NCyTE CENTER
National Cybersecurity Training & Education Center

NCyTE FACULTY EXTERNSHIP PROGRAM:

2025 ANNUAL REPORT

Connecting Cybersecurity Faculty with Industry

PROGRAM YEAR 2025

AUTHOR

Kyle Jones

Department of Information Technology,
Sinclair Community College

Prepared from participant final reports, program records, and applicant data.

Table of Contents

ABOUT THIS REPORT

This annual report documents the 2025 NCyTE Faculty Externship Program and its impact on participating faculty, their institutions, and the broader cybersecurity education community. Drawing on participant final reports, program records, applicant data, and host engagement, it highlights externship experiences, curriculum innovations, industry partnerships, and operational improvements. Beyond capturing the accomplishments of the 2025 cohort, this report establishes a benchmark for measuring future program growth and continuous improvement.

Executive Summary

In 2025, the NCyTE Faculty Externship Program placed ten cybersecurity and information technology faculty members inside working industry environments for a minimum of 80 on-site hours each. Drawn from a competitive pool of 39 applicants across 17 states, the cohort represented community colleges and universities in seven states and completed externships with nine host organizations spanning steel manufacturing, managed security services, global telecommunications, cybersecurity advisory, systems modeling, and national laboratory research.

The program's central purpose is to close the gap between classroom instruction and current industry practice. The outcomes were strongly validated by the participants. Faculty consistently reported that the experience is reshaping how they teach: away from certification-only preparation and toward practice-focused instruction that blends technical skill with documentation, communication, governance, ethical judgment, and structured decision-making. Every completing participant returned with strong curriculum changes planned for the 2025–26 academic year, and most secured lasting industry partnerships that will bring guest speakers, internships, site visits, and professional tools into their classrooms.

39	10	17	7	80+
Applicants	Participants	Applicant States	Participant States	On-Site Hours Each

Program Overview

The Faculty Externship Program connects educational institutions with industry partners to give instructors direct, hands-on exposure to real-world cybersecurity operations. Faculty participants commit to a minimum of 80 hours on-site during the summer, engaging in group meetings, one-on-one interviews, facility tours, research, and project contributions. Each externship must be completed, verified, and documented in a comprehensive final report. This includes clear recommendations for new processes, procedures, or curricula delivered by the September 30, 2025, deadline. Participants are further required to develop pedagogical goals before the externship begins, share their experience with departmental colleagues, and deliver a fall-semester presentation covering the host company, the externship experience, and the resulting curriculum changes.

2025 Selection Pipeline

Applications Received	39 faculty from 17 states
Review Panel	8 reviewers scored each applicant (1–5 scale) on qualifying criteria and program fit
Qualifying Criteria	Full-time faculty status; 80-hour commitment; on-site availability; administration approval; comfort in manufacturing environments; MEP familiarity
Cohort Selected	10 faculty from 7 states, placed with 9 industry hosts
Completion Window	Summer 2025, with reports and verification due September 30, 2025

Applicant interest in 2025 was strong and geographically broad, with the 39 applicants representing institutions in Alabama, California, Connecticut, Florida, Illinois, Indiana, Iowa, Louisiana, Massachusetts, Maryland, Michigan, Minnesota, North Carolina, Ohio, Tennessee, Texas, and Washington. An eight-member review panel scored applicants against qualifying criteria and each candidate's written statement of fit. Program administration also refined its operations during the year: acceptance and rejection letter templates were standardized, a candidate tracking sheet monitored each participant's document milestones (questionnaire, acknowledgment letter, résumé, bio, and final report), and planning discussions explored future directions such as an adjunct-faculty pathway and energy-sector placements under Department of Energy funding.

The 2025 Cohort

Ten faculty members were selected and matched with host organizations, in most cases arranged through their own advisory boards, local business networks, or regional Manufacturing Extension Partnership (MEP) offices. The cohort and placements were as follows:

Cohort Placements

Faculty Participant	Home Institution	Externship Host	Host Location
Thomas "Tony" Brown	Forsyth Technical Community College (NC)	NOCDOC	Winston-Salem, NC
Yaritza Garcia-Rivera	Houston Community College (TX)	Cyber Point Advisory, LLC	Houston, TX
Doug Hampton	Sinclair Community College (OH)	Tenet3	Dayton, OH
Tony Hills	Northwest State Community College (OH)	North Star BlueScope Steel	Delta, OH
M. Ajmal Khan	Ohio Northern University (OH)	Business Technology Management Group, USA	Aurora, IL
Andrew Leiren	South Puget Sound Community College (WA)	Intelligent Technical Solutions	Olympia, WA
Michael Olaolu-Arowolo	Xavier University of Louisiana (LA)	Idaho National Laboratory	Idaho Falls, ID
Adeoye Olaoluwa	Prince George's Community College (MD)	Digital Global Hub	—
Diego Tibaquira	Miami Dade College (FL)	Telefónica Tech Americas	Miami, FL

Externship Highlights

Inside a Steel Mill: Tony Hills - North Star BlueScope Steel

Tony Hills, cybersecurity faculty at Northwest State Community College, embedded with the IT, Operational Technology (OT), and Industrial Control Systems (ICS) teams at North Star BlueScope Steel, an electric arc furnace steel mill in Delta, Ohio. Stationed among the plant's security personnel, he observed live security investigations, learned how centralized logging and Endpoint Detection and Response (EDR) platforms drive incident management, and — in full personal protective equipment — participated directly in an upgrade of the fault-tolerant, fiber-optic communication ring supporting the melting furnaces. All four of his stated learning goals were met, and the experience is driving new course content on EDR platforms, administrative controls, and cybersecurity policy, alongside a commitment to bring North Star into his classroom to discuss student internships.

Mapping Cybersecurity Careers: Diego Tibaquira - Telefónica Tech

Diego Tibaquira, Professor of Computer Science at Miami Dade College, completed his externship with Telefónica Tech Americas, a global cybersecurity and cloud services firm. He conducted one-on-one interviews with three senior executives and twelve engineers, analysts, and architects to build detailed job-role profiles covering tools, skills, certifications, and career pathways — including the value of bilingual fluency in global operations. From these insights he developed a comprehensive Canvas course with modules on professional skills, certifications, résumé development, interview readiness, and 24/7 datacenter work expectations. The partnership produced immediate classroom collaboration: Telefónica's Head of IT Services and Operations visited his classes and performed a live social-engineering demonstration, and invitations followed for datacenter visits and potential travel to Latin American facilities, including the Bogotá Digital Operations Center. Findings will be shared across all eight Miami Dade College campuses.

Additional Placements Across the Cohort

- **Thomas "Tony" Brown (Forsyth Tech)** — At NOCDOC, a managed service provider and advisory-board partner, he took a deep dive into industry frameworks — ITIL, FCAPS, CIS Controls, MITRE ATT&CK, NIST, the OODA loop, and PMI — and identified structured decision-making as a critical gap in current coursework.
- **Yaritza Garcia-Rivera (Houston CC)** — At Cyber Point Advisory, a fractional-CISO advisory firm, she gained a governance-level view of cybersecurity — policy development, risk assessment, and technