WIDENING THE APERTURE PART III

Installation – Community Cooperation Against Cyber Threats

OCTOBER 2026

ASSOCIATION OF DEFENSE COMMUNITIES | Matrix

ACKNOWLEDGEMENTS

Authors

Peter Keiser, Matrix Design Group

Sal Nodjomian, Matrix Design Group

Brad Johnson, Matrix Design Group

Charlie Perham, Matrix Design Group

Eric Turner, Matrix Design Group

Editor

Alyssa Evans, Association of Defense Communities

Layout

Will Noonan, Association of Defense Communities

CREDITS

Front Cover: Photo by Sgt. 1st Class Benjamin Crane

Page 2: Photo by Josef Cole

Page 4: Photo by Sgt. 1st Class Mireille Merilice-Roberts

Page 6: Photo by Spc. Christ-Claude Mowandza-Ndinga

Page 8: Photo by Airman 1st Class Devyn Waits

Page 11: Photo by Master Sgt. David Eichaker

Page 14: Photo by Sgt. 1st Class Andrew Mallett

The appearance of U.S. Department of War visual information does not imply or constitute DOW endorsement.

CONTENTS

Introduction 4

The Nature of the Threat 5

The Policies of Cyber Defenses 7

Solutions — What Does Success Look Like? 8

Increase Cyber Hygiene: 9

Plan and Prepare for the Worst 10

Build Talent and Capacity 11

Support and Contribute to High-Value State-Led Initiatives 12

A Note on Resourcing 12

Conclusion 14

INTRODUCTION

Any national defense stakeholder following the news recently has undoubtedly been swamped with analyses of airpower, economic security, and naval force projection. However, cybersecurity and cyber defense have received much less coverage despite being equally relevant to the current conflict in the Middle East and equally critical to our national security. In April 2026, in between headlines on a heroic rescue of downed aviators in Iran, a Joint Cybersecurity Advisory bulletin was issued by six federal agencies and departments. The Advisory provided an "urgent warning" that Iran-affiliated actors are successfully engaging in cyber exploitation of internet-connected devices, particularly specific brands of industrial computers "deployed across multiple U.S. crucial infrastructure sectors (including Government Services and Facilities, and Water and Wastewater Systems and Energy sectors) within a wide variety of industrial automation processes."[1] This Advisory is a representation of a disturbing truth: individuals and organizations linked to U.S. adversaries are constantly developing and deploying complex tools and methods in cyberspace to attack defense and other critical infrastructure on U.S. soil.

The potential for these kinds of cyberattacks represents an emergent threat to our defense installations and their partner communities for two reasons. First, the cyber threat is evolving at the same rapid pace as artificial intelligence (AI), and other complex modern technology and defense communities will need to take active measures to prevent them. Second, because cyber threats only require an internet connection to turn hostile intent into reality, they transcend the physical security barriers and fence lines that have traditionally protected military installations and defense assets. Similarly to combating drones that can simply fly over a "hard" target, countering cyber threats will require shifts in the way defenses are built around our most critical assets and how we think about those defenses.

This article provides an in-depth, unclassified start to the discussion of cyber-based emergent threats and the cybersecurity challenges that defense communities and their partner military installations share. This discussion begins with an overview of relevant cybersecurity topics and an explanation of why cyber threats must be considered emergent threats of high importance in defense-related contexts. Next comes a brief analysis of how current Department of Defense (DOD) and Department of Homeland Security (DHS) policies are aligned to combat cyber threats, followed by case study-style examination of actions that are currently moving the needle on cyber defense in defense communities and other municipalities across the country. The article closes by exploring possible pathways for installation-community partnerships to meet shared cyber-related challenges.

1 Federal Bureau of Investigation, Cybersecurity and Infrastructure Security Agency, National Security Agency, Environmental Protection Agency, Department of Energy, United States Cyber Command – Cyber National Mission Force. (2026). *Joint Cybersecurity Advisory: Iranian-Affiliated Cyber Actors Exploit Programmable Logic Controllers Across US Critical Infrastructure*. Product ID: AA26-097A.

THE NATURE OF THE THREAT

Key Takeaways:

- **The rise of Software as a Service (SaaS) and use of third-party applications with data-sharing abilities have created major cybersecurity challenges for both government agencies and defense industry corporations.**
- **Cyberattacks are increasingly sophisticated and more frequent across the U.S., particularly against dual-use infrastructure that supports both civilian communities and U.S. military installations.**

At first glance, it may be difficult to see why cyber threats should be classified as emergent. After all, the first documented "hack" of a computer occurred in 1962, and the French Resistance executed attacks on data fed into Nazi punched card computers in 1940.[2]

If computers, hacking, and digital security have been normalized in our society for a generation, why are the threats presented by cyberattacks suddenly so pronounced and urgent?

The answer lies in the way digital infrastructure has evolved over the past two decades, particularly concerning the Internet of Things (IoT) and Software as a Service (SaaS).

IoT is a term used to describe devices and systems that are linked together by an internet network. As more internet-capable devices are brought online and linked to each other, IoT expands. This logic has drastically impacted both industrial and military capabilities. Production lines are increasingly interlinked and automated with some factories customized for automated networks to the point that they don't need lights for human workers.[3] On the battlefields of eastern Ukraine, internet connections enable drones, artillery targeting systems, and communications devices. Elon Musk's decision to block Russian forces' access to Starlink internet terminals was widely reported as a major disruption to Russian units, which were forced to scramble for alternative products to facilitate their internet-based command and control systems.[4]

Having internet-linked networked systems is not bad, especially considering how the networks can enhance productivity and ease communication. However, the modern methods by which these networked systems are created and linked are problematic. Over the past 10 years, the use of SaaS products (products that are predominately cloud-based software tools provided to a user by an application or browser) has exploded to establish them as key tools of virtually every organization. Common SaaS examples are Slack, Zoom, Teams, Salesforce, and Docusign; but also include Netflix, Amazon Web Services, and countless other subscription-based products we utilize in our professional and private lives every day. A recent report indicated that private companies in the U.S. used an average of 106 SaaS products in 2024, slightly less than a peak of 130 in 2022, but significantly more than the average of just 16 products in 2018.[5]

The SaaS-driven expansion of the IoT is problematic because it severely degrades the old firewall-based safeguards that traditionally protect Operational Technology (OT), defined as the software and hardware that control physical devices. As James Dempsey and Andrew Grotto of Stanford University stated in an excellent article from The Cyber Defense Review, "Traditionally

2 Trampski, H. (2024). *How much do you know about the history of cybersecurity?* Purdue.edu. https://cyber.tap.purdue.edu/blog/articles/how-much-do-you-know-about-the-history-of-cybersecurity/.

3 The Tech Enabling China's "Dark Factories." (2025, August). Industrial Equipment News. https://www.ien.com/redzone/blog/22948773/the-tech-enabling-chinas-dark-factories.

4 Adams, P. (2026, February 19). *Musk cuts Starlink access for Russian forces, giving Ukraine an edge at the front*. https://www.bbc.com/news/articles/c0q3ndj7052o.

5 Robb, N. (2025, October 3). *The big list of 2025 SaaS statistics that you should know*. BetterCloud. https://www.bettercloud.com/monitor/saas-statistics/.

OT devices had no connectivity and the air gap between OT and an enterprise's information technology infrastructure was relied on as the primary guarantor of OT security … Many OT systems are now routinely connected to corporate networks … making components discoverable by attackers."[6]

Stated differently, the key question is: if a business or critical infrastructure provider depends on a subscription to a third-party app that is integrated into its systems and process, how does it maintain separation between its critical data and potential intruders? More distressingly, SaaS content is commonly developed or enabled by third-party content, often to ensure essential platform integration functionality.[7] This creates situations by which an organization's SaaS app may have access to critical data, and critical code within that SaaS app may have been developed by a completely separate third-party actor that may or may not be fully known by the SaaS provider. Because the same issues with third-party code and content use exist in AI models, the AI boom has further potential to create concerns surrounding external supply chains in cyber platforms.

Key Terms

Internet of Things: internet-capable devices and physical objects — things — containing embedded software and connected to a network, allowing them to share and collect data

SaaS: Software as a Service, a cloud-based software delivery model where individuals and organizations subscribe to applications rather than purchasing them and installing them locally

Supply Chain Attack: a cyberattack that uses a less-secure third-party tool or service to exploit a target network

Ransomware: malicious software (malware) that encrypts sensitive data and demands a ransom payment for the user to regain access

Operational Technology (OT): hardware and software that directly control physical devices and infrastructure

While SaaS programs and other third-party-reliant software make cybersecurity more complex and difficult to administer, hackers and adversaries have grown in sophistication and can take advantage of the higher bar for successful cyber defense. Recent cases demonstrate the operational difficulties of the modern cybersecurity landscape and the effect cyberattacks can have on military-related infrastructure. One widely reported incident was the 2020 SolarWinds attack. This attack was a large-scale effort perpetrated by Russian Foreign Intelligence Service hackers who injected hidden code into the SolarWinds Orion Platform suite of software products. These products were employed by the U.S. government and various defense industry companies. SolarWinds included

6 Dempsey, J. and Grotto, A. *Ensuring the Cyber Resilience of Critical Infrastructure Serving Domestic Military Installations*. (2025, November 28). The Cyber Defense Review. 2025, VOL. 10, NO. 2, 115-138.

