

Building Nuclear-Specific Cybersecurity Expertise in Higher Education

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

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

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 rapid digitalization of nuclear power plants (NPPs) and the deployment of advanced and small modular reactors (A/SMRs) have expanded the cybersecurity attack surface within the nuclear sector. This evolution introduces unique challenges beyond those faced in general information technology (IT), operational technology (OT) and industrial control system (ICS) security, due to nuclear power's regulatory rigor, safety-critical nature, and operational needs.

A pressing workforce gap persists; cybersecurity graduates typically lack nuclear-specific context and retraining them for industry readiness requires 12–18 months, creating a significant burden. This paper addresses this gap by defining the domains of knowledge that nuclear cybersecurity specialists must master, spanning cybersecurity, nuclear engineering, OT/ICS security, and regulatory governance. We propose a curricular framework integrating technical, regulatory, and applied learning components to accelerate workforce readiness.

Our approach builds on existing findings that current curricula inadequately integrate nuclear engineering and cybersecurity, shifting the discourse from why specialization is needed to what knowledge must be taught. The recommendations have implications for workforce development and long-term resilience of the nuclear energy sector.

Keywords—*nuclear cybersecurity, workforce development, higher education, OT/IT cybersecurity*

I. INTRODUCTION

The nuclear energy sector is undergoing a period of significant transformation, driven by the modernization of legacy nuclear power plants and the deployment of advanced technologies such as A/SMRs and artificial intelligence (AI)-enabled systems. As these systems become increasingly digitalized, cybersecurity concerns are amplified. Unlike other critical infrastructure sectors, nuclear power must navigate additional dimensions of regulatory trust, safety culture, and national security considerations. The consequences of a successful cyberattack in this sector extend beyond economic or reputational harm, potentially compromising reactor safety and eroding public confidence.

The global energy landscape underscores the urgency of these concerns. Nuclear energy is expected to play a central role in achieving net-zero climate goals and enhancing energy security. The International Energy Agency (IEA) projects a growing reliance on nuclear as a stable, low-carbon power source, while organizations such as the Organisation for Economic Cooperation and Development (OECD) Nuclear Energy Agency (NEA) and World Nuclear Association (WNA) highlight the rapid development of SMRs to meet emerging energy demands [1]–[3]. These advances coincide with ongoing modernization efforts at existing plants and increasing interest in AI applications for plant operations, which the U.S. Nuclear Regulatory Commission (NRC) has acknowledged in its external engagement on AI [4]. However, this digitalization and automation also introduce new cyber vulnerabilities, raising the stakes for both regulators and operators.

Although OT and ICS cybersecurity practices have matured in industries such as oil, gas, and electric power, the nuclear sector requires additional specialization. Regulatory frameworks such as the NRC's 10 CFR 73.54 rule and Regulatory Guide 5.71 establish unique compliance and governance obligations not found in other sectors [5], [6]. Likewise, the International Atomic Energy Agency (IAEA) embeds cybersecurity within broader nuclear safety and safeguards requirements through the Nuclear Security Series [7]–[9]. This intersection of technical, regulatory, and cultural demands sets nuclear cybersecurity apart and underscores the need for a tailored educational framework. The purpose of this paper is therefore to define the specialization needs of nuclear cybersecurity and to propose integrated curricular pathways that can prepare the next generation of specialists for this complex environment.

A. Why Specialization is Needed

Generic cybersecurity education, even when focused on OT and ICS, is insufficient to prepare professionals for the nuclear operating environment. Cybersecurity incidents in nuclear facilities carry uniquely high and irreversible consequences, with the potential to affect reactor safety, trigger cascading system failures, or undermine compliance with domestic and international safeguards. Although critical infrastructure sectors operate under a wide range of cybersecurity regulatory frameworks, even mature regimes

such as the NERC Critical Infrastructure Protection (CIP) standards governing the electric power sector do not capture the full set of constraints and risk characteristics unique to nuclear facilities. Safety licensing requirements, national security considerations, and the presence of safety-critical systems significantly limit system modification, patching, and architectural change, rendering many standard cybersecurity practices impractical or unacceptable. Moreover, nuclear facilities operate within a multi-layered regulatory ecosystem that includes domestic oversight by the NRC, international standards established by the IAEA, and governance expectations from the U.S. Department of Energy (DOE). Collectively, these frameworks impose obligations that exceed those faced in most other critical infrastructure sectors, requiring prescriptive asset classification, rigorous compliance auditing, and consequence-driven risk analysis that cannot be adequately addressed by traditional cybersecurity or traditional nuclear engineering curricula. As global demand for nuclear energy accelerates, this mismatch between educational preparation and operational reality creates an urgent need for dedicated nuclear cybersecurity education tailored to the sector's distinct technical, regulatory, and risk landscape.

