

Mapping the Gap: Analysis of Nuclear Cybersecurity Education in U.S. Universities

Myles Nelson
Dept. of Computer Science
University of Texas at Dallas
Dallas, TX, USA
0009-0008-2601-4992

Amorita A. Christian
School of Cyber Studies
University of Tulsa
Tulsa, OK, USA
0009-0000-1264-4469

Tiffany Haney
Idaho National Laboratory
Idaho Falls, ID, USA
0000-0003-0196-4787

Charles Nickerson
Idaho National Laboratory
Idaho Falls, ID, USA
0009-0002-4034-7378

Abstract—The U.S. nuclear sector is undergoing rapid transformation, driven by the expansion of advanced reactors, digital modernization of legacy systems, and increasing interest in nuclear energy to meet AI-fueled energy demands. However, the cybersecurity talent pipeline is not keeping pace with this growth. This paper investigates the significant gap in nuclear cybersecurity education and proposes scalable strategies for colleges to address this critical need by promoting it as a viable and essential career path. Through a multi-institutional landscape analysis of 16 cybersecurity and 12 nuclear engineering programs, we found that nuclear cybersecurity is largely absent from university curricula. Most students are unaware of the field's existence, and few institutions offer hands-on training or interdisciplinary exposure. This lack of awareness leads to a shortage of specialized talent, forcing nuclear facilities to retrain generalist hires or rely on costly external consultants. We present a framework for early pipeline cultivation grounded in Social Cognitive Career Theory and workforce development principles. Proposed solutions include student-led clubs, guest lectures, modular classroom kits, and summer boot camps. By increasing visibility and access to nuclear cyber content, we aim to break the self-reinforcing cycle of low awareness and limited specialization. This work underscores the critical role of education and advocacy in cultivating early interest and guiding students toward this emerging field. We call on academic institutions, national laboratories, and industry stakeholders to collaborate in establishing nuclear cybersecurity as a distinct and accessible career path within the broader cybersecurity and nuclear engineering ecosystems.

Keywords—*nuclear cybersecurity, workforce development, curriculum, OT/IT cybersecurity*

I. INTRODUCTION

The U.S. nuclear sector is entering an era of rapid expansion and transformation, marked by the emergence of numerous stakeholders and a renewed interest in nuclear energy. The current Federal administration is implementing policies, including executive orders and Department of Energy (DOE) investments, to increase nuclear energy capacity from

100 Gigawatts (GW) to 400 GW by 2050 [1]. Traditional nuclear power plants (NPPs) are transitioning from legacy analog systems to digital systems while artificial intelligence (AI) tools and platforms are advancing rapidly, surpassing the capabilities of existing energy infrastructure [2].

However, this transformation has outpaced the development of a cybersecurity workforce equipped to secure the digital infrastructure of modern nuclear systems. Operational technology (OT) and industrial control systems (ICS), long isolated from external networks, are now increasingly integrated into interconnected digital environments. These systems were not designed with cybersecurity in mind, making them particularly vulnerable to cyber threats when exposed to modern networking protocols and remote access capabilities [3]–[5]. The resulting vulnerabilities raise urgent concerns about safety, reliability, and regulatory compliance in a sector where the consequences of failure are uniquely severe.

From a systems engineering perspective, these risks underscore the importance of integrating cybersecurity considerations early in the design and development lifecycle. As Blanchard and Fabrycky [6] emphasize, late-stage security retrofits are often less effective and more costly than proactive, secure-by-design approaches. Yet, the ability to implement such strategies depends on the availability of professionals who understand both the technical and regulatory dimensions of nuclear systems.

This convergence of digital transformation and national energy priorities has elevated nuclear cybersecurity from a niche concern to a strategic imperative. Ensuring the safety, reliability, and regulatory compliance of digital nuclear systems requires a workforce with specialized knowledge at the intersection of cybersecurity and nuclear engineering. However, the preparation of that workforce depends on the ability of academic institutions to expose students to this interdisciplinary domain early in their educational journey.

Cybersecurity education has made significant strides in recent years, with the proliferation of degree programs, Centers of Academic Excellence, and workforce development initiatives. Yet, questions remain about how well these efforts address the needs of critical infrastructure sectors with

unique technical and regulatory constraints. Nuclear energy, in particular, presents a compelling case for examining how emerging cybersecurity challenges are reflected in university curricula.

This study is motivated by the need to understand how nuclear cybersecurity is positioned within the broader landscape of cybersecurity and engineering education. It explores the structural, institutional, and perceptual factors that shape student exposure to this field and considers how educational interventions might help align academic preparation with national security needs. Subsequent research was conducted to characterize the technical, regulatory, and risk-based factors that uniquely distinguish nuclear cybersecurity from other critical infrastructure sectors and to develop a sample curriculum responsive to the findings of this study [7].

II. BACKGROUND AND LITERATURE REVIEW

The cybersecurity workforce shortage is well documented across critical infrastructure sectors, but it is particularly acute in high-consequence domains such as nuclear energy. Industry leaders consistently report difficulty finding entry-level professionals with the technical skills and contextual awareness needed to secure operational technology (OT) environments, especially those governed by strict regulatory frameworks and safety requirements [8]. In the nuclear sector, this challenge is compounded by an aging workforce and a declining replacement rate, raising concerns about knowledge transfer and long-term resilience [9].

Workforce development in specialized cybersecurity domains depends not only on technical training but also on the existence of educational pathways that make such careers visible and accessible to students. In the case of nuclear cybersecurity, the highly interdisciplinary nature of the field, spanning nuclear engineering, digital instrumentation and control, regulatory compliance, and cyber defense, poses unique challenges for curriculum design and student engagement.

Theoretical models from career development research offer insight into how students come to pursue specialized technical fields. Social Cognitive Career Theory (SCCT), for example, emphasizes the role of early exposure, self-efficacy, and perceived career relevance in shaping students' academic and professional trajectories [10]. In emerging or underrepresented fields, the absence of visible role models, hands-on experiences, or curricular integration can suppress interest before it has a chance to form. This is particularly relevant in cybersecurity education, where students often gravitate toward well-known subfields such as penetration testing or digital forensics, while overlooking less visible but equally critical domains like OT security or nuclear cyber defense.

Recent studies in cybersecurity education have also highlighted the importance of experiential learning in preparing students for workforce demands. Ball *et al.* [11]

found that employer satisfaction was significantly higher for graduates who had participated in hands-on projects, capstone experiences, or real-world simulations, compared to those who completed traditional coursework alone. These findings suggest that bridging the gap between academic preparation and industry expectations requires not only content alignment but also pedagogical innovation. Despite growing recognition of the cybersecurity risks facing nuclear infrastructure, there has been limited research on how nuclear cybersecurity is represented in higher education. This study addresses that gap by examining the current state of curricular integration, student exposure, and institutional readiness to support nuclear cybersecurity as a viable and visible career path.

III. METHODOLOGY

This study employed a multifaceted, mixed-methods approach to provide a holistic view of the educational landscape in cybersecurity and nuclear engineering programs, highlighting areas of strength and opportunities for improvement. The research involved both quantitative analysis of program structures and qualitative insights from expert interviews.

A. Research Questions

The study sought to investigate the extent to which university programs in cybersecurity and nuclear engineering are equipping students for careers in nuclear cybersecurity. The research questions were designed to assess the visibility, integration, and practical relevance of nuclear cybersecurity content within the curricula, laboratory experiences, faculty research, and institutional partnerships.

Specifically, the study explored the following:

1. Curricular Integration

- Do cybersecurity programs include content related to critical infrastructure systems such as ICS, SCADA, DCS, or OT?
- Do nuclear engineering programs explicitly address cybersecurity in the context of nuclear systems?
- Are there overlapping courses, electives, or degree requirements shared between cybersecurity and nuclear engineering programs?

2. Hands-On Learning and Technical Skills

- Are students exposed to real or simulated ICS/SCADA environments (e.g., PLCs, RTUs, HMIs)?
- Do lab environments include industrial protocols such as Modbus, DNP3, OPC, PROFINET, or IEC 61850?

- Are students trained in threat modeling, attack simulation, or red/blue team exercises involving OT systems?
- Are students introduced to frameworks such as MITRE ATT&CK for ICS or concepts like cyber-informed engineering?
- What specific technical competencies are emphasized (e.g., OT packet analysis, control system fingerprinting)?

3. Faculty Expertise and Research Activity

- Do faculty members conduct research at the intersection of cybersecurity and nuclear engineering?
- Are there capstone projects, theses, or publications that bridge these domains?
- Are there joint research centers, labs, or initiatives that connect cybersecurity and nuclear faculty?

4. Industry and Government Alignment

- Do programs collaborate with national laboratories (e.g., Idaho National Laboratory (INL), Oak Ridge National Laboratory (ORNL), vendors, or utilities)?
- Are DOE, NRC, NEI, or NIST frameworks referenced in coursework or research?
- Are students offered experiential learning opportunities such as internships, guest lectures, or joint projects with industry or government partners?

These questions guided the data collection and analysis across program websites, course materials, lab descriptions, and expert interviews, providing a comprehensive view of the current educational landscape.

B. Theoretical Framework.

The research was guided by two central hypotheses, each grounded in distinct theoretical principles. The first hypothesis posits that limited collaboration between cybersecurity and nuclear engineering programs contributes to a shortage of nuclear cybersecurity specialists. The absence of integration between cybersecurity and nuclear engineering programs may limit students' early exposure to nuclear-relevant challenges, thereby narrowing the pipeline of future specialists.

The second hypothesis contends that universities currently lack structured programs to support nuclear cybersecurity education. As early as 2000, the OECD Nuclear Energy Agency (NEA) emphasized the importance of attracting students early in the educational process to ensure a steady supply of nuclear professionals [12]. The report warned that

declining enrollments, aging faculty, and reduced course offerings were already threatening the long-term viability of nuclear education. More recently, Cizelj *et al.* [13] proposed a European strategic agenda for nuclear education and training that continues to advocate for early exposure to nuclear topics, including outreach at the high school level. Because nuclear cybersecurity is a relatively new and highly specialized field, it has not yet benefited from the kind of structured educational pipeline that has long been emphasized as critical in the broader nuclear sector.

C. Data Collection and Analysis.

The study included a comparative analysis of 16 cybersecurity programs and 12 nuclear engineering programs across 20 universities in the United States (see complete list in Appendix Table I). The institutions of higher learning used for this study were selected based on recommendations from INL nuclear experts and the strength and renown of either their cybersecurity or nuclear engineering program. Evaluation was based on the available resources of their nuclear engineering/cybersecurity program, relevant research being pursued by faculty, and whether the university had both a nuclear engineering and a cybersecurity program. Institutions varied in size, type (public/private), and geographic location. For consistency and simplicity, programs offering cybersecurity-related coursework (whether under Cybersecurity, Computer Science, or Computer Engineering) were collectively categorized under the term "Cybersecurity."

Data were collected through a detailed review of program structures, curricula, and key focus areas using open-source data, including course catalogs, laboratory descriptions, and program syllabi. Special attention was given to identifying courses specifically related to OT and ICS. In addition to the quantitative analysis of program content, interviews were conducted with subject matter experts, including operators, vendors, and regulators, and industry stakeholders from both the cybersecurity and nuclear sectors. These interviews provided qualitative data on current trends, challenges, and best practices.

Data analysis integrated quantitative and qualitative approaches. The quantitative analysis provided a granular view of the specific topics covered in each program, the methodologies employed, and the resources available to students. Meanwhile, the qualitative analysis, informed from expert interviews, provided deeper insights into the practical implications of the educational programs and their alignment with industry needs. The role of experiential learning was also examined, focusing on examples such as the Cybersecurity and Infrastructure Security Agency (CISA) 301 course and cyber-in-a-case (CIAC) kits. These were analyzed for their effectiveness in bridging the gap between theoretical knowledge and practical application. The authors completed the CISA 300 and 301 courses and used CIAC kits to gain firsthand knowledge and experience, directly assessing the effectiveness of these programs in preparing students for industry roles.

IV. FINDINGS

This analysis examined 20 universities: eight offered cybersecurity programs, four offered nuclear engineering programs, and eight offered both programs. The findings highlighted a significant disciplinary divide between cybersecurity and nuclear engineering programs. Researchers found no formal joint coursework or interdisciplinary projects connecting nuclear engineering and cybersecurity programs. In nearly all cases, these programs operated independently, with little to no curricular overlap or interdisciplinary integration. Cybersecurity curricula lacked nuclear-specific context and were typically centered on traditional IT topics such as network security, cryptography, and ethical hacking. When operational technology (OT) was addressed, it was most often in the context of sectors like oil, gas, or water.