7 Woodring, B. *What Are Third-Party Integrations and Why are They Essential?* | Prismatic. (2024, February 29). Prismatic.io. https://prismatic.io/blog/third-party-integrations/.

the hidden code in a regular update to its Orion products, effectively providing the Russian hackers with access to private and government networks through the corrupted software.[8] This Supply Chain Attack affected a total of 18,000 organizations including numerous government agencies,[9] and U.S. companies that were impacted reportedly lost an average of 14% of annual revenue10 in damage control and mitigation costs.

Other incidents, such as the 2024 attack on the Seattle-Tacoma International Airport, have affected dual-use military and civilian infrastructure. Similarly, in July 2026, the FBI issued a warning bulletin addressing numerous cyberattacks on water and wastewater systems across the country.11

Perhaps most critically, cyberattacks are becoming more frequent and weaponized against specific industry targets. Iranian attacks against U.S. government and defense industry targets surged after the U.S. and Israel began airstrikes in Iran this year with a notable success against the major medical-technology firm Stryker.12 With these attacks increasing, the capabilities of adversaries expanding, and the pace of technological growth continuously growing, it is vital for entities at all levels secure critical infrastructure and industries, particularly those that bridge the gap between military entities and their civilian support systems.

THE POLICIES OF CYBER DEFENSES

Key Takeaways:

- **The Department of Homeland Security (DHS) is the lead agency in most cybersecurity matters relevant to installation-community partnerships.**
- **President Donald Trump's Cyber Strategy for America provides the current focus on cybersecurity policy via six policy pillars for action across government and industry.**

Any discussion of responses to the cybersecurity challenges described above must acknowledge that it is unrealistic at this time to expect SaaS practices and the IoT to fundamentally change. Our nation, the world's major industries, and mainstream society at large have adopted these products and methods, and it's far too late to put that genie back in its bottle. With this in mind, there are plenty of proactive actions that installation-community partnerships can take to safeguard against cyberattacks on shared infrastructure or critical data. Although DHS is the primary cybersecurity coordination agency in the U.S. government, a variety of federal agencies help shape relevant cybersecurity standards for U.S. communities, and their guidance can serve as a starting point for these actions. These agencies include:

Cybersecurity and Infrastructure Security Agency (CISA): This agency, housed within DHS, is the primary lead for domestic cybersecurity including infrastructure protection.

8 GAO. (2021, April 22). *SolarWinds cyberattack demands significant federal and private-sector response*. www.gao.gov; U.S. Government Accountability Office. https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic.

9 Tahir. (2024, November 17). *The SolarWinds Hack: Implications, Lessons, and Future Cybersecurity Strategy*. Medium. https://medium.com/@tahirbalarabe2/the-solarwinds-hack-implications-lessons-and-future-cybersecurity-strategy-08a0afa48637.

10 *SolarWinds Supply Chain Attack*. (2025). Fortinet. https://www.fortinet.com/resources/cyberglossary/solarwinds-cyber-attack.

11 *Malicious Cyber Actors Targeting Water and Wastewater Sector Internet- Facing Programmable Logic Controllers, Causing Operational Disruptions*. (2026, July 30). Federal Bureau of Investigation. https://www.fbi.gov/investigate/cyber/alerts/2026/malicious-cyber-actors-targeting-water-and-wastewater-sector-internet--facing-programmable-logic-controllers-causing-operational-disruptions.

12 Rundle, J. and Volz, D. (2026, March 11). *Iran Expands War with Major Cyberattack Against U.S. Company.* The Wall Street Journal. https://www.wsj.com/articles/stryker-hit-with-suspected-iran-linked-cyberattack-52f6615c.

Federal Bureau of Investigation (FBI): The lead investigative agency for cyberattacks and criminal activity in cyberspace.

National Institute of Standards and Technology (NIST): Per an Executive Order published on June 6, 2025,[13] NIST, within the Department of Commerce, is tasked with developing cybersecurity and privacy standards and resources for federal agencies, industry, and the public.

U.S. Cyber Command (USCYBERCOM): One of 11 unified combatant commands within the DOD, its mission is to integrate DOD cyberspace capabilities and operations.

The centralization of most federal cybersecurity authorities within DHS provides a positive outlook for installation-community partnerships seeking to improve their cybersecurity capabilities and readiness. Unlike needing to sort through the various authorities involved in combating emergent threats from drones (discussed in the previous article in this series), installation-community partnerships can confidently prioritize DHS resources and funding sources to develop actions against cyber threats and coordinate defenses on either side of the fence line.

The other significant document that should guide any discussion of installation-community cybersecurity progress is Trump's Cyber Strategy for America. Published in March 2026, this document outlines the current federal approach to defending U.S. interests in cyberspace. This document is arranged around six policy pillars,[14] providing guidance for federal departments, defense industry and academia organizations, and more general principles for action in cybersecurity.

Much of the guidance from these agencies is applicable to larger-scale cybersecurity efforts which installation-community partnerships are not equipped to take on. However, they provide valuable starting points for installation-community partnerships and aligned municipalities to consider.

SOLUTIONS — WHAT DOES SUCCESS LOOK LIKE?

Key Takeaways:

- **Current events demonstrate that municipal organizations must be prepared to confront cyber attacks on their networks.**
- **Installation-community partnerships should focus their cybersecurity support actions on assisting in developing specific solutions that address individual localities, companies, or systems.**

Because of the need to fund and provide structure for complex requirements, many initiatives to improve cybersecurity originate at the state level. However, there are a variety of proactive actions that can be accomplished by localities with support from installation-community partnerships and similar municipal or county-level organizations. These actions include:

13 *Sustaining Select Efforts to Strengthen the Nation's Cybersecurity and Amending Executive Order 13694 and Executive Order 14144.* (2025, June 6). The White House. https://www.whitehouse.gov/presidential-actions/2025/06/sustaining-select-efforts-to-strengthen-the-nations-cybersecurity-and-amending-executive-order-13694-and-executive-order-14144/.

14 *President Trump's Cyber Strategy for America.* (2026, March). The White House. https://www.whitehouse.gov/releases/2026/03/white-house-unveils-president-trumps-cyber-strategy-for-america/.

Increase Cyber Hygiene:

Cyber hygiene is a blanket term which refers to the health of networks, devices, and IT infrastructure. Common practices include requirements for multi-factor authentication, regular updates and data backups for IT systems, and encryption for internal networks and Wi-Fi. Responsible cyber hygiene has proven to be effective in countering most basic threats, so much so that CISA provides various free cyber hygiene vulnerability assessments to SLTT government entities and non-governmental organizations.[15] While often not flashy nor groundbreaking, simple actions to establish and maintain cyber hygiene provide disproportionate value to front-line cyber defense.

Case Study: Newport News strengthens cybersecurity for joint-use water infrastructure.[16] In August 2026, the city of Newport News, Virginia; home to Joint Base Langley-Eustis; announced a $6 million investment in cybersecurity upgrades for the Newport News Waterworks: a utility provider for nearly 500,000 residents of the Virginia peninsula and multiple regional military installations. This investment will update the utility's IT infrastructure, establish increased multi-factor authentication standards and fund other improvements in accordance with FBI recommendations for cyber hygiene. Newport News also appointed a Chief Information Officer (CIO) and Chief Technology Officer (CTO) to provide centralized governance and coordination across its IT infrastructure and policies. These proactive actions were partly taken in response to a series of cyberattacks which specifically targeted over 30 municipal-level water systems across Minnesota earlier in the summer[17] With these actions, Newport News demonstrated dedication to proactive action in securing critical joint-use infrastructure.

Case Study: Pennington County rebuilds systems to last.[18] Pennington County, South Dakota, home of Ellsworth Air Force Base, suffered a massive cybersecurity attack in July 2026 which disrupted nearly every government system and forced many to shut down. In response to the attack, the county has dedicated resources to rebuilding its entire IT infrastructure, using a variety of state and federal best practices to increase its resiliency against future incidents. Major cyber hygiene improvements included in this rebuild include adopting a .gov suffix for county operating systems (thereby complying with top-tier federal cybersecurity standards and requirements) and establishing a Security Information and Event Management (SIEM) system, a CISA-approved best practice for collating and visualizing cybersecurity data.[19] The county is conducting a robust after-action process and intends to release a full report by the one-year anniversary of the attack.[20] While unfortunate that Pennington County suffered a significant cybersecurity incident, by rebuilding its IT systems from the ground up, the county shows its intent to fortify its data and operations against future cyberattacks.