To meet these demands, cybersecurity professionals must acquire competencies that extend beyond traditional IT or OT security. The IAEA's Model Academic Curriculum in Nuclear Security demonstrates the breadth of nuclear-specific knowledge needed, spanning radiation protection, safeguards, nuclear law, and policy in addition to technical cyber skills [10]. Without such integration, graduates enter the workforce with critical knowledge gaps, forcing facilities to rely on prolonged retraining before individuals become operationally effective.

The urgency of specialization is heightened by both workforce challenges and evolving cybersecurity practices. An aging nuclear workforce, combined with the planned expansion of nuclear energy, particularly A/SMRs, is driving demand for qualified specialists [1], [11]. At the same time, emerging methodologies such as Consequence-driven, Cyber-informed Engineering (CCE) highlight the need to train students to evaluate cyber risks based on safety and national security consequences rather than technical vulnerabilities alone [11], [12]. Complementary frameworks like MITRE ATT&CK for ICS further support education by providing structured adversary models that can be applied in practical OT/ICS defense training [13]. Together, these factors point to the need for an educational framework that integrates nuclear engineering fundamentals, regulatory compliance, advanced cybersecurity practices, OT/ICS defense, and consequence-based risk methodologies. Building a deliberate specialization will be essential for the next generation of professionals to protect the nuclear sector from evolving cybersecurity threats, ensuring the resilience and security of the nuclear sector in an era of rapid technological change.

II. WHAT NUCLEAR CYBERSECURITY SPECIALISTS NEED TO LEARN

The digitalization of nuclear facilities has created opportunities for operational efficiency and vulnerabilities to cyber threats, making cybersecurity a critical component of nuclear safety. Developing a competent nuclear cybersecurity workforce requires an integrated curriculum encompassing cybersecurity principles, nuclear systems and operations, regulatory frameworks, OT security, and incident management. A well-designed, specialized curriculum equips practitioners with the focused knowledge and hands-on experience necessary to protect critical digital assets (CDAs), anticipate and mitigate threats, respond effectively to incidents, and maintain regulatory compliance.

As part of a research initiative led by Idaho National Laboratory (INL), a sample curriculum was developed to address the growing need for nuclear-specific cybersecurity education, as shown in Table I. The project began with a landscape analysis of existing cybersecurity and nuclear engineering programs, followed by interviews with INL subject matter experts (SMEs) in both nuclear cybersecurity and instructional design [24]. Insights from these engagements directly informed the design of the curriculum, ensuring that it reflects both the operational realities of nuclear facilities and the expectations of industry and regulatory stakeholders.

The sample curriculum was designed to prepare students for cybersecurity roles within the nuclear sector by bridging the gap between traditional IT expertise and the specialized operational technology (OT) and regulatory requirements of nuclear power plants. The curriculum integrates regulatory compliance (10 CFR 73.54, RG 5.71), NIST Cybersecurity Framework principles, and Consequence-Driven, Cyber-Informed Engineering (CCE) methodologies. Graduates of the program would enter the workforce equipped with nuclear-specific knowledge and applied skills, reducing retraining time and accelerating readiness for critical infrastructure protection. In this context, the following sections describe the core technical, operational, and governance competencies and the applied skills necessary for nuclear cybersecurity professionals.

A. *Cybersecurity Foundations*

At its core, nuclear cybersecurity relies on a strong foundation in cybersecurity principles. This includes competencies such as network security, adversarial thinking, Zero Trust architectures, layered defense, and incident response. These principles are not taught in isolation but are contextualized within the unique operational and regulatory environment of nuclear power.

In the proposed curriculum, students begin by learning to map CDAs to NRC security levels using realistic plant architectures. This exercise, introduced in Week 1, helps students understand how digital assets are prioritized based

TABLE I. Sample Introduction to Cybersecurity for Nuclear Power Course

NIST Cybersecurity Framework Function	Week(s)	Learning Objectives
Govern	1, 2	<ul style="list-style-type: none"> • Explain the purpose and scope of 10 CFR 73.54 and Regulatory Guide 5.71 • Classify Critical Digital Assets (CDAs) in a simplified NPP architecture • Describe the role of governance policies in NPP cybersecurity • Draft basic Cyber Security Plan (CSP) governance policies
Identify	3-5	<ul style="list-style-type: none"> • Document NPP systems, networks, and CDAs • Map potential adversary tactics, techniques, and procedures (TTPs) against CDA assets • Prioritize risks using consequence-driven methods
Protect	6-8	<ul style="list-style-type: none"> • Apply access control principles and network segmentation to protect CDAs • Implement secure baselines and change controls to maintain CDA protections • Design role-based access control policies to mitigate insider risk
Detect	9, 10	<ul style="list-style-type: none"> • Configure monitoring systems to detect cyber anomalies affecting CDAs • Correlate behavioral and cyber indicators to identify potential insider misuse
Respond	11, 12	<ul style="list-style-type: none"> • Develop an incident response playbook aligned with NRC reporting and operational procedures • Apply incident response plan during a simulated NPP cyber event
Recover	13, 14	<ul style="list-style-type: none"> • Restore compromised CDAs to a secure operational state and validate system integrity • Implement corrective actions to strengthen defenses
Capstone Integration	15	<ul style="list-style-type: none"> • Integrate regulatory, technical, and consequence-driven approaches to defend a fictional NPP against a simulated multi-vector cyber-attack

on their safety, security, and emergency preparedness (SSEP) functions. In Week 2, students draft governance policies for a fictional nuclear facility, linking cybersecurity controls to regulatory mandates under 10 CFR 73.54 and Regulatory Guide 5.71 [5], [6]. These early exercises establish a foundation for understanding how cybersecurity principles are applied in a nuclear context.

The curriculum also incorporates adversary modeling using MITRE ATT&CK for ICS and consequence-driven thinking through CCE [13], [14]. These methodologies are introduced in Weeks 4 and 5, where students map threat vectors to CDAs and assess the potential consequences of successful attacks. This approach shifts the focus from generic vulnerability management to mission-critical protection, a key distinction in nuclear cybersecurity.

By Week 6, students are designing access control matrices and implementing network segmentation strategies using VLANs, firewalls, and data diodes. They simulate unauthorized access attempts and evaluate the effectiveness of their defenses. These labs reinforce the principle of defense-in-depth and prepare students to implement layered protections that align with NRC expectations, while working within the safety and operational constraints of the nuclear field.

B. Nuclear Engineering Context

A foundational understanding of nuclear engineering is essential for contextualizing cyber risks within operational environments and distinguishing nuclear cybersecurity from general OT/ICS security. Specialists should be familiar with basic concepts in reactor operations, nuclear systems design, radiation protection, reactor safety, and physical protection systems. This baseline knowledge enables them to assess how cyber incidents could affect safety-critical functions and to understand the interdependencies between digital and physical security measures.

The curriculum integrates this knowledge through scenario-based labs that simulate plant operations. Students learn to distinguish between systems that support safety functions (e.g., reactor protection systems) and those that do not, applying consequence-based prioritization to guide protection strategies. This technical grounding is reinforced through exercises that require students to collaborate across disciplines. In the capstone simulation, students must defend a fictional NPP against a coordinated cyberattack. Success depends not only on technical skill but also on the ability to understand how cyber events affect plant operations, safety margins, and regulatory compliance.

By embedding nuclear engineering fundamentals into cybersecurity training, the curriculum ensures that graduates can speak the language of plant operators, understand the implications of system failures, and design protections that support both safety and security objectives.

C. Regulatory and Governance Literacy

Regulatory knowledge and governance frameworks are essential for ensuring that cybersecurity practices in nuclear facilities comply with national and international standards.

In Weeks 1 and 2, students are introduced to the regulatory landscape through readings and discussions on 10 CFR 73.54, RG 5.71, and NEI 08-09 [5], [6], [15]. They draft Cyber Security Plan (CSP) governance policies and participate in peer reviews to refine their understanding of compliance requirements. These exercises emphasize the importance of aligning technical controls with governance structures and institutional policies.

