UC BERKELEY

CENTER FOR LONG-TERM CYBERSECURITY

CLTC WHITE PAPER SERIES

Cyber Resilience and Social Equity

TWIN PILLARS OF A SUSTAINABLE ENERGY FUTURE

EMMA STEWART, REMY STOLWORTHY, AND VIRGINIA WRIGHT

Idaho National Laboratory

DISCLAIMER

CLTC WHITE PAPER SERIES

Cyber Resilience and Social Equity

TWIN PILLARS OF A SUSTAINABLE ENERGY FUTURE

EMMA STEWART, REMY STOLWORTHY, AND VIRGINIA WRIGHT

Idaho National Laboratory

September 2024

Idaho National Laboratory | Idaho Falls, Idaho 83415 | http://www.inl.gov

Prepared for the U.S. Department of Energy Office of Nuclear Energy Under DOE Idaho Operations Office

Contract DE-AC07-05ID14517

Contents

Abstract

This paper examines the intersection of security and accessibility within energy systems amidst the rise of grid modernization and digitization, especially considering the regulatory changes and the imperatives of inclusive energy strategies. It addresses the dual need for secure, resilient infrastructure and a commitment to mitigate energy poverty while maintaining equitable access to energy. Amid escalating cybersecurity and physical threats, the paper advocates for sustainable energy delivery systems that ensure robust defenses without compromising the goals of reducing energy poverty and ensuring energy security.

This paper identifies the pressing need for cyber-informed engineering (CIE) and secure-by-design (SbD) principles, highlighting how these strategies can protect critical infrastructure and democratize access to secure energy, particularly for disadvantaged communities. The analysis underscores the challenges presented by the expansion of attack surfaces, interoperability requirements, and grid-edge analytics, and offers innovative solutions that leverage advanced technologies and data-driven insights.

Furthermore, this paper addresses the workforce development gap, emphasizing the necessity for public-private partnerships and vendor engagement in creating a skilled cybersecurity workforce. This paper has a dual focus on both the technological aspect of cybersecurity and the social dimension of equity within the context of sustainable energy development. It suggests a comprehensive examination of how these two critical elements interact and support the overarching goal of a sustainable energy future.

Summary

The future energy grid confronts layered challenges that necessitate a reevaluation of current practices. Technical challenges in energy delivery, like the growing number of cyber threats, weather events, and reliability failures, are best countered with innovative approaches that integrate clean energy, interoperability, and intelligence to augment defenses and ensure seamless energy distribution.

Along with addressing these technical solutions, addressing the workforce gap, particularly within smaller utilities, is crucial. This report recognizes the disparity in resources and expertise available to small- and medium-sized utilities compared to large, investor-owned utilities, and recommends a series of collaborative efforts to enhance cyber resilience and social equity. Vendors play a significant role by aligning with the specific needs of these utilities and empowering them with the skills needed to maximize their cybersecurity measures, for example through right-sized technology, alternative workforce models, and targeted training.

This holistic approach towards cybersecurity is a strategic investment that serves the broader interest of the industry. Cybersecurity vendors, by fostering an environment of shared growth and security, contribute to a more formidable and unified energy grid. The future of the U.S. grid depends on a synergy of technological innovation, policy reform, and dedicated workforce cultivation, ensuring that security and equity are at the forefront of the energy industry's evolution.

Acronyms

AI	Artificial Intelligence
CCE	Consequence-driven Cyber-Informed Engineering
CIE	Cyber-Informed Engineering
ML	Machine Learning
OT	Operational Technology
SbD	Secure-by-Design
SMU	Small and Medium Utilities

Introduction

Cyber Resilience and Social Equity

Twin Pillars of a Sustainable Energy Future

The United States energy sector is undergoing a critical transition, underpinned by investments in sustainable and protected energy systems, with an emphasis on equity for marginalized communities.[1] This transformation is driven by the need to increase resilience against climate disruptions, reduce the impact of future energy delivery on the environment, and mitigate heightened cybersecurity risks. By investigating the nexus of energy equity and digitalization, this paper highlights the increased risks to underprivileged populations and calls for essential cybersecurity measures to become core to resilient infrastructure developments. This paper outlines a vision for the energy future through a thorough analysis of public-private collaborations, federal investments, and coordinated strategies, aiming to simultaneously enhance security, equity, and sustainability.