Nuclear engineering programs, by contrast, emphasized core technical domains such as reactor physics, thermal hydraulics, and safety analysis. Digital security and other cybersecurity applications were seldom addressed, and explicit references to cybersecurity were largely absent from undergraduate coursework. Nuclear-specific cybersecurity content was particularly scarce and, when present, was typically confined to graduate-level research or isolated electives.

Hands-on training opportunities that simulate real-world OT environments were also limited. Few programs offered laboratory experiences involving industrial protocols such as Modbus, DNP3, OPC, PROFINET, or IEC 61850. Even fewer provided students with opportunities to simulate cyberattacks or conduct red/blue team exercises in ICS or SCADA environments.

Additional analysis failed to identify dedicated nuclear cybersecurity programs, particularly at the undergraduate level. Similar offerings at the graduate level were limited and lacked hands-on training or implementation-focused coursework. Neither level contained courses that specifically bridged cybersecurity and nuclear engineering.

Despite the observed gaps, several institutions stood out for their contributions to critical infrastructure cybersecurity research and education. Appendix Table II highlights a selection of universities with notable programs, research centers, or partnerships relevant to OT and ICS security. Data were synthesized from publicly accessible sources, including course catalogs, faculty research profiles, and specialized certificate programs. The institutional selection for Appendix Table I was prioritized based on curricula alignment with OT cybersecurity, ultimately informing the comparative analysis presented in Appendix Table II [7].

V. DISCUSSION

Our research identified a disconnect between cybersecurity and nuclear engineering educational programs, manifesting in curricular and institutional fragmentation, limited hands-on training, and lack of specialized talent.

Curricular and institutional fragmentation. Our analysis revealed a persistent disconnect between nuclear engineering and cybersecurity education, both in curriculum content and institutional structure. Many universities with strong nuclear engineering programs lack instruction in cybersecurity principles, particularly in the context of OT and ICS. Conversely, cybersecurity programs often overlook OT and ICS entirely, or when included, focus on sectors such as oil, gas, or water, with little to no attention to nuclear applications. This disciplinary divide is compounded by a lack of institutional integration. Nuclear engineering and cybersecurity departments typically operate in silos, with separate faculty, facilities, and curricula. Even when interdisciplinary research occurs, it is rarely embedded in the student experience. As a result, nuclear engineering students often graduate without exposure to cybersecurity frameworks, while cybersecurity students remain unaware of nuclear regulatory and safety contexts. The absence of early, structured engagement with nuclear cybersecurity leads to a lack of specialization, requiring extensive and costly retraining for those entering the field.

Limited hands-on training. The absence of hands-on cybersecurity OT training within nuclear engineering programs represents a critical educational gap. While theoretical instruction provides foundational knowledge, practical experience is indispensable, especially in high-consequence, safety-critical fields. Most students entering the nuclear cybersecurity field lack interaction with real-world OT systems to understand how cyber threats manifest in a nuclear context. This deficiency in practical learning significantly impacts students' readiness and capabilities as viewed by industry leaders. Although students may have a conceptual understanding of risk management, compliance frameworks, and data flows, this knowledge is rarely applied within a nuclear context.

Lack of specialized talent. The field of nuclear cybersecurity faces a critical shortage of specialized talent, driven by both the expansion of the nuclear energy sector and the retirement of experienced specialists. The underdeveloped talent pipeline is insufficient to meet the replacement needs, forcing the industry to rely heavily on expensive consultants, which is unsustainable and severely impacts operational efficiency and escalates costs. This talent gap presents a strategic opportunity for universities to incorporate nuclear-specific standards and regulation frameworks, such as those from NIST, the Nuclear Regulatory Commission (NRC), and the Nuclear Energy Institute (NEI), into their curricula. The lack of specialized talent has led to a workforce readiness gap. According to an NRC official, while new cybersecurity hires possess strong IT skills, their exposure to OT is limited, and their nuclear experience is nonexistent. Similarly, an NPP operator noted that nuclear engineering graduates have a baseline understanding of plant operations, but cybersecurity graduates require 12-18 months of additional training to understand cybersecurity in nuclear systems. Addressing these gaps through targeted education programs can enhance

workforce readiness and reduce the industry's dependence on costly external consultants [7].

Proposed Solutions. Addressing the disconnect between cybersecurity and nuclear engineering requires a scalable, tiered approach that reflects institutional differences in readiness, resources, faculty expertise, and strategic priorities. Based on our research, we propose a three-tiered strategy of short-, mid-, and long-term interventions designed to support institutions at different stages of readiness. Each tier aligns with the time and resources required for successful implementation and can be adopted independently or sequentially, depending on institutional constraints and goals. Short-term strategies include low-cost, high-impact activities such as student clubs, guest lectures, and hands-on kits that introduce nuclear cybersecurity concepts in accessible ways. Mid-term interventions involve more formal integration, including elective courses and faculty development programs that build curricular depth and instructional capacity. Long-term strategies aim to institutionalize nuclear cybersecurity education through certificate and degree programs, as well as partnerships with industry and national laboratories that provide students with real-world experience. Together, these tiers offer a flexible roadmap for strengthening the nuclear cybersecurity talent pipeline, beginning with foundational exposure. Given the importance of early exposure in developing specialized expertise, initial effort should focus on the undergraduate level.

VI. CONCLUSION

This study reveals a persistent and self-reinforcing gap in the development of nuclear cybersecurity talent, driven by limited collaboration between nuclear engineering and cybersecurity programs and a lack of early exposure for students. Without structured undergraduate engagement, students remain unaware of nuclear cybersecurity as a viable specialization, constraining the pipeline of qualified professionals. As a result, the nuclear sector is increasingly reliant on costly retraining and external consultants to meet its cybersecurity needs, which is neither scalable nor sustainable.

The findings underscore the urgent need for academic institutions to integrate nuclear cybersecurity concepts into existing curricula and to foster interdisciplinary learning experiences that bridge technical and regulatory domains. By embedding nuclear-relevant cybersecurity content at the undergraduate level, universities can align academic preparation with industry demands, reduce workforce onboarding time, and enhance sector-wide resilience. Addressing this educational gap is not only a strategic imperative for national security but also a timely opportunity for academic institutions to equip students with the interdisciplinary skills required to meet the growing cybersecurity demands of the nuclear sector.

REFERENCES

- [1] Office of Nuclear Energy, "9 Key Takeaways from President Trump's Executive Orders on Nuclear Energy," 2025. [On-line]. Available: <https://www.energy.gov/ne/articles/9-key-takeaways-president-trumps-executive-orders-nuclear-energy>
- [2] W. Huang and Y. Zhang, "Will grid construction keep up with the pace of AI development?" in *2022 7th International Conference on Power and Renewable Energy (ICPRE)*, 2024, pp. 1447–1451. [Online]. Available: <https://doi.org/10.1109/ICPRE62586.2024.10768566>
- [3] S. Kumar, "Cybersecurity in industrial control systems: Best practices & threats," *Cyber Tech Journals*, 2025. [Online]. Available: <https://cybertechjournals.com/cybersecurity-in-industrial-control-systems-best-practices-threats-in-2025/>
- [4] NIST, "SP 800-82 Rev. 3: Guide to OT Security," 2023, National Institute of Standards and Technology. [Online]. Available: <https://doi.org/10.6028/NIST.SP.800-82r3>
- [5] A. A. Cardenas, S. Amin, and S. Sastry, "Research challenges for the security of control systems," in *Proceedings of the 3rd Conference on Hot Topics in Security*, 2008. [Online]. Available: <https://dl.acm.org/doi/10.5555/1496671.1496677>
- [6] B. S. Blanchard and W. J. Fabrycky, *Systems Engineering and Analysis*, 5th ed. Prentice Hall, 2010. [Online]. Available: <https://www.pearson.com/en-us/pearsonplus/p/9780137980888>
- [7] A. Christian, M. Nelson, T. Haney, and C. Nickerson, "Building nuclear-specific cybersecurity expertise in higher education," Pending publication.
- [8] A. Bachmann, G. Meyers, and M. Zerphy, "Nuclear cybersecurity course development," in *Proceedings of the INMM 65th Annual Meeting*, 2024. [Online]. Available: <https://resources.inmm.org/annual-meeting-proceedings/nuclear-cybersecurity-course-development>
- [9] E. McAndrew-Benavides, "Maintaining a highly-qualified nuclear industry workforce," *Health Physics*, vol. 100, pp. 86–87, 2011. [Online]. Available: <https://doi.org/10.1097/hp.0b013e3181fa2a84>
- [10] R. W. Lent, S. D. Brown, and G. Hackett, "Toward a unifying social cognitive theory of career and academic interest, choice, and performance," *Journal of Vocational Behavior*, vol. 45, no. 1, pp. 79–122, 1994. [Online]. Available: <https://doi.org/10.1006/jvbe.1994.1027>
- [11] J. Ball, M. Lyons, and K. Evans, "Bridging the cybersecurity skills gap: Aligning educational programs with industry needs," *Journal of The Colloquium for Information Systems Security Education*, vol. 12, no. 1, 2025. [Online]. Available: <https://doi.org/10.53735/cisse.v12i1.196>
- [12] Nuclear Energy Agency (NEA), *Nuclear Education and Training: Cause for Concern?* Paris: OECD Publishing, 2000. [Online]. Available: <https://doi.org/10.1787/9789264187627-en>
- [13] L. Cizelj, C. Pesznyák, J. Starflinger, G. L. Pavel, F. Wastin, and E. Michailidou, "Towards strategic agenda for european nuclear education, training, and knowledge management," *Nuclear Engineering and Design*, vol. 420, p. Article 113001, 2024. [Online]. Available: <https://doi.org/10.1016/j.nucengdes.2024.113001>

APPENDIX

TABLE I. Universities and Colleges Reviewed

University Name	Program(s)	Location	Public / Private	Student Population
Carnegie Mellon University	Cybersecurity	Pittsburgh, Pennsylvania	Private	15,818
Case Western Reserve University	Cybersecurity	Cleveland, Ohio	Private	12,475
Fisk University	Cybersecurity	Nashville, Tennessee	Private	1,055
Georgia Institute of Technology	Cybersecurity & Nuclear Engineering	Atlanta, Georgia	Public	47,961
Idaho State University	Cybersecurity & Nuclear Engineering	Pocatello, Idaho	Public	12,614
Massachusetts Institute of Technology	Cybersecurity & Nuclear Engineering	Cambridge, Massachusetts	Private	11,886
Meharry Medical College	Cybersecurity & Nuclear Engineering	Nashville, Tennessee	Private	956
Mississippi State University	Cybersecurity	Starkville, Mississippi	Public	22,986
North Carolina State University	Nuclear Engineering	Raleigh, North Carolina	Public	37,873
The Pennsylvania State University	Cybersecurity & Nuclear Engineering	University Park, Pennsylvania	Public	87,995
Purdue University	Cybersecurity & Nuclear Engineering	West Lafayette, Indiana	Public	52,211
Texas A&M University	Nuclear Engineering	College Station, Texas	Public	74,829
University of California, Berkeley	Cybersecurity & Nuclear Engineering	Berkeley, California	Public	45,307
University of Illinois Urbana-Champaign	Cybersecurity & Nuclear Engineering	Urbana-Champaign, Illinois	Public	56,299
University of Michigan	Nuclear Engineering	Ann Arbor, Michigan	Public	52,855
University of South Carolina	Cybersecurity	Columbia, South Carolina	Public	35,364
University of Tennessee	Nuclear Engineering	Knoxville, Tennessee	Public	31,701
University of Texas at San Antonio	Cybersecurity	San Antonio, Texas	Public	34,742
University of Tulsa	Cybersecurity	Tulsa, Oklahoma	Private	3,769
Vanderbilt University	Cybersecurity	Nashville, Tennessee	Private	13,537

TABLE II. Selected Highlights from University Programs

University	Program Highlights
Carnegie Mellon University	Hosts the Software Engineering Institute (SEI); ICS/SCADA security research at CERT division; strong ties to DOE and DHS.
Georgia Institute of Technology	SCADA security research via GTISC and the Cyber-Physical Systems group.
Idaho State University	Offers a Nuclear Operations Technology pathway to BAS in Cyber-Physical Systems; includes industrial cybersecurity certification.
Massachusetts Institute of Technology	While more theoretical, its Lincoln Lab conducts substantial ICS cybersecurity research.
Mississippi State University	One of the earliest ICS security testbeds; DHS/DOE partnership experience.
Purdue University	Center for Education and Research in Information Assurance and Security (CERIAS); OT-focused labs.
University of California, Berkeley	Strong ICS security and critical infrastructure protection work in EECS.
University of Illinois Urbana-Champaign	Cyber Resilient Energy Delivery Consortium (CREDC); extensive work on securing energy systems.
University of South Carolina	Home of the Critical Infrastructure and Industrial Control Systems Cybersecurity Lab.
University of Texas at San Antonio	Top-tier NSA-designated Center of Academic Excellence.