15 CISA. (n.d.). *Cyber Hygiene Services | CISA*. Www.Cisa.Gov. Retrieved October 7, 2026, from https://www.cisa.gov/cyber-hygiene-services.

16 Anstaett, C. (2026, August 12). *Newport News spending more than $6 million to protect water supply from cyber attacks.* News 3 WTKR Norfolk. https://www.wtkr.com/news/in-the-community/newport-news/newport-news-spending-more-than-6-million-to-protect-water-supply-from-cyber-attacks.

17 Marohn, K. (2026, August 4). *Cyberattacks in Minnesota expose vulnerability of U.S. water systems*. MPR News. https://www.mprnews.org/story/2026/08/04/water-system-cyberattacks-in-minnesota-expose-us-vulnerability.

18 Pfankuch, B. (2026, October 5). *Lessons learned from recent SD cyberattacks*. South Dakota News Watch. https://www.sdnewswatch.org/south-dakota-pennington-county-cyberattack-ransomware/.

19 *Guidance for SIEM and SOAR Implementation | CISA*. (2025, May 27). Cybersecurity and Infrastructure Security Agency CISA. https://www.cisa.gov/resources-tools/resources/guidance-siem-and-soar-implementation.

20 Mitchell, R. (2026, September 24). *Pennington County Commission provide updates in cybersecurity incident.* Rapid City NewsCenter1. https://www.newscenter1.tv/news/pennington-county-commission-provide-updates-in-cybersecurity-incident.

Plan and Prepare for the Worst

There are limits to what local governments and installation-community partnerships can do to prevent cyberattacks, especially considering the growing capabilities of cyber adversaries. Where localities and local-level entities have the most advantage is in pre-incident planning and incident procedures. All public and private stakeholders in critical systems should design IT systems and infrastructure with the assumption that they will be tested by cyberattacks, not that they might be tested. Regular exercises, audits, and stress tests will assist in making certain these designs response procedures are as robust and effective as possible.

Case Study: Barnstable County's partnerships model pays dividends. Barnstable County, Massachusetts, covers the state's Cape Cod region including Joint Base Cape Cod, a conglomerate of various National Guard installations. The county recently received national recognition for its cybersecurity practices, taking third place in its population group in the 2026 Digital Counties Survey for cybersecurity and technology-based innovation.[21] The county was specifically recognized for its ability to coordinate IT and cybersecurity support for multiple municipals via a structure of inter-municipal contracts. This structure allowed the county to provide support to the town of Bourne, Massachusetts, during a cyberattack in 2025, despite Bourne not possessing dedicated IT personnel of its own. While the attack disrupted some city systems, all emergency response networks and communications remained operational, and no significant negative effects occurred.[22] With these agreements in place and mutually supportive cyber infrastructure managed at the county level, Barnstable County and its municipalities remain protected from cyber threats despite the county's comparatively low number of dedicated personnel and resources.[23]

Case Study: Louisiana National Guard (LANG) supports small-scale training with local power suppliers. Large-scale, state and regional exercises provide great value in testing overarching cybersecurity practices and promoting coordination between various levels of government agencies. However, smaller-scale exercises with local focus should not be overlooked. Smaller partnerships and less-complex exercises provide stakeholders below the state and federal levels with the training and experience they need to be a responsive and effective first line of defense in a cyberattack against shared military-civilian infrastructure. A prime example of these smaller-scale exercises is LANG's actions in a 2017 training seminar. LANG's specialty cyber formations partnered with Louisiana power supplier CLECO to simulate cyber threat detection and response. This direct coordination of military personnel with civilian networks is highly beneficial because it provides military cyber specialists with firsthand familiarity with the networks they would be called upon to assist in the case of a major cyberattack on critical infrastructure. Events such as this are crucial readiness-building activities since they circumvent military-civilian language barriers and train cybersecurity experts on the systems and processes of non-federal networks in realistic settings.[24]

21 *The Transaction Costs of Municipal Cyber Risk Management*. (n.d.). Retrieved October 7, 2026, from https://cltc.berkeley.edu/wp-content/uploads/2024/04/Transaction-Costs-of-Municipal-Cyber-Risk-Management.pdf.

22 PERKINS, J. (2025, January 16). *Bourne Cyberattack: Here's What We Know.* CapeNews.Net. https://www.capenews.net/bourne/news/bourne-cyberattack-heres-what-we-know/article_2e017b1c-d400-11ef-98db-83a27da106a7.html.

23 Editorial Staff. (2026, July 15). *Digital Counties 2026: 150,000-249,999 Population Category.* GovTech. https://www.govtech.com/digital-counties-2026-150-000-249-999-population-category.

24 Dipuma, S. G. (2017). *La. National Guard trains with local power company on cyber defense*. Dvids. https://www.dvidshub.net/news/230115/la-national-guard-trains-with-local-power-company-cyber-defense.

Build Talent and Capacity

A significant concern of cyber policymakers is the ability of the nation's cybersecurity workforce to fill the growing cybersecurity needs of both public and private industry. According to 2024 data from the nonprofit International Information System Security Certification Consortium (ISC2), the worldwide workforce gap stood at 4.8 million cybersecurity professionals.[25] This gap naturally has a disproportionate effect on more technologically developed nations such as the U.S. Additionally, more recent reports have cited a skills gap in the cybersecurity workforce, raising the possibility that a larger redesign of training programs and curricula is more critical than simply raising the output of cybersecurity professionals into the workforce.[26]

Installation-community partnerships can be part of the solution to this issue. These organizations have an outstanding track record of supporting workforce development initiatives across a wide range of industries and professions. By acting as links between military and defense entities, employers, academia, and policymakers, installation-community partnerships can help activate networks to train, retain, and upskill the workforce required to provide cybersecurity in both the private and public sectors.

Case Study: San Diego Cyber Clinic trains workforce and services its community.[27] The San Diego Cyber Clinic is a partnership between multiple universities and private industry including Google. The clinic, which celebrated its first anniversary in October 2025, provides hands-on training to upcoming cybersecurity professionals by offering cybersecurity services free of charge to local industries, filling vulnerabilities in cyber infrastructure while enabling practical application of skills. Cyber clinics such as the San Diego Cyber Clinic have been compared to free medical or law clinics offered by some universities, and are an excellent system to provide workforce training and assist in filling critical needs in local communities.

Case Study: Louisiana State University's (LSU) unique application of cybersecurity training directly supports the petroleum industry.[28] LSU is taking advantage of the unique combination of capabilities and programs offered at its campus to expand its cybersecurity training programs, specifically in the critical energy infrastructure field. Because the campus already has a significant petroleum lab, policymakers are supporting the development of a specialty cyber test range called The Tiger Skid to assess vulnerabilities in real-world petroleum equipment. The potential benefits of this training and research are significant enough that CISA is directly engaged in developing a curriculum and securing funding for the program. This effort is a key example of the wide range of possibilities that can provide specialty training in cybersecurity and infrastructure protection, and fill specific needs of individual localities or industries.

25 Pfankuch, B. (2026, October 5). *Lessons learned from recent SD cyberattacks*. South Dakota News Watch. https://www.sdnewswatch.org/south-dakota-pennington-county-cyberattack-ransomware/.

26 *Guidance for SIEM and SOAR Implementation* | CISA. (2025, May 27). Cybersecurity and Infrastructure Security Agency CISA. https://www.cisa.gov/resources-tools/resources/guidance-siem-and-soar-implementation.

27 Team, S.N. (2025, October 20). *San Diego Cyber Clinic celebrates first anniversary*. San Deigo State University News. https://www.sdsu.edu/news/2025/10/san-diego-cyber-clinic-celebrates.

28 *"A Slam Dunk": LSU Emerges as National Leader in Cyber for Critical Infrastructure*. (2025). Louisiana State University. https://www.lsu.edu/blog/2025/07/wfl-tiger-skid.php.

Support and Contribute to High-Value State-Led Initiatives

Many states have established efforts that actively contribute to cybersecurity improvements within their borders and beyond. Higher profile efforts include regular statewide tabletop exercises, and forums or conferences meant to promote discussion between private and public entities. These are excellent actions and should be continued, but there are additional examples of innovative state efforts that specifically contribute to municipal and county-level cybersecurity development. Installation-community partnerships have an opportunity to research these innovative best practices that are occurring across the country and advocate for appropriate, specialized support to address specific local concerns or resource cybersecurity enhancements that would otherwise be out of reach for localities.

Case Study: North Carolina's comprehensive contracting methods provide cybersecurity tools for localities.[29] In 2024, the North Carolina Department of Information Technology (NCDIT) debuted a contracting vehicle designed to ease the procurement processes for cybersecurity products across its local government partners. NCDIT designed the procurement vehicle to resource tools in bulk, allowing the state to then pass on the tools to individual agencies and localities at a lower price point. Specialty contracts such as this provide localities and municipal partners with pathways to access cybersecurity technology that would otherwise be out of reach due to funding or acquisition complexity. They can also enable standardized technology across their areas of influence, easing future reporting and incident response processes.

Case Study: Connecticut Cyber Assessment Teams shore up cyber defense for local infrastructure.[30] In January 2025, Connecticut launched a specially designated Joint Cyber Team consisting of hand-selected members of the state's National Guard. This team coordinates with localities across the state to perform assessments of cybersecurity at public sites such as health districts, water and wastewater facilities, schools, and local governments. The process not only provides immediate enhancements to cybersecurity infrastructure, but also allows for training opportunities for local IT staff, and furnishes localities with the basis to apply for select federal and state grants to make additional improvements against cyber threats. Within its first two months of operations, the Joint Cyber Team had completed 39 assessments and booked another 40.

A NOTE ON RESOURCING

As with most installation-community partnership initiatives, resourcing and funding limitations restrict the ability of local stakeholders to coordinate cybersecurity solutions. However, multiple federal and non-federal sources are available for installation-community partnerships seeking funding for local cybersecurity enhancement or vulnerability mitigation projects. The following list provides starting recommendations for defense communities in need of funding or other resources for efforts related to cybersecurity and cyber defense:

Department of Homeland Security Resources

State and Local Cybersecurity Grant Program:[31] This program represents the most significant opportunity for local governments seeking to improve their cyber infrastructure

29 Rueter, T. (2024, September 27). *What Do Cities and Counties Get from Whole-of-State Cyber?* GovTech. https://www.govtech.com/security/what-do-cities-and-counties-get-from-whole-of-state-cyber.

30 Vega, D. *CT Cyber Team begins cybersecurity assessments*. (2025, January 16). Connecticut National Guard. https://ct.ng.mil/News/Article/4031696/ct-cyber-team-begins-cybersecurity-assessments/.

31 *State and Local Cybersecurity Grant Program.* (n.d.). Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/cybergrants/slcgp.

and best practices. Available for state, local, tribal and territorial (SLTT) governments, the program allocates funds for implementation of cyber governance and planning, capabilities assessments, vulnerabilities mitigation, and cyber workforce initiatives. CISA serves as the program manager for grant awards while the Federal Emergency Management Agency (FEMA) is tasked with grant administration and oversight of funds.

Tribal Cybersecurity Grant Program:[32] This is an independent offshoot of the State and Local Cybersecurity Grant Program that was established in 2023. Its objectives are largely identical to those of the State and Local Cybersecurity Grant Program, but funding is specifically targeted toward tribal governments.

Other CISA and DHS Resources: Although not funding vehicles, CISA and other agencies within DHS offer a variety of free resources on cybersecurity. These include templates for tabletop exercises, data-visualization tools, and free Cyber Hygiene Services for both private and public industries. The CISA Gateway is the primary repository for these resources but may require some training and certification to enable access.[33]

Cyber.org:[34] This is a CISA-funded initiative that provides curriculum, tools, and resources for cyber educators from kindergarten through 12th grade. Through a variety of programs across all 50 states, Cyber.org's mission is to enable cyber education and knowledge development to meet the nation's future cyber workforce requirements.

Environmental Protection Agency (EPA) Resources[35]

The EPA maintains a variety of specialized grant programs that can assist utility providers in implementing cybersecurity projects. These include the Clean Water State Revolving Fund, the Drinking Water State Revolving Fund, and the Midsize and Large Drinking Water System Infrastructure Resilience and Sustainability Program. Additionally, for Fiscal Year 2027, the EPA has requested dedicated cybersecurity funding within its Drinking Water Infrastructure Resilience Grant Program. If approved, the agency will have a nearly $20 million budget to "support responsible implementation of AI initiatives and critical cybersecurity solutions."[36]

Department of Energy (DOE) Resources

The DOE offers the Rural and Municipal Utility Cybersecurity (RMUC) Program, designed to assist eligible electric utility providers in protecting, detecting, responding to, and recovering from cybersecurity threats.[37] The DOE also maintains other resources and possible funding opportunities through its Office of Cybersecurity, Energy Security, and Emergency Response, primarily focusing on energy infrastructure and related risk management topics.[38]

Non-Federal Initiatives and Resources

A variety of other state-sponsored or private industry resources can support and enable local cybersecurity-related initiatives. A partial list of significant resources includes:

32 *Tribal Cybersecurity Grant Program*. (n.d.). Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov. https://www.cisa.gov/cybergrants/tcgp.

33 *CISA Gateway*. (2024). Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/resources-tools/services/cisa-gateway.

34 *About Us*. (2016). Cyber.org. https://www.cyber.org/about-us.

35 *Cybersecurity Funding*. (2023, July 10). United States Environmental Protection Agency. https://www.epa.gov/cyberwater/cybersecurity-funding.

36 *FY 2020 Budget*. (2017, May 17). United States Environmental Protection Agency. https://www.epa.gov/planandbudget/cj.

37 *Rural and Municipal Utility Advanced Cybersecurity Grant and Technical Assistance (RMUC) Program*. (2024). Energy.gov. https://www.energy.gov/ceser/rural-and-municipal-utility-advanced-cybersecurity-grant-and-technical-assistance-rmuc.

38 *Office of Cybersecurity, Energy Security, and Emergency Response*. (n.d.). Energy.gov. https://www.energy.gov/ceser/office-cybersecurity-energy-security-and-emergency-response.

- **State specialty offices such as the Texas Cyber Command.**[39] These entities are primarily dedicated to coordinating state-level responses to cyberattacks and developing actions and standards for cyberattack prevention. They can also coordinate between academia, law enforcement, and municipal governments.
- **The Multi-State Information Sharing and Analysis Center (MS-ISAC)**. MS-ISAC is a collaborative cybersecurity resource operated by the Center for Internet Security. Until October 2025, it was financially supported by CISA.[40] Because of the current lack of funding, the MS-ISAC is no longer an entirely free resource, but it is nevertheless a significant repository of information on cybersecurity and describes itself as entirely tailored toward U.S. SLTT governments.[41]
- **Cyber Ranges.** These are specialty facilities that provide simulated environments to train cybersecurity personnel and test or simulate cybersecurity scenarios. They are located in a variety of states and usually maintained as public-public or public-private partnerships between governments, academia, or National Guard entities.

CONCLUSION

Cybersecurity is an emergent threat that has been baked into our societal norms and is not going away. Recent events, such as the rise of hacking groups and the increase in cyberattacks on U.S. companies and critical industries demonstrate the severity of the challenges in the cyber realm. These events also illustrate how this emergent threat category is escalating and show the urgent need for additional proactive measures and policies to protect our defense industry, especially critical shared infrastructure, from cyber threats.

Installation-community partnerships are positioned to play a key role in combating cyber threats and increasing cybersecurity for our nation's critical infrastructure and military installations. Because of the rapid evolution of technology, including SaaS products and the ever-expanding Internet of Things, the most effective responses to cyber threats will be flexible, scalable, and tailored to individual organizational requirements. These responses should also distill best practices and standards set by federal agencies into actions that are affordable and accessible to local entities and defense industry organizations.

As premier coordinating entities standing in the middle of the web of overlapping state, federal, public, and private industry stakeholders, installation-community partnerships are perfectly positioned to help increase the use of effective cybersecurity practices and advocate or coordinate for action to close vulnerabilities in critical cyber networks. Through their core processes of harnessing support and building trust, our nation's installation-community partnerships can help enable a bright future for critical U.S. infrastructure where cyber technology continues to be viewed as a valuable tool and not as a golden opportunity for our nation's enemies.

39 *Texas Cyber Command becomes law*, UTSA to play key role. (2025, June 3). UT San Antonio Today. https://news.utsa.edu/2025/06/texas-cyber-command-becomes-law-utsa-to-play-key-role/

40 Wood, C. (2025, September 29). *CISA confirms it's ending MS-ISAC support*. StateScoop. https://statescoop.com/cisa-confirms-its-ending-ms-isac-support/.

41 *Multi-State Information Sharing and Analysis Center*. (n.d.) Center for Internet Security. https://www.cisecurity.org/ms-isac.

The Association of Defense Communities (ADC) builds resilient communities that support America's military. It is the connection point for leaders from communities, states, the military and industry on community-military issues by enhancing knowledge, information sharing, and best practices. With nearly 300 communities, states, regions and affiliated industry organizations, ADC represents every major defense community/state in the nation.

defensecommunities.org

Matrix Design Group is an award-winning interdisciplinary firm, providing professional engineering, consulting, environmental and planning and program management for both the public and private sectors. As specialists in sustaining installations, community advocacy and BRAC services, Matrix is a complete provider of innovation and solutions. With the industry's most comprehensive experience, the Matrix team has the necessary expertise to assess installation closure susceptibility and the tools and knowledge to help defense communities remain vibrant.

matrixdesigngroup.com

1300 Connecticut Ave NW
Suite 200
Washington, DC 20036

defensecommunities.org