In the United States, economically disadvantaged areas have disproportionately suffered from the consequences of extreme weather and power outages.[2] Affordable housing, frequently situated in high-risk environmental zones like floodplains, has historically lacked adequate safeguards against extreme weather events due to the high cost of preventative measures.[3] Recent severe weather incidents have highlighted the consequence and need for a change in planning for these communities in the future. Today's decisions in clean energy infrastructure must balance security and cost to avoid perpetuating these disparities, by installing lesser quality or insecure but affordable technology in disadvantaged communities. Ensuring equitable access to secure and resilient energy systems is not only a matter of justice but a foundational necessity for the well-being of these communities, and modernization must not drive new burdens for the future.[4–7]

Market-driven cybersecurity refers to cybersecurity practices, tools, and strategies that are shaped by market forces, rather than by centralized regulation, government initiatives, or policy mandates. In such a system, organizations are incentivized to protect their assets based on the

competitive advantages cybersecurity can provide, customer demand, and compliance with market standards. However, this approach often leads to significant disparities in cybersecurity capabilities, cost of solutions, and misplaced priorities driven by investment and return. The inequities within market-driven cybersecurity, particularly in the energy sector, illuminate a complex nexus of challenges spanning compliance costs, solutions that are ill-suited for small utilities, and the paradox of both sharing ubiquitous data for improving energy delivery and infrastructure modernization, while protecting it from cyber risk. Small utilities are often the primary provider of electricity for disadvantaged communities, with rural cooperatives and municipal entities serving most persistent poverty regions in the U.S.[8]

Recent data from the World Economic Forum highlights these disparities. In 2022, the cybersecurity economy grew significantly faster than the world economy, and this trend accelerated in 2023.[9] Despite rising investments in cyber resilience, the benefits of technological advancements are unevenly distributed. Larger organizations and developed economies benefit disproportionately from new technologies, while smaller entities and less developed regions lag behind, exacerbating systemic inequities.

The 2024 Global Cybersecurity Outlook reveals a troubling trend: organizations that once maintained minimum viable cyber resilience are disappearing. The gap between those with robust cyber resilience and those struggling to keep up is widening. Smaller organizations, which are often critical providers in underserved areas, are significantly less likely to have the cyber resilience needed to meet operational requirements. For instance, smaller organizations are more than twice as likely to report inadequate cyber resilience compared to their larger counterparts, and they are three times more likely to lack necessary cyber skills. This disparity is further highlighted by the fact that only 25% of smaller organizations carry cyber insurance, compared to 75% of larger organizations.[9]

Moreover, the rise in cyber insurance costs disproportionately affects smaller organizations, compounding their vulnerability. The global divide is mirrored in cybersecurity capabilities, with Latin America and Africa reporting lower cyber resilience compared to North America and Europe. This “cybersecurity poverty line” illustrates how prohibitive costs and insufficient resources create barriers for smaller entities to achieve robust cyber protection.

1
Harmonizing Cybersecurity Investment With Critical Infrastructure

The current state-of-play in the energy sector is that cybersecurity is often seen as a necessary but burdensome compliance requirement, rather than an integral part of strategic planning and innovation, leading to gaps in proactive defense measures. It is imperative to shift the current perspective on cybersecurity within the energy sector, recognizing it not as a burdensome afterthought but a vital component essential to maintaining and progressing the nation's critical infrastructure. This shift demands embedding security considerations deeply within the realms of energy policy, planning, and investment. Such a holistic integration calls for collaborative efforts spanning across various agencies, industries, and communities to fortify advancements in energy delivery with resilience, security, and fairness. This approach not only enhances infrastructure but also strengthens trust between energy providers and their consumers.[10]

The U.S. Department of Energy (DOE) recently announced a significant investment of $45 million into cybersecurity research for the energy sector.[11] This investment aims to improve the nation's defenses against cyberattacks that threaten our electricity grids, oil pipelines, and natural gas infrastructure. Due to the rise in cyber threats, escalated investments in cybersecurity have positioned many energy delivery service providers at the forefront of defending critical infrastructure. However, there remains a noticeable disparity, with smaller utilities, especially those catering to low-income groups, falling behind their larger, more affluent counterparts.[12] This gap is exacerbated by a dearth of skilled cybersecurity professionals, the challenge of security poverty (i.e., limited resources dedicated to cybersecurity implementation), and the burden of technical debt.[13]

To achieve this, there is a pressing need for knowledgeable advocates and personnel dedicated to overcoming the lack of human and technological resources in this field. Challenges include the following:

- **Compliance Costs and Energy Security:** When cybersecurity efforts are primarily driven by compliance, the focus often shifts to meeting only the minimum required security standards. While this approach may fulfill regulatory obligations, it can lead to increased operational costs as utilities invest in necessary compliance measures. These additional costs are often passed on to consumers, which can in turn affect energy affordability.

- **Data Protection Paradox:** In their efforts to comply with regulatory requirements, utilities often face the challenge of sharing potentially sensitive infrastructure data with external entities, such as government agencies, third-party vendors, or regulatory bodies.[14] While this sharing is necessary for transparency, reporting, and legal compliance, it can inadvertently compromise data security. External entities may not have the same stringent security protocols as the utility, leading to potential vulnerabilities. Additionally, the process of transferring data between different systems and organizations introduces risks of interception, unauthorized access, or data breaches. Consequently, while utilities strive to meet regulatory standards, they may expose their data to heightened security risks through knowledge of their operations.[15]

- **People vs. Product and Public-Private Partnerships:** Small energy providers struggle with the increasing cybersecurity demands and fail to make the capital investments needed that are implemented by their larger counterparts.

- **Federal Initiatives and Infrastructure Development:** While policy initiatives such as the Infrastructure Investment and Jobs Act aim to upgrade energy infrastructure, cybersecurity often falls through the funding cracks or is deemed nonessential compared to grid improvements or other priorities.

- **Cost-Benefit Communication:** Small utilities face the challenge of justifying the cost of cybersecurity measures over immediate and visible improvements to services, such as pole replacements and other resilience-based improvements.

Market-driven solutions, with profit margins and investment goals, tend to cater to larger organizations with more substantial budgets, leaving small utilities with tools that may not fit their specific needs. This creates a gap where smaller, often rural utilities, serving disadvantaged or persistent poverty regions, are left vulnerable. The market for cybersecurity is flooded with solutions that are ill-suited for small- to medium-sized and not-for-profit energy suppliers that serve a substantial segment of the population.[16] For example, many of the cybersecurity oper-

ational technology monitoring solutions are costed on a per-substation basis. Similar to the challenges small utilities have with economies of scale on purchases of traditional equipment with a smaller customer base to cover cost, these solutions are expensive for a small number of substations, and the associated infrastructure scale is not aligned with the number of customers served. This misalignment is particularly striking given the massive energy-poverty gap within the U.S. Often, in the pursuit of clean energy, security is sidelined due to concerns about cost and limited return on investment, especially in low-income areas, creating a rift that needs bridging. For example, an inverter is a linchpin technology for clean energy.[17] Manufacture of these inverters is primarily offshore, leading to enhanced U.S. security concerns. To manufacture and purchase these items on shore would cost at least 20% to 50% more, and as such there is limited incentive to do that from the customer base.[18]

The energy sector faces a dichotomy: entities that can afford cybersecurity have many options, while those that cannot face tough choices with insufficient support, such as purchasing offshore equipment with enhanced security risks or utilizing the cloud because of lack of data infrastructure, but potentially in both cases introducing new or enhanced security risks, with no resources to manage. This issue parallels the broader challenge of energy security. This paper seeks to bridge these divides, offering security and equity-driven solutions modeled after existing federal initiatives, and alternative strategies pertaining to regulation, data management, staffing, and procurement, a trend particularly noticeable in areas with lower income. This creates a crucial gap that requires urgent attention and resolution.[19]

Reflecting on historical precedents, such as past decision-making processes in housing development, it is clear that focusing solely on present conditions without considering future adaptability can lead to suboptimal outcomes. Historical examples remind us to avoid design strategies focused on current conditions rather than future adaptability. Thus, while the U.S. Department of Housing and Urban Development, Department of Commerce, and Department of Energy (DOE) offer programs for energy-efficient housing, government agencies need to prioritize cybersecurity resilience as a foundational element of equitable energy distribution, not as an afterthought.[20–22]

Larger entities are better equipped to act upon government-provided cybersecurity information, such as guidance on recommended controls, due to their more substantial resources and capabilities. In contrast, smaller utilities often lack the funding, staff, and infrastructure needed to implement these measures effectively, leaving them more vulnerable. This challenge is further exacerbated by public cyberthreat disclosures that do not account for the limited capabilities and resources of smaller entities.

This scenario calls for an equitable integration of cybersecurity measures across all critical infrastructure, especially in support of underserved communities. It suggests a business model overhaul by which equitable security provisions take precedence over profit in the cybersecurity realm of critical infrastructure, ensuring that utilities of every scale have access to appropriate security solutions. Cybersecurity standards and regulations should be designed with flexibility to accommodate the varying capabilities of different-sized utilities, ensuring that all are held to a high standard without being overwhelmed by compliance costs. Ultimately, this approach aims to create a more resilient and secure critical infrastructure landscape, where all utilities—regardless of size or resources—can safeguard their systems and the communities they serve.

2
Cyber-Informed Engineering and Secure-By-Design Approaches

Incorporating cybersecurity into the fabric of community energy planning — and the design of future technology, software, and hardware — is crucial for enhancing resilience and reliability of energy delivery for all. Cyber-informed engineering (CIE)[23] and secure-by-design (SbD)[24] initiatives both introduce a proactive paradigm in cybersecurity, advocating for the integration of security considerations right from the initial stages of component design and development. This approach implores vendors and original equipment manufacturers (OEMs) to embed resilience into their products from the very beginning. These frameworks aim to create systems that are inherently more secure, reducing the likelihood and potential impact of cyberattacks on the energy infrastructure and its consumers. By adopting a secure-by-design mindset, as outlined in the National Cybersecurity Strategy,[25] energy systems can be developed with inherent resilience, decreasing dependency on post hoc defenses.

CYBER-INFORMED ENGINEERING FOR COMMUNITIES

The 2023 White House National Cyber Strategy, recognizing the escalating threats of cyberattacks on critical infrastructure, advocated for CIE as a key approach to bolster defenses.[23, 25] The National Cyber Strategy also highlights the necessity of collaborative efforts among the government, private sector, and academia to advance CIE practices, including the sharing of best practices, development of standards, and encouragement of research and development.

Prioritizing security in procurement, leveraging market dynamics, and early design-cycle integration are strategic moves that can help build robust, affordable energy systems for all sectors. CIE offers a focused strategy, emphasizing the identification and protection of the most critical elements within the energy system. By assessing and prioritizing components whose compromise could lead to the most severe consequences, CIE provides a targeted approach to cybersecurity. This method ensures that the most impactful aspects of the energy delivery system receive the highest level of protection against potential cyber threats.

By doing so, CIE aims to minimize vulnerabilities and enhance resilience against cyber threats. Moving beyond just reactive measures like patching and incident response, CIE advocates for proactive steps, such as integrating security features into system design, conducting thorough vulnerability assessments, and adhering to secure coding practices. This forward-thinking approach is crucial for preempting cyberattacks, thereby conserving time and resources and avoiding potential damages.

This advanced methodology, detailed in the CIE implementation guide,[28] entails conducting a comprehensive threat assessment to understand the domino effects of different threats and prioritize the security of components based on their impacts on grid operations. This approach is crucial for preserving the integrity and resilience of the electric grid against evolving cyber threats. CIE is governed by the following 12 key principles:

Principle 1: Consequence-Focused Design

Principle 2: Engineered Controls

Principle 3: Secure Information Architecture

Principle 4: Design Simplification

Principle 5: Layered Defenses

Principle 6: Active Defense

Principle 7: Interdependency Evaluation

Principle 8: Digital Asset Awareness

Principle 9: Cyber-Secure Supply Chain Controls

Principle 10: Planned Resilience

Principle 11: Engineering Information Control

Principle 12: Organizational Culture

These principles collectively ensure that cybersecurity is an integral aspect of engineering, rather than a supplementary element, guiding the process to identify and protect against high-consequence events. CIE offers a structured approach to making cybersecurity decisions based on the potential consequences of security breaches.

This methodology is particularly advantageous for disadvantaged communities, where resources for cybersecurity are limited. Through CIE, disadvantaged communities can focus

their limited resources on protecting the most crucial aspects of their infrastructure, ensuring that the most severe potential impacts are mitigated.

SECURE-BY-DESIGN AS AN APPROACH TO SHIFTING RESPONSIBILITY

The drive for cybersecurity in the contemporary technological landscape seeks to embed resilience in product design itself, a methodology championed by the SbD initiative of the Cybersecurity and Infrastructure Security Agency (CISA).[24] By adopting security measures at the outset of development, the initiative aims to relocate the onus of cybersecurity from end-users, who often are the least equipped, to manufacturers, who can build in safeguards at the foundational level. CISA lays out crucial principles that focus on the following principles:

- **Ownership of Security Outcomes:** Manufacturers should be accountable for customer security outcomes by ensuring their products are designed with a secure and trusted environment from the outset.

- **Transparency:** Openness about the security features of products provides insight into the cybersecurity integrity of a product and fosters trust with consumers.

- **Leadership Commitment:** Security should be championed from the top, with leadership actively participating in and promoting the integration of robust security measures.

These guiding principles are particularly beneficial for smaller and lower-income communities that often face challenges with implementing security enhancements due to constraints in budget and technical expertise. SbD levels the playing field, ensuring equitable access to secure products for all users, regardless of their economic background or market influence. SbD changes the cybersecurity landscape for disadvantaged communities by shifting the responsibility for secure systems to the vendors and manufacturers of products. By embedding security measures into the products during the design stage, SbD ensures that the systems and devices used by these communities are inherently secure, reducing their vulnerability to cyber threats.

This shift in responsibility means that disadvantaged communities can rely on the inherent security of the products they use, without needing to invest heavily in additional cybersecurity measures. Under the SbD framework, vendors and manufacturers are incentivized to produce more secure products, leading to broader availability of secure and resilient systems that are suitable for use in resource-constrained environments.

3
Building Equitable Security through Workforce Development in Small Utilities

The security of the electric grid is only as strong as the workforce maintaining it. Skilled cybersecurity and power systems engineers are the linchpin in this equation, yet smaller utilities often find themselves at a disadvantage in both attracting and retaining talent from these fields. The disparity in resources and opportunities in rural areas, compared to their urban counterparts, has created a chasm that needs to be addressed to strengthen the cybersecurity and physical security of the entire grid.[26]

VENDOR RESPONSIBILITY IN WORKFORCE DEVELOPMENT

Vendors play an essential role in supporting small and medium utilities (SMUs) beyond simply supplying advanced tools. Effective support requires a nuanced understanding of the unique challenges SMUs face, including staffing and operational constraints. By engaging with SMUs, vendors can tailor cybersecurity solutions to fit the specific needs and environments of these utilities.

TARGETED TRAINING AND UPSKILLING

Custom training programs and opportunities for skill development are transformative for SMUs. Vendors are instrumental in this process, providing the necessary training to ensure SMUs can effectively employ advanced cybersecurity technologies. Collaborative initiatives that consolidate resources and expertise are vital for bridging the skills gap.

LEVERAGING MANAGED SECURITY SERVICE PROVIDERS

Managed security service providers (MSSPs) present an outsourcing model that can alter the cybersecurity landscape for SMUs. By using managed security service providers, SMUs can

maintain robust security management without the overhead of a large internal team, streamlining their operations and focusing on core competencies.[27]

VENDOR PARTICIPATION FOR MUTUAL GAIN

Vendors that invest in the upskilling of SMUs' workforces can become indispensable partners in the grid's future security and efficiency. This investment not only enhances the vendor-customer relationship but also expands utilities' cybersecurity capabilities, improving the grid's overall resilience and opening new market avenues previously constrained by knowledge gaps.

Conclusion

There is a critical need for a paradigm shift that transcends traditional frameworks of ownership and responsibility to steer the nation toward a resilient and inclusive grid. The challenges in cybersecurity, operational complexity, grid-edge intelligence, and workforce development are not merely obstacles, but opportunities to catalyze a new era of sophisticated and sustainable energy infrastructure.

The technical challenges of attack-surface expansion, interoperability, and grid-edge analytics demand innovative solutions that leverage data-driven intelligence, standardized protocols, and distributed power architecture. These solutions foster a cyber-resilient grid, accommodating the integration of diverse energy resources and contending with the complexity of modern power systems.

However, the implementation of these technical solutions hinges on addressing the talent gap that threatens the very fabric of grid security. SMUs, which are vital components of the energy ecosystem, face unique hurdles in attracting and retaining skilled professionals. Collaborative efforts from vendors and government initiatives are essential to amplify the workforce competency across the grid's expanse, thereby bolstering the collective defense against emerging threats.

In conclusion, the convergence of collaborative governance, cutting-edge technology, and enhanced workforce-development strategies presents a roadmap for creating a secure, affordable, and equitable grid. Championing open-source innovation, implementing machine learning (ML) for threat detection, embedding intelligence at the grid edge, and nurturing the growth of cybersecurity talent within under-resourced communities will cultivate a foundation for a future-proof energy sector. This is not the sole endeavor of a single entity; rather, it requires concerted efforts from vendors, utilities, and policymakers alike. Through shared responsibility and a commitment to unity, the vision of a sustainable and secure energy future can become a reality for all.

Implementing comprehensive cybersecurity for utilities requires meticulous strategies that span multiple facets of the organization. The solutions discussed in this paper can contribute to a stronger, more proactive security posture.

References

1. The White House. 2023. "The Bipartisan Infrastructure Deal Boosts Clean Energy Jobs Strengthens Resilience and Advances Environmental Justice." Statements and Releases. Accessed May 16, 2023. https://www.whitehouse.gov/briefing-room/statements-releases/2021/11/08/fact-sheet-the-bipartisan-infrastructure-deal-boosts-clean-energy-jobs-strengthens-resilience-and-advances-environmental-justice/
2. Denholm, P., et al. 2022. "Examining Supply-Side Options to Achieve 100% Clean Electricity by 2035." NREL/TP-6A40-81644, National Renewable Energy Laboratory. (NREL). https://doi.org/10.2172/1885591
3. Pittman, L. 2023. "Energy Justice: Addressing Energy Burden Inequalities and the Electricity Grid's Infrastructure Inequities." *Natural Resources & Environment* 37(3): 21–25. https://www.proquest.com/openview/2f595b60c0d142245a589e2cbfb2f15b/1?pq-origsite=gscholar&cbl=46452
4. National Centers for Environmental Information. 2024. "Billion-Dollar Weather and Climate Disasters." Accessed January 14, 2024. https://www.ncei.noaa.gov/access/billions/
5. Cañizares, C., J. Nathwani, and D. Kammen. 2019. "Electricity for All: Issues, Challenges, and Solutions for Energy-Disadvantaged Communities [Scanning the Issue]." Proceedings of the IEEE 107(9):1775–1779. https://doi/org/10.1109/JPROC.2019.2935856
6. Reardon, K. M., M. Ionescu-Heroiu, and A. J. Rumbach. 2008. "Equity Planning in Post-Hurricane Katrina New Orleans: Lessons from the Ninth Ward." *Cityscape* 10(3): 57–76. https://www.jstor.org/stable/20868670
7. Taylor, K., and I. Murtazashvili. 2021. "Co-Ops and the Last Mile." Center for Governance and Markets Working Paper. https://dx.doi.org/10.2139/ssrn.3932510
8. World Economic Forum. 2024. "Global Cybersecurity Outlook 2024." Accessed August 28, 2024. https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf
9. U.S. Department of Energy. 2024. "DOE Announces $45 Million to Protect Americans from Cyber Threats and Improve Cybersecurity." Accessed August 28, 2024. https://www.energy.gov/articles/doe-announces-45-million-protect-americans-cyber-threats-and-improve-cybersecurity
10. Internet Security Alliance. n.d. "Social Contract." Accessed January 14, 2024. https://isalliance.org/isa-publications/social-contract/
11. U.S. Department of Energy. 2024. "DOE Announces $45 Million to Protect Americans from Cyber Threats and Improve Cybersecurity." Accessed August 28, 2024. https://www.

energy.gov/articles/doe-announces-45-million-protect-americans-cyber-threats-and-improve-cybersecurity

12. Pawlack, P. 2014. "Riding the Digital Wave: The Impact of Cyber Capacity Building on Human Development." European Union Institute for Security Studies (EUISS). https://doi.org/10.2815/43313
13. Hanus, N. L., et al. 2023. "Assessing the Current State of U.S. Energy Equity Regulation and Legislation." Lawrence Berkeley National Laboratory (LBNL), Berkeley, CA. https://doi.org/10.2172/1958540
14. National Association of Regulatory Utility Commissioners (NARUC). n.d. "Electric Vehicles: Grid Data Sharing." Accessed August 28, 2024. https://www.naruc.org/core-sectors/energy-resources-and-the-environment/electric-vehicles/grid-data-sharing/
15. E&E News. 2024. "Tensions at Home and Abroad Pose Growing Threat to U.S. Grid." Accessed August 28, 2024. https://www.eenews.net/articles/tensions-at-home-and-abroad-pose-growing-threat-to-us-grid/
16. Cooperative.com. n.d. "Essence Program." Accessed August 28, 2024. https://www.cooperative.com/programs-services/essence/Pages/default.aspx
17. Perry, S. 2024. "House Representative Scott Perry News Release." Accessed August 28, 2024. https://perry.house.gov/news/documentsingle.aspx?DocumentID=402899
18. Basore, P., and D. Feldman. 2022. "Solar Photovoltaics: Supply Chain Deep Dive Assessment." U.S. Department of Energy. https://doi.org/10.2172/1871588.
19. Hanus, N. L., J. Barlow, A. Satchwell, and P. Cappers. 2023. "Assessing the Current State of U.S. Energy Equity Regulation and Legislation." Lawrence Berkeley National Laboratory (LBNL). https://doi.org/10.2172/1958540
20. U.S. Department of Energy. n.d. "Community Solar." Accessed January 14, 2024. https://www.energy.gov/communitysolar/community-solar
21. U.S. Department of Housing and Urban Development. n.d. "Green Retrofit Program." Accessed January 14, 2024. https://www.hud.gov/grrp
22. U.S. Department of Energy. n.d. "Grid Resilience State/Tribal Formula Grant Program." Accessed January 14, 2024. https://www.energy.gov/gdo/grid-resilience-statetribal-formula-grant-program
23. Wright, V. L. 2023. "Cyber-Informed Engineering." INL/MIS-23-71048-Revo00, Idaho National Laboratory, Idaho Falls, ID. https://www.osti.gov/biblio/1960207
24. Cybersecurity and Infrastructure Security Agency. n.d. "Secure by Design." Accessed January 14, 2024. https://www.cisa.gov/securebydesign
25. The White House. 2023. "National Cybersecurity Strategy 2023." Accessed January 14, 2024. https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

26. Covert, E. (2023). Case study: Conducting a risk assessment for an electrical utility. In Proceedings of the International Conference on Cyber Warfare and Security, Academic Conferences International Limited.
27. Ramezan, C. A. (2023). Examining the Cyber Skills Gap: An Analysis of Cybersecurity Positions by Sub-Field. Journal of Information Systems Education, 34, 94–105.
28. V. L. Wright, J. P. Meng, R. S. Anderson, J. R. Gellner, L. B. Barnes, S. D. Chanoski, R. M. Edsall, M. R. Holtz, J. M. Jones, K. L. Le Blanc, J. C. Mahanes, T. R. McJunkin, J. Robinson, D. J. Rucinski, G. E. Shannon, J. J. Welch, M. Ayala, V. Atkins, K. A. Baker, and K. Castillo, "Cyber-Informed Engineering Implementation Guide," Idaho National Laboratory, Idaho Falls, ID, USA, INL/RPT-23-74072-Rev000, Sep. 2023. [Online]. Available: https://www.osti.gov/biblio/1995796

About the Authors

VIRGINIA "GINGER" WRIGHT is the program manager for Cyber-Informed Engineering (CIE) at the Idaho National Laboratory (INL). She leads INL's implementation of the National Strategy for Cyber-Informed Engineering developed by the Department of Energy. Ms. Wright has led multiple cyber research programs at INL including DOE-CESER's Cyber Testing for Resilient Industrial Control Systems (CyTRICS™) program, Software Bills of Material for the Energy Sector, critical infrastructure modeling and simulation, and nuclear cybersecurity.

EMMA STEWART is a Chief Power Grid Scientist at Idaho National Laboratory (INL) Emma is a strong electric grid technology professional skilled in Power distribution, Renewable Energy, Modeling & Simulation, Operational Cybersecurity, and Power Systems Integration.

REMY STOLWORTHY is a Cyber Vulnerability Analyst at Idaho National Laboratory (INL), focusing on fortifying the digital resilience of U.S. manufacturing and safeguarding the nations critical infrastructure. Specializing in securing industrial control systems, she focuses on enhancing cybersecurity within operational technology (OT) environments.


CLTC
Center for Long-Term
Cybersecurity
UC Berkeley