Building Nuclear-Specific Cybersecurity Expertise in Higher Education

Amorita A. Christian, University of Tulsa
Myles Nelson, University of Texas at Dallas
Tiffany Haney, Idaho National Laboratory
Charles Nickerson, Idaho National Laboratory

November 12-14, 2025

Cyber Fellows

THE UNIVERSITY of TULSA

Partners


THE UNIVERSITY of
TULSA


Cyber
Fellows


OCII
Oklahoma Cyber
Innovation Institute


INL
Idaho National Laboratory

The New World of Nuclear

- Significant transformation
  - Modernization of legacy nuclear power plants
  - Increased momentum behind Advanced/Small Modular Reactors (A/SMRs)
  - AI-fueled energy demand, with corporate investment from leaders like Microsoft and Amazon
  - Stakes in nuclear operations are uniquely high
- Unique compliance and governance obligations
- Digitalization introduces new cyber risks

Why Specialization is Needed

- General cybersecurity education is insufficient
- Stakes in nuclear operations are uniquely high
- Nuclear facilities operate in a multi-layered regulatory ecosystem
- Cybersecurity professionals' competencies must extend beyond traditional information technology (IT) and operational technology (OT)
- Urgency heightened by workforce challenges and evolving cybersecurity practices

What Nuclear Cybersecurity Specialists Need to Learn

- Cybersecurity foundations
- Nuclear engineering context
- Regulatory and governance literacy
- OT/ICS security in the nuclear context
- Insider threat mitigation
- Incident response and recovery
- Applied integration and capstone simulation

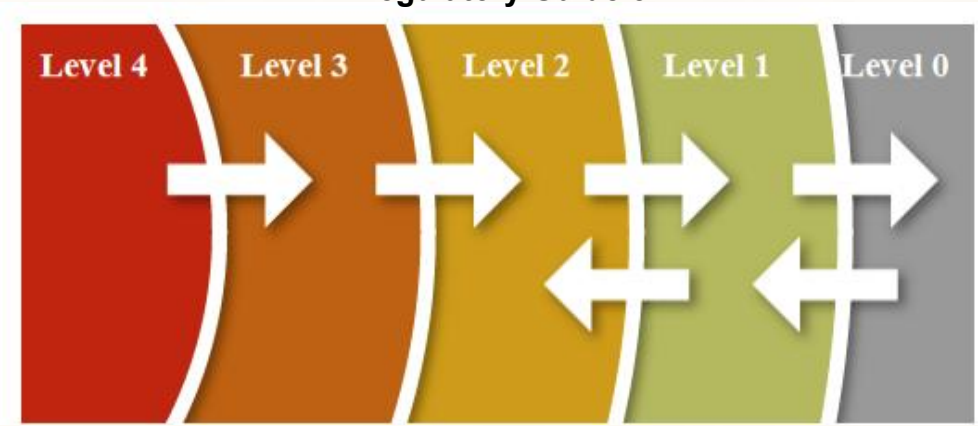
Educational Framework Recommendations

- National Institute of Standards and Technology's Cybersecurity Framework (NIST CSF)
- Nuclear Regulatory Commission (NRC)
  - 10 Code of Federal Regulations (CFR) 73.54
  - Regulatory Guide (RG) 5.71
- Nuclear Energy Institute (NEI) 08-09
- Training on OT components
- MITRE ATT&CK for ICS
- Consequence-driven, Cyber-informed Engineering (CCE)
- Immersive simulations
- Credentialing pathways
- Institutional partnerships

Sample Curriculum

- Weeks 1 & 2 — Foundations & Governance
- Weeks 3-5 — Identify
- Weeks 6-8 — Protect

NRC Regulatory Guide 5.71



Introduction to the regulatory landscape
Asset identification & classification
Threat vectors & attack paths
Consequence & risk assessment
Design access control matrices
Implement network segmentation strategies
Establish secure baselines for control systems
Process simulated change requests
Implement controls for portable media & mobile devices

Sample Curriculum

• Weeks 9-12	Detect & Respond	Configure Security Information & Event Management tools Analyze simulated logs Develop incident response playbooks
• Weeks 13 & 14	Recover	Restore compromised digital assets from backups Validate system integrity Draft corrective action plans Conduct post-incident reviews
• Week 15	Capstone Simulation	Red Team/Blue Team exercise simulating a multi-vector attack on a fictional nuclear power plant

Conclusion

- Planned nuclear expansion
- Aging workforce: retirement outpacing replacement
- Limited undergraduate exposure to nuclear cybersecurity
- Nuclear engineering graduates
  - Solid understanding of nuclear power plant operations
  - Limited/No cybersecurity expertise
- Cybersecurity graduates
  - Strong technical skills
  - Require several months of retraining to acquire nuclear context
- Opportunity for universities to develop programs to meet the workforce demands of planned nuclear expansion

Thank You

Amorita A. Christian
MS, MBA, PMP

amorita-christian@utulsa.edu

www.utulsa.edu

Cyber Fellows