there familiar, affordable, pragmatic, and timely ways to increase the resilience of our most-consequential water utilities against destructive cyber attacks affecting their most consequential customers? With funding from Craig Newmark Philanthropies, we are working with hospital communities across the nation—*and the water systems who support them*—to apply engineering solutions that will meaningfully mitigate the impact of cyber attacks.

Our goal at U27 is to *innovate narrowly* so that we can *replicate widely*. This kind of hands-on approach, at the nexus of engineering, computer science, and public policy, is critical for helping both the sector itself and the sectors that depend upon it. Water utilities face significant funding challenges, making investments in resilience—particularly for national security reasons—hard to justify. These funding challenges, in turn, also make it unlikely that the private sector will develop solutions. Unless or until incentives change this dynamic, the responsibility for developing solutions to help the ecosystem boost its resilience falls to academia, civil society, and government labs.

Co-creation is essential. The types of solutions we are after must fit the operational constraints of water system owners and operators, as well as the broader funding limitations within the sector. They also must be designed to scale across the 53,000 community water systems across the nation.

To that end, the Committee should consider creating or supporting programs in systems engineering that are specifically designed to reduce national security and public safety risk.

The Committee should also consider how to strengthen the pipeline between researchers and the Water and Wastewater Systems Sector Risk Management Agency team at the Environmental Protection Agency and grant program managers. More broadly, the Committee should continue to support social, behavioral, and economic research in cybersecurity, including by creating a specific cross-directorate program within the National Science Foundation to address this intersectional area of research. Finally, the Committee should support programs that examine cross-sector dependency mapping, including detailed examinations of supply chains.

I. About IST

The Institute for Security and Technology (IST)[3] is a 501(c)(3) charitable non-profit critical action think tank focused on the implications of technology for our national security. Home of the Ransomware Task Force,[4] IST's cybersecurity program conducts applied research and policy development to address misaligned incentives in the technology ecosystem that leave critical infrastructure vulnerable to abuse and misuse. Beyond UnDisruptable27, core areas of ongoing research include the K-12 Cyber Defense Coalition;[5] efforts to strengthen and improve CISA's CVE Program;[6] support for the International Counter Ransomware Initiative (CRI) as part of its Private Sector Advisory Panel; and work to adapt the Ransomware Task Force model in other countries.[7]

II. Risks to Water

The Water and Wastewater Systems Sector is particularly vulnerable to cyber operations. Historically, few threat actors have been positioned and motivated to take advantage of this vulnerability. That is changing with the rise of People's Liberation Army (PLA) hacking campaigns targeting civilian critical infrastructure, the increased threat from Iran as part of the ongoing conflict, and the rapid evolution in vulnerability discovery capabilities among leading artificial intelligence models that create the possibility of AI-powered *hacking* without either AI-powered *fixing* or *application of fixes*.

Water is Vulnerable

Of the 16 Critical Infrastructure sectors, water is among the least well-funded and has the least mature public private partnerships in place, including the lowest participation in the sector's information sharing and analysis center. It has extremely limited federal cybersecurity

[3] https://securityandtechnology.org/
[4] https://securityandtechnology.org/ransomwaretaskforce/
[5] https://securityandtechnology.org/blog/announcing-the-k12-cyber-defense-coalition/
[6] https://securityandtechnology.org/virtual-library/report/cve-at-a-crossroads/
[7] https://securityandtechnology.org/blog/mexico-rtf/

or resilience regulations and the least downtime tolerance for both human life and utilities. At the same time, other critical infrastructure and other lifeline critical functions depend on the water sector to work.[8]

Water delivery is highly federated in the U.S. There are approximately 148,000 water systems in the United States.[9] Roughly a third of them (53,000) are classified as community water systems, meaning they provide water to the same population, year-round.[10] Public water systems are largely independent, such that they rely on their own information and communications technology and services (ICTS) and operational technology (OT), rather than being part of a larger conglomerate.[11]

Water infrastructure is also long-lasting. Capital investments in water have declined as the pace of population growth has slowed. Many of the core elements of water systems have been in service for decades.[12] The slow pace of capital expenditures makes it difficult for utilities, whose rates are generally tightly regulated, to make investments in technology.

Compounding this exposure is the legacy nature of much of the equipment. Water systems run older software and hardware, some of which is no longer being maintained. In many cases, systems being connected to computers and networks were designed before remote, internet-based operations were an accepted practice—and they thus lack even basic cybersecurity features. Granted, in some circumstances, connectivity can improve operations, and help to save money. Yet ironically, the same remote connectivity being used to save money, is the very thing exposing us to accidents and adversaries–which ultimately cost far more than the cost savings to be had in the first place. There is a cost to connectivity, and we will either pay that cost or "pay the price." As I said in the 405c Healthcare Task Force:[13] If you can't afford to protect it, then you can't afford to connect it.

What's more, many new systems wind up connected by default, as opposed to connected in order to meet a specific business purpose. Some do not work at all without an internet connection, and others may have no option for manual backups.[14]

---

[8] https://www.cisa.gov/national-critical-functions-set
[9] https://www.epa.gov/dwreginfo/information-about-public-water-systems
[10] https://www.amwater.com/corp/Customers-and-Communities/Water-Learning-Center/the-water-industry
[11] Contrast this with hospitals, for instance, which are often parts of chains with dozens of facilities sharing corporate leadership and ICTS such as electronic medical records.
[12] https://www.awwa.org/wp-content/uploads/Buried-No-Longer.pdf; https://theconservationfoundation.org/water-infrastructure-threatens-conservation/
[13] https://healthsectorcouncil.org/wp-content/uploads/2018/06/CYBERSECURITY-TASK-FORCE-REPORT-ON-IMPROVING-CYBERSECURITY-IN-THE-HEALTH-CARE-INDUSTRY.pdf
[14] https://www.congress.gov/event/118th-congress/house-event/LC73307/text

Deepening the risk facing water utilities is the fact that they currently participate in cybersecurity programs at very low rates. For example, of the 53,000 community water systems nationwide, only approximately 420 of them belong to the Water Information Sharing and Analysis Center.[15] A further complication is the aging of the water workforce: 57 percent of operators expect to retire in the next ten years.[16]

Threats on the Rise

The vulnerability in the water sector has not translated into spectacular failures due to cybersecurity incidents. While there have been cybersecurity incidents at utilities, all but a few have targeted business systems (e.g., billing),[17] not the OT systems that actually control physical processes. Most public incidents that have crossed over to OT networks[18] have been stopped before they can cause *significant* harm[19] or have been mitigated through manual interventions.[20] However, the threat landscape is becoming significantly more dangerous.

Volt Typhoon

In January 2024, senior government leaders testified before Congress about a group of People's Liberation Army hackers.[21] They shared that the military units, called "Volt Typhoon" by a private sector threat intelligence team, were pre-positioning on U.S. critical infrastructure, cultivating unauthorized access to utilities, transportation hubs, and communications networks. In a time of crisis or conflict with the United States, the People's Republic of China could use their access to these systems to disrupt operations or even cause physical damage. Doing so could directly impair military mobilization.

However, some of the Volt Typhoon targets have no connection to the military–a fact that is of chief concern for me and for my efforts through UnDisruptable27. These targets include water facilities that serve civilian populations.[22] Per public assessments from the U.S.

---

[15] https://www.waterisac.org/waterisac-surpasses-600-members-strengthening-water-and-wastewater-security-nationwide
[16] https://wastewatervisibility.com/national-rural-water-association-releases-policy-paper-centered-on-the-water-workforce-and-national-security/
[17] https://www.cnbc.com/2024/10/08/american-water-largest-us-water-utility-cyberattack.html
[18] According to the Office of the Director National Intelligence, over one six-month period, incidents occurred in Georgia, Illinois, Ohio, Pennsylvania, South Carolina, Texas, and West Virginia. https://www.dni.gov/files/CTIIC/documents/products/Recent_Cyber_Attacks_on_US_Infrastructure_Underscore_Vulnerability_of_Critical_US_Systems-June2024.pdf
[19] https://www.databreachtoday.asia/russian-attacks-on-polish-water-utilities-use-fear-as-weapon-a-31681
[20] https://edition.cnn.com/2024/04/17/politics/russia-hacking-group-suspected-texas-water-cyberattack
[21] https://www.c-span.org/program/public-affairs-event/select-committee-hearing-on-chinas-cyber-threat-to-the-us/637719
[22] https://www.cbsnews.com/news/china-hacking-us-critical-infrastructure-retired-general-tim-haugh-warns-60-minutes-transcript/

government, attacks on these targets would serve "to incite chaos and panic across our country and deter our ability to marshal military might and citizen will."[23]

Pre-positioning activity does not, itself, constitute an "attack," but it should worry us nonetheless. While not quite the equivalent of placing "digital bombs," we would still consider "trespassing" in someone's property or "breaking and entering" into someone's home to be criminal, even if nothing has been taken yet or damaged yet. Further, such payloads could potentially be delivered to water systems at will and instantly via the level of access that China's leadership continues to enjoy. Regardless, the PRC's intent to hold us at risk is evident. Failing to better secure key infrastructure, including water utilities, threatens our ability to act in our national security interests at pivotal moments and, more importantly, endangers the lives of our fellow citizens, especially when it comes to healthcare and hospitals. Of note, while Volt Typhoon has not formerly targeted hospitals, given hospitals' dependence upon a stable water supply, any disruptions to water will in turn disrupt healthcare delivery.

Iran

Pro-Iranian government hackers have been actively targeting the United States and Israel following the onset of Operation Epic Fury. While much of the activity in cyberspace has been focused on sowing misinformation, these hackers have succeeded in disrupting critical infrastructure. In particular, a top U.S.-based medical device and supply manufacturer, Stryker, was the victim of an attack and had to significantly curtail operations following a cyber intrusion.[24]

Pro-Iranian government groups also have a history of targeting the water sector. Following the events of October 7, 2023, utilities across the country were defaced by "hacktivists." In Aliquippa, PA, utilities were forced to resort to manual operations after being hit.[25] This pattern of targeting water systems dates back to at least 2020, when an Iranian cyber operation attempted to interfere with chemical levels at a water treatment facility in Israel.[26]

As tensions remain high with Iran, the United States continues to face significant risk. In April, the Cybersecurity and Infrastructure Security Agency (CISA) released an advisory highlighting vulnerabilities in programmable logic controllers (PLCs), equipment used in a wide range of industrial settings, including water and wastewater systems. CISA punctuated the advisory by

[23] https://www.cisa.gov/news-events/news/opening-statement-cisa-director-jen-easterly
[24] https://securityandtechnology.org/event/the-fight-comes-to-our-shores-breaking-down-the-cyber-attack-on-stryker/
[25] https://whyy.org/articles/pennsylvania-water-authority-breach-iran-affiliated-hackers/
[26] https://www.timesofisrael.com/iran-cyberattack-on-israels-water-supply-could-have-sickened-hundreds-report/

noting that Iranian-affiliated advanced persistent threat groups had actually been observed *exploiting* the vulnerabilities on internet-connected devices.[27]

Artificial Intelligence Assisted Vulnerability Discovery and Weaponization

Frontier large language models (LLMs) have shown promise in assisting with vulnerability discovery and exploitation. In April, Anthropic announced "Project Glasswing,"[28] an initiative intended to allow a limited group of companies to test its latest model ("Mythos") on cybersecurity-related tasks. Another company, OpenAI, has announced a similar initiative.[29]

However, the Glasswing "early access" did not include a single OT or industrial control system (ICS) vendor. This is not specific to Anthropic, as most cybersecurity is biased both to information and communications technology and services (not OT/ICS) and to the largest enterprises. The goal of these initiatives is, purportedly, to give defenders time to uncover latent vulnerabilities in their systems and create patches for them before attackers have the opportunity to exploit them. However, the devices that are most closely tied to direct physical harm—including the devices used in water and wastewater systems—are largely not included. If these models, or the next iteration of them, prove capable of quickly discovering and exploiting novel vulnerabilities in OT systems, more threat actors will become capable of targeting and even damaging water systems. Further, many of the flaws that are being found may exist in open source libraries that are embedded within OT/ICS products. These dependencies are poorly understood, as their mapping pre-dates requirements for software bills of materials (SBOM).[30] As a result, even nominally *patchable* flaws may fail to be fixed in OT/ICS systems.

Given the promise of AI-assisted vulnerability discovery and exploitation, there is good reason to believe that the number of threat actors (human or otherwise) capable of disrupting water systems will soon increase dramatically. Even the availability of patches will not translate into the swift, pervasive *application* of those patches at scale, and certainly not at the speed of AI-empowered offensive operations. Many of those actors will not be nation-states, most of whom feel at least somewhat constrained by norms of responsible behavior in cyberspace, but individuals or groups trying to gain money or influence. The threat level is likely to go up significantly in the coming months; we must act urgently and decisively to protect our vital systems. These AI developments alone may tip the Internet into an environment that is "too dangerous" for large swaths of water systems, at least for the time being.

---

[27] https://www.cisa.gov/news-events/cybersecurity-advisories/aa26-097a
[28] https://www.anthropic.com/glasswing
[29] https://openai.com/index/scaling-trusted-access-for-cyber-defense/
[30] https://www.cisa.gov/sites/default/files/2025-09/joint-guidance-a-shared-vision-of-software-bill-of-materials-for-cybersecurity_508c.pdf

III. UnDisruptable27

In the face of a worsening threat landscape, policymakers and utilities alike need actionable, affordable, familiar solutions to buy down risk. I created UnDisruptable27 (U27) as an applied research project intended to create such solutions by *innovating narrowly* while ensuring our work was designed from the outset to *scale broadly*. We are midway through our pilot program.

No Water. No Hospitals. No Kidding.

U27 started with a single question: how could we best prepare communities across the country for potential disruption by Chinese threat actors? Public reporting has indicated that Chinese political leadership has set 2027 as the year when its armed forces should be prepared to seize Taiwan. If such a scenario should happen, pre-positioned access to U.S. critical infrastructure obtained by Volt Typhoon actors would be most likely to be employed by Chinese policymakers to deter U.S. involvement in a China-Taiwan conflict. While there is certainly no guarantee that 2027 will see a conflict, it begins a period of heightened risk, and we need to be prepared by bolstering our resilience.[31]

With *resilience* in mind, we next turned to prioritization. We aimed to focus on the National Critical Functions for which downtime tolerance is low enough that after 24-48 hours, they would contribute to loss of life or societal panic. Mapping against sectors, we narrowed down to energy; food and agriculture; healthcare; and water. Across these sectors, where would interventions be most useful? Where were we most vulnerable? Both the energy and healthcare sectors are regulated for cybersecurity. While the latter's regulations almost exclusively focus on confidentiality of patient data, rather than continuity of care,[32] both sectors are relatively more mature than food or water.

Next, we examined the consequences of significant disruptions in either of these more vulnerable sectors. Interfering with the food supply, while potentially devastating, could take weeks (or months) for the harm to fully materialize.[33] Even for the more damaging attacks one

[31] The most likely and most devastating timing continues to be in flux, and U27 tracks both the geopolitical situation as well as other developments that could increase the likelihood of water disruptions (such as Iran and advances in AI, discussed above).
[32] https://www.youtube.com/watch?v=8QyAQKyepcw
[33] Consider, for instance, the timing of anticipated disruption to the world fertilizer supply due to the ongoing Iran conflict.
https://www.reuters.com/world/china/iran-war-fertiliser-squeeze-could-spell-trouble-next-years-grain-harvests-2026-04-27/

could imagine, such as broadscale disruption of the cold chain,[34] stockpiles of non-perishable items and substitution would limit the immediate risk to human life. The Food and Agriculture Sector also does not have extensive overlap with other sectors. Most of the cascading effects from attacks on the food supply stem from their impact on the people who carry out critical functions, not on the critical functions themselves.

Water, in contrast, is vital for dozens of critical functions, from power generation and cooling data centers to growing food and manufacturing key products. Water is also essential to healthcare. Most hospitals can operate for two to four hours once water is cut off.[35] After that, they have to close and evacuate patients. Without HVAC in peak summer heat, that number can drop below one hour. Interruption of care and delayed care both lead to worse patient outcomes. Attacks on water utilities can start affecting worsened outcomes and even loss of life within minutes for heart conditions and an hour or few for strokes, as ambulances are re-routed to hospitals farther away.[36]

The vulnerability of these water systems and the high consequences of their failure make them attractive targets for adversaries looking to sow chaos. But even with our sector of concern identified, UnDisruptable27 still needed to prioritize further. With 53,000 public water systems, we couldn't reach them all—or even a significant fraction of them—in time.

To scope the project, we zeroed in on ensuring that water supply in the nation's 6,000 hospital towns would continue to flow to healthcare facilities, regardless of the magnitude of a cyber attack on a utility. In particular, we homed in on destructive attacks. Stopping the flow of water through a pipe is a major challenge, but destroying pipes (at scale) is a disaster.

Through manipulation of OT, a malicious cyber actor can rapidly open and close valves to cause a "water hammer," which could burst a main or junction.[37] Other inputs can do similar damage via too much (or even too little) water pressure, depending on the type and age of pipes and the time of year. Attackers could also manipulate pumps to the degree that they burn out. Heavy equipment repairs and replacements could take months—and if demand is sufficiently concurrent, because of an organized cyber campaign, full recovery could take years.

We recognized that being so specific—destructive attacks that affect hospitals— would mean that other important customers, from energy companies to communications facilities, might

[34] I studied the cold chain extensively as part of CISA's COVID Task Force. https://www.cisa.gov/sites/default/files/publications/Insights_Critical_Questions_and_Considerations_for_Cold_Chain_Storage_and_Dry_Ice_Operations.pdf
[35] https://www.nacwa.org/docs/default-source/resources---public/niac-water-report.pdf?sfvrsn=f1fac061_2
[36] https://www.nejm.org/doi/full/10.1056/nejmsa1614073
[37] https://www.youtube.com/watch?v=GnozKc3gFsM

not benefit from the same degree of resilience. But by addressing the clearest immediate risk to human life, UnDisruptable27 aims to build a methodology that can be applied to other priorities (whether dialysis centers or data centers), as appropriate.

Co-Creation on the Front Lines

With our scope identified, we needed to design pragmatic interventions that would meet our goal. Doing so required analysis of the constraints faced by water utilities that prevent them from taking action to reduce their vulnerability—or, worse, that actually increase their exposure.

Utilities Face Constraints

First, consider the information environment for utilities. With less than one percent of the community water systems participating in the primary information sharing mechanism (Water-ISAC), many owners and operators might not be aware of the threat facing them, especially as water systems do not have a history of being frequent targets. They might also not think about the fact that they could be targeted because of the downstream impacts. If a power utility is hardened against cyber intrusions, an adversary looking to take out the grid might still target a water system that provides critical cooling for the generators. We refer to this as the *education* gap.

But education does not, in and of itself, beget action. There are no national level cybersecurity requirements for water. Utilities might assume that the federal government would protect them from cyber threats and that the responsibility for dealing with foreign hackers lies elsewhere. Cybersecurity is not an issue they often hear about from their customers or from their governing bodies, whether public or private. This is the *motivation* gap.

Finally, consider the inherent asymmetry between foreign military units and water system owners and operators. The gaps in resourcing and training are both glaring and potentially insurmountable. For any one water utility in the crosshairs, it might be extremely challenging to entirely prevent a malicious actor from getting access to the system; what's more important is limiting what they're able to do with that access. But how do you do that? And is it achievable? This is the *enablement* gap.

U27 Addresses these Gaps and More...

Our approach aims to address all three of these gaps.

Education and *motivation* go hand-in-hand. When we approach a hospital community, we aim to bring both the water system and its key stakeholders—emergency managers, town planners, and the hospital itself—to the table. We then will conduct a tabletop exercise that exposes all three elements of risk: the threat of adversary activity, the vulnerability inherent in the system, and the consequences of failing to act.

The tabletop also intends to address common misconceptions that could sap motivation. We have heard sincere, but false, beliefs, including concerns over insurance coverage, durability of mutual aid agreements in a crisis, and gaps in incident response plans. Tabletops let us move beyond the scenarios simply being dismissed as peddling FUD (fear, uncertainty and doubt) and instead actually engage with the topic.

Cross-sectoral participation is critical to our success. For the water utility, having customers and elected oversight bodies in the room immediately raises the salience of the conversation. The dialogue between these different entities often exposes faulty assumptions and illuminates dependencies that are not intuitive but could prove catastrophic. Bringing together these stakeholders also serves an eminently practical purpose. In many communities, this tabletop exercise may be the *first time* that representatives from all these organizations are in the room together.

Addressing the *enablement* gap is most important to our success. To achieve this, we turned to Idaho National Laboratory (INL), a Federally Funded Research and Development Center (FFRDC). INL has pioneered the concept of Cyber-Informed Engineering (CIE),[38] which provides a framework for systems design that is cognizant of connectivity. Civil engineering projects often rely on fences, gates, and guards to protect them against misuse. A system being responsive to operators is a benefit, not a deficiency, as it's assumed that the operator is authorized to be there.

CIE challenges system designers to consider that connectivity means malicious actors may be able to get access much easier than through physical means. With an updated threat model, what changes would they make to the operations? What *engineering,* not cybersecurity, mitigations could prevent the most damaging consequences of unfettered remote access?

One example is an analog pressure arrestor. These non-connected devices are essentially "circuit breakers," preventing excessive pressure from causing permanent damage to pipes. Pressure arrestors are already used in engineering for specific circumstances.[39] CIE

[38] https://inl.gov/national-security/cie/

[39] For instance, households may use pressure arrestors to stop banging (and potential pipe damage) associated with large household appliances like washing machines.

challenges system designers to expand those arrays of circumstances to be in line with the threat environment.[40]

CIE is a framework. It does not provide prescriptive, one-size-fits-all solutions, as each community water system is different. Going from *enablement* to execution requires *co-creation*. UnDisruptable27 works directly with engineering teams to help identify risks within their systems and then develop bespoke project plans to mitigate those risks, at least with respect to the hospitals. Just last week, one of our pilot communities identified five engineering mitigations, one of which had not yet arisen in our research. Thanks to the generosity of our funder, we are even able to help purchase equipment to take a utility all the way through implementation.

...And Is Designed to Scale

Our goal with the dozen pilot communities we will work with over the life of U27 is to prove that by closing the *education*, *motivation*, and *enablement* gaps, and co-creating with utilities, we can meaningfully improve community resilience, even against threats from foreign militaries. However, there are thousands of hospital communities across the country. U27 cannot reach all of them. We know that we will need help, including from policymakers in Congress, to scale.

And that is why we have designed our approach with scaling in mind from the outset. We are committed to actually implementing solutions so that we can show future motivators—whether hospitals, grantmakers, or regulators—that it is possible for even a water utility in a small town to stand up to the Chinese army. In selecting our pilot communities, we aim to work with utilities that are not already cybersecurity experts because so few are—and a program that only works for that small fraction will never translate to a utility where the superintendent is also the groundskeeper and the IT person. We aim for small-dollar fixes because finding the political—and actual—capital for billion-dollar resilience projects is a massive undertaking in and of itself.

We also recognize that our co-creators are our best ambassadors. We lead with empathy, taking as a given that all of our stakeholders care deeply about their communities and our national security. Taking on advanced persistent cyber threat actors is daunting for anyone. We aim to empower utilities so that they feel they *can* make a difference and then lift up their voices to help their peers understand the same. This means capturing stories as we go. And it means helping our partners write the playbooks in their own language.

---

[40] INL has been providing CIE for water training at several U27 events. One of our volunteers co-authored an entire book on using CIE for water: "Resilience Through Cyber-Informed Engineering: An Engineering and Operations Approach to Cybersecurity" by Andrew Ohrt, PE, CISSP and Daniell Groves, PE, CISSP,

We also look for opportunities to help communities continue on their cybersecurity journeys. Engineering mitigations are a first step, but as organizations mature, they may benefit from other initiatives, including support from Cyber Resilience Corps volunteers,[41] participation in the DEF CON Franklin initiative,[42] or practices shared at the annual Critical Effect conference we co-sponsor.[43]

Lessons for Cybersecurity Research

Cybersecurity research often focuses on technical solutions. It aims to better detect anomalous behavior, discover and patch new vulnerabilities, or more securely verify identity.

Yet in devising and now implementing U27, we have several salient observations about where additional cybersecurity research efforts will be useful:

- **Prioritize Target Rich, Cyber Poor Sectors**[44] - Technical solutions can take years—or decades—to make it from the cyber "haves," well-resourced sectors like financial services, to the "have nots." Yet water utilities are uniquely vulnerable and increasingly targeted. Research programs should explicitly consider how projects will translate to lifeline services that are both essential and under-resourced.
- **Secure-By Solutions Aren't Just in Software** - One of our consistent findings has been that tried and true *engineering* fixes can dramatically reduce cyber risk. Rather than focusing myopically on how to raise "cyber shields up", research should also explore how to effectively bring "connections down," or at least to "engineer down" the consequences. This also means that research must go beyond "best practices" to fit-for-purpose solutions for OT/ICS and lifeline functions. Most security practices are implicitly biased to *confidentiality* of data, not the *availability* of the systems.
- **Incentives Are Key** - In our research, we started by examining the *education*, *motivation*, and *enablement* gaps. Too often, solutions stop with resources or tools that start and end with just the first of these. While well-meaning, efforts to educate utilities about general cybersecurity best practices or the specific risks they face have come up short.[45] Research projects should consider the *economics* of cybersecurity, not simply technical controls. In some cases, we are incentivizing more exposure.

---

[41] https://cltc.berkeley.edu/program/cyber-resilience-corps/
[42] https://defconfranklin.com/
[43] https://securityandtechnology.org/event/critical-effect-2026/
[44] https://www.help.senate.gov/imo/media/doc/Corman.pdf
[45] "[F]ree cybersecurity resources alone rarely translate into operational improvements." https://cyberreadinessinstitute.org/news-and-events/beyond-the-tap-scaling-cyber-readiness-across-critical-infrastructure/

- **Design with Scale in Mind** - Cyberspace keeps growing. New devices—and classes of devices—are connected all the time. Generative AI has led to predictions that the amount of computer code will increase by an order of magnitude over the next several years.[46] Cybersecurity solutions that only work under very limited circumstances (e.g., having an expert on staff) are not solutions at all.
- **Cascading Effects Are a Force Multiplier** - The technical changes we are making through U27 are solely for water utilities. Yet, if our pilots are successful, most of the benefits will accrue to hospitals. Understanding how failures of critical functions cascade across sectors is the only way to grasp the true consequence of a cyber incident. Bringing in additional stakeholders can also add demand (and support) for change.
- **Don't Fight the Last War** - We chose to focus on water not because it has a history of being attacked but because there is strong evidence that the threat actors are moving into the sector. Research is inherently forward-looking; priorities must be set based on what we expect going forward, not simply what we know has already happened. This is particularly relevant when considering how advances in AI may upend long-held cybersecurity assumptions.

These are some of our preliminary findings as we continue to move through our pilot utilities. We remain open for nominations of hospital communities. Nominations can be submitted by emailing undisruptable27@securityandtechnology.org.

IV. Recommendations for Congress

This Committee plays an important role in the Congressional cybersecurity ecosystem. We have several recommendations on how to ensure federal research and development efforts meet the needs of water utilities.

Specific to the water sector, the Committee should:

- **Systems Engineering** - The Committee should consider creating or supporting programs in systems engineering that are specifically designed to reduce national security and public safety risk. These programs should apply tools like Idaho National Laboratory's Cyber Informed Engineering and reflect lessons learned from the U27 project and the CISA COVID Task Force.[47]
- **Incorporate EPA** - The Environmental Protection Agency (EPA) is the Sector Risk Management Agency for the Water and Wastewater Systems Sector. The Committee should ensure that EPA staff performing SRMA functions have input into cybersecurity

[46] https://www.nytimes.com/2026/04/06/technology/ai-code-overload.html
[47] https://www.youtube.com/watch?v=XrSVXbWGZHw

and resilience research agendas. The Committee should also consider ways to ensure the Sector Coordinating Council, comprising utility owners and operators, also can share views. Co-creation encourages buy-in and increases the relevance of applied research to the needs of the operators.

There are also broader recommendations for the scientific establishment that will benefit water in addition to other sectors. The Committee should:

- **Threat Modeling** - The Committee should require that program managers awarding funding for cybersecurity research and development participate in regular threat modeling exercises (both at the water system level and with the communities they support - "No Water, No Hospital"). Rigorous threat modeling can shape notices of funding opportunity and ensure they are relevant for an evolving risk landscape.
- **Social, Behavioral, and Economic Research** - Social, behavioral, and economic research is foundational to closing the motivation gap we identified in the initial phase of U27. The Committee should create an interdisciplinary research program, jointly managed by the Directorate for Computer and Information Science and Engineering and the Directorate for Social, Behavioral and Economic Sciences, to examine cybersecurity economics, particularly with respect to implementing technical controls or improving resilience.
- **Cross-sector Dependency Mapping** - The Committee should create or support programs that examine cross-sector dependency mapping, including detailed examinations of supply chains. This dependency mapping serves several important functions. For example, few knew the name Change Healthcare until its ransom disrupted operations at 74 percent of hospitals and disrupted cashflow at 94 percent of them.[48] I designed a cross-sector dependency mapping effort for Operation Warp Speed, and those methods could be applied here. They improve planning by illuminating common suppliers that could pose systemic risk. They also help to more accurately measure the consequences of failure, which in turn improves cost-benefit analyses for investments in cybersecurity and resilience.
- **Cyber Clinics**[49] - Cybersecurity clinics, supported by the Consortium of Cybersecurity Clinics, currently provide hands-on support to under-resourced organizations across 29 states. These clinics offer free assistance to community organizations that otherwise could not afford it, including non-profits, cities, schools, hospitals, and small utilities. This assistance ranges from strategic advice, like cyber risk assessments and policy writing, to more hands-on activities like vulnerability scanning and penetration testing. Clinics are often associated with research universities and can provide a

[48] https://www.aha.org/change-healthcare-cyberattack-underscores-urgent-need-strengthen-cyber-preparedness-individual-health-care-organizations-and
[49] https://cybersecurityclinics.org/

valuable teaching tool for students studying the cybersecurity aspects of a range of disciplines. The Committee should support innovative workforce programs, like clinics, that both train students and provide tangible benefits to their communities.

- **Data Generation** - The Committee should consider supporting research projects that focus on generating empirical data to guide future R&D efforts, including social, behavioral, and economic research. In particular, the Committee should consider supporting research programs aimed at conducting regular, anonymized cyber censuses that snapshot the current health of the ecosystem and give an important baseline to measure improvements against and to identify key gaps for further exploration.

Finally, while not directly within this Committee's jurisdiction, we urge members to work with their colleagues to:

- **Pass Long-term or Permanent Extensions of Cybersecurity Authorities** - In particular, Congress should reauthorize:
    - **The Cybersecurity Information Sharing Act of 2015**, which expires on September 30, 2026, and which enables the free flow of cyber threat indicators among the private sector and between the private sector and government.
    - **The State and Local Cybersecurity Improvement Act of 2021**, which expires on September 30, 2026, and which provides assistance to state, local, Tribal, and territorial governments to develop and execute against strategies to improve their cybersecurity.
- **Support Appropriations for Water Cybersecurity** - In particular, Congress should:
    - **Fully fund State and Tribal Assistance Grants for cybersecurity** in the President's Fiscal Year 2027 budget request. The Drinking Water System Infrastructure Resilience and Sustainability Program includes a new request for $10,000,000 to further enhance system resilience, including cyber security improvements.[50]
    - **Fund the State and Local Cybersecurity Grant Program.** Even with its temporarily extended authorization, no funds are currently appropriated to support this program.
    - **Support the expansion of the Water ISAC** - Funding can help expand ISAC membership, particularly to smaller utilities. Although sustainable funding will likely need to come from within the sector, seed money from Congress can help catalyze participation and the initial development of fit-for-purpose content that will be relevant further down-market.

[50] https://www.epa.gov/system/files/documents/2026-04/epa-fy27-congressional-justification.pdf

- **Codify the Critical Infrastructure Partnership Advisory Council (CIPAC)** - It is essential that non-federal critical infrastructure owners and operators have mechanisms to offer candid feedback to their U.S. government partners with respect to cybersecurity and resilience policy. Congress should pass legislation amending Section 9002 of the Fiscal Year 2021 National Defense Authorization Act to codify the CISA Director's ability to convene critical infrastructure providers, including in the water sector, rather than relying on the broad authority of the Secretary of Homeland Security.

America's success is built on a foundation of innovation. We must carry on that legacy in the realm of water cybersecurity. The threats are dire and the consequences grave. But I have faith that Congress will continue to advance meaningful, non-partisan legislation that brings the country together to tackle this core issue of national security and public safety. At IST, we welcome the opportunity to continue to engage with you and your colleagues. Thank you again for the invitation to testify.