Later in the course, students simulate NRC inspections and develop documentation that mirrors what would be required during a regulatory audit. They learn to justify their asset classifications, access control decisions, and incident response procedures using language and logic consistent with NRC expectations. This regulatory fluency is critical for workforce readiness. Graduates must be able to navigate complex compliance environments, communicate effectively with regulators, and design cybersecurity programs that are both technically sound and legally defensible.

D. OT/ICS Security in the Nuclear Context

A solid grasp of OT/ICS cybersecurity is essential for nuclear cybersecurity specialists, though this course assumes students enter with foundational knowledge of ICS environments. Unlike IT systems, industrial control systems were not originally designed with cybersecurity in mind. They often rely on legacy hardware and software, use proprietary or insecure-by-design protocols (e.g., Modbus, DNP3, OPC, PROFINET), and prioritize availability and deterministic performance [16]–[18]. These characteristics limit the applicability of traditional IT security measures.

Students must understand these constraints and how they shape defensive strategies. For example, patching a safety-critical control system may not be feasible. Similarly, introducing active scanning tools or intrusive monitoring can disrupt time-sensitive operations. The curriculum addresses these nuances through labs that simulate control system environments and require students to implement protections that respect operational constraints. Exercises include designing network segmentation strategies, applying role-based access controls, and configuring anomaly detection systems tailored to ICS traffic patterns.

The curriculum also emphasizes the importance of secure configuration and change management. In Week 7, students establish secure baselines for control systems, process simulated change requests, and implement controls for

portable media and mobile devices (PMMD). These labs reflect the operational realities of nuclear facilities, where even minor configuration changes can have significant safety implications. By the end of the course, students are expected to demonstrate the ability to design and defend OT/ICS environments that are both secure and compliant—balancing the constraints of legacy systems, the demands of nuclear safety, and the expectations of regulatory oversight.

E. Insider Threat Mitigation

Protecting nuclear facilities requires a combination of technical controls and strategies to mitigate insider threats. Technical measures include access management, network segmentation, role-based access control (RBAC), least privilege principles, and controls over PMMD. Equally important is insider threat awareness, which integrates both behavioral and cyber indicators to detect anomalous activity.

In Week 8, students design RBAC policies and simulate insider misuse scenarios. They analyze access logs, identify anomalies, and propose policy changes to strengthen separation of duties. These exercises are grounded in DOE and NRC guidance on insider threat programs and emphasize the importance of integrating behavioral analysis into cybersecurity monitoring [19], [20]. Week 10 builds on this foundation by introducing fusion analysis, where students correlate cyber indicators (e.g., unusual login times) with behavioral red flags (e.g., policy violations or financial stress). They complete insider threat case analysis reports and present their findings in peer-reviewed sessions.

These activities reinforce the idea that insider threats are not just technical problems but socio-technical challenges that require holistic detection and response strategies.

F. Incident Response and Recovery

Detection and response capabilities are critical for minimizing the impact of cyber incidents in nuclear facilities. Specialists must implement continuous monitoring, logging, and Security Information and Event Management (SIEM) systems specifically designed for OT and ICS environments to provide situational awareness and early anomaly detection. In Weeks 9–12, students configure SIEM tools, analyze simulated logs, and develop incident response playbooks. They participate in tabletop exercises that simulate malware infections, lateral movement, and regulator inquiries. These exercises require students to make real-time decisions, escalate appropriately, and document their actions in compliance with NRC reporting requirements [21].

Recovery is addressed in Weeks 13–14, where students restore compromised CDAs from backups, validate system integrity, and draft corrective action plans. They conduct post-incident reviews to identify root causes and propose improvements to governance, detection, and response protocols. This iterative approach ensures that facilities not only recover rapidly from incidents but also enhance their cybersecurity posture over time, reducing the likelihood of

recurrence and strengthening both operational effectiveness and regulatory compliance.

G. *Applied Integration and Capstone Simulation*

Applied integration is critical for translating theoretical, technical, and regulatory knowledge into practical expertise. The curriculum culminates in a capstone simulation (Week 15) where students participate in a Red Team/Blue Team exercise simulating a multi-vector attack on a fictional NPP.

Blue Teams must defend plant operations using the full spectrum of NIST CSF functions from governance and asset identification to implementing protections to detection, response, and recovery. They document their actions in incident logs, produce after-action reports, and reflect on gaps in their strategies.

This immersive experience reinforces the interconnectedness of technical, regulatory, and operational domains. It also provides a realistic preview of the challenges students will face in the field, ensuring they graduate with the confidence and competence to protect nuclear facilities from evolving cyber threats.

III. EDUCATIONAL FRAMEWORK RECOMMENDATIONS

To address the critical need for a specialized nuclear cybersecurity workforce, educational programs must align with established frameworks and integrate practical experiences. The National Institute of Standards and Technology's Cybersecurity Framework (NIST CSF) provides a structured approach encompassing Govern, Identify, Protect, Detect, Respond, and Recover functions, which can be mapped to the NRC's guidance in 10 CFR 73.54 and Regulatory Guide 5.71 [22]. These regulations mandate defense-in-depth strategies to protect digital assets associated with safety, security, and emergency preparedness (SSEP) functions, ensuring timely detection and response to cyber threats.

Experiential learning is vital for bridging theoretical knowledge with practical application. Training must include OT components such as Supervisory Control and Data Acquisition (SCADA) systems and Programmable Logic Controllers (PLCs), which are critical to nuclear plant operations and often targeted by cyber adversaries. Immersive simulations such as Red/Blue Team exercises, tabletop exercises, and case-based learning enable students to apply security principles to these control systems in realistic scenarios, enhancing problem-solving and incident response capabilities [11], [23].

Credentialing pathways, such as professional certificates, elective courses, continuing education modules, and eventually full specialization tracks, are essential for formalizing expertise in nuclear cybersecurity. Most U.S. institutions currently offer only general certificates in nuclear security or cybersecurity (e.g., Texas A&M University's professional certificate program). However, Idaho State University offers a rare, more flexible option. While the university does not offer a nuclear cybersecurity degree or

graduate-level specialization, students can pursue a two-year associate's degree in Nuclear Operations Technology and pair it with an intermediate technical certificate in industrial cybersecurity as part of a Bachelor of Applied Science in Cyber-Physical Systems.

This pathway illustrates how existing programs could be combined to approximate the type of interdisciplinary training needed in the field. Given the absence of dedicated nuclear cybersecurity degrees in the U.S., such hybrid approaches could help fill a critical gap by showing how institutions can creatively leverage existing resources. These efforts point toward the type of integrated educational models ultimately necessary to prepare professionals who are both technically competent and compliance-ready.

Institutional partnerships further strengthen workforce development. Collaborations with DOE national laboratories, regulators, and industry vendors play a pivotal role in providing real-world experience and fostering industry connections. These partners provide internships, co-ops, and research opportunities that expose students to real-world nuclear cybersecurity challenges, reinforcing regulatory compliance and operational readiness. By integrating these educational framework recommendations, educational institutions can effectively prepare a skilled workforce capable of addressing the complex challenges of nuclear cybersecurity.

IV. WORKFORCE DEVELOPMENT AND PIPELINE IMPLICATIONS

The nuclear industry faces a critical workforce development challenge, particularly in cybersecurity. Recent nuclear engineering graduates bring a solid understanding of plant operations but often lack the cybersecurity expertise necessary to protect CDAs. Conversely, as noted by INL industry experts, cybersecurity graduates often possess strong technical skills but require 12 to 18 months of retraining to acquire nuclear context, including familiarity with plant operations, regulatory requirements, and OT systems. This dual-gap challenge is further compounded by limited undergraduate exposure to nuclear cybersecurity, resulting in low awareness of the field as a potential career path. Coupled with an aging workforce and planned nuclear expansion, these factors underscore the urgent need for a multidisciplinary approach that integrates nuclear engineering, cybersecurity, and regulatory knowledge to develop a workforce capable of protecting CDAs, safeguarding sensitive operational environments, and ensuring regulatory compliance.

V. CONCLUSIONS

This paper identifies the core competencies essential for nuclear cybersecurity education, emphasizing the need for curricula that go beyond general OT/ICS training. In contrast, existing literature primarily highlights the critical need for cybersecurity in the nuclear sector and identifies gaps in current training programs. While these discussions underscore the urgency of developing a specialized workforce, they lack detailed guidance on the specific skills and

knowledge areas that educational curricula should encompass.

Neglecting these educational needs carries significant consequences. Retraining cybersecurity professionals to operate in nuclear environments is time-consuming and costly, delaying workforce readiness and increasing operational expenses. Overreliance on external consultants introduces inconsistency and potential vulnerabilities, while non-compliance with standards like 10 CFR 73.54 and Regulatory Guide 5.71 can result in regulatory penalties and reputational harm. Most critically, an underprepared workforce weakens the sector's resilience against cyber threats, leaving CDAs vulnerable to attacks.

Investing in a specialized, technically proficient workforce offers long-term advantages. A curriculum that integrates regulation, OT/ICS defense, nuclear engineering, insider threat mitigation, and incident response equips professionals to meet compliance requirements and adapt to evolving threats. By embedding these competencies into applied educational frameworks, institutions can accelerate workforce readiness and strengthen the cybersecurity posture of nuclear facilities. The time to act is now: building this workforce is critical to ensuring the secure and reliable future of nuclear energy.

REFERENCES

- [1] IEA, "The Path to a New Era for Nuclear Energy," 2025, International Energy Agency.
- [2] OECD-NEA, "SMR Dashboard (Edition II/III)," 2024/2025, Nuclear Energy Agency.
- [3] WNA, "Small Nuclear Power Reactors (SMRs): Overview," 2025, World Nuclear Association.
- [4] NRC, "Artificial Intelligence – NRC Activities and External Engagement," 2025, U.S. Nuclear Regulatory Commission.
- [5] NRC, "10 CFR 73.54: Protection of Digital Computer and Communication Systems and Networks," 2023, U.S. Nuclear Regulatory Commission.
- [6] NRC, "Regulatory Guide 5.71 (Rev. 1): Cyber Security Programs for Nuclear Power Reactors," 2023, U.S. Nuclear Regulatory Commission.
- [7] IAEA, "Computer Security at Nuclear Facilities (NSS No. 17)," 2011, International Atomic Energy Agency.
- [8] IAEA, "Computer Security at Nuclear Facilities: Technical Guidance (NSS No. 17-T, Rev. 1)," 2015, International Atomic Energy Agency.
- [9] IAEA, Computer Security for Nuclear Security, ser. IAEA Nuclear Security Series No. 42-G. International Atomic Energy Agency, 2021.
- [10] IAEA, "Model Academic Curriculum in Nuclear Security (2nd ed.)," 2022, International Atomic Energy Agency.
- [11] DOE, "National Cyber-Informed Engineering Strategy," 2022, U.S. Department of Energy.
- [12] S. G. Freeman, C. St Michel, R. Smith, and M. Assante, "Consequence-driven cyber-informed engineering (CCE)," Idaho National Laboratory, Idaho Falls, ID (United States), Tech. Rep., 10 2016.
- [13] MITRE, "ATT&CK for ICS," <https://attack.mitre.org>, n.d.
- [14] INL, "Consequence-driven, Cyber-informed Engineering (CCE) (fact sheet/white paper)," 2023, Idaho National Laboratory.
- [15] NEI, "NEI 08-09, Revision 7: Cyber Security Plan for Nuclear Power Reactors," 2023, Nuclear Energy Institute.
- [16] 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.
- [17] K. Stouffer, J. Falco, and K. Scarfone, "Guide to industrial control systems (ics) security," National Institute of Standards and Technology, Tech. Rep., 2011.
- [18] Kumar, "Cybersecurity in industrial control systems: Best practices & threats," Cyber Tech Journals, 2025.
- [19] U.S. Department of Energy, "DOE Order 470.5A: Insider Threat Program," December 2024, approved December 6, 2024. [Online]. Available: <https://www.directives.doe.gov/directives-documents/400-series/0470.5a-border>
- [20] NRC, "Regulatory Guide 5.77, Revision 1: Insider Mitigation Program," 2022, U.S. Nuclear Regulatory Commission.
- [21] NRC, "Regulatory Guide 5.83, Revision 1: Cyber Security Event Notifications," 2023, U.S. Nuclear Regulatory Commission.
- [22] NIST, "SP 800-82 Rev. 3: Guide to OT Security," 2023, National Institute of Standards and Technology.
- [23] M. Bada, A. Sasse, and J. R. C. Nurse, "Cyber Security Awareness Campaigns: Why do they fail to change behaviour?" <https://arxiv.org/pdf/1901.02672>, 2019.
- [24] M. Nelson, A. Christian, T. Haney, and C. Nickerson, "Mapping the gap: Analysis of nuclear cybersecurity education in U.S. universities," Pending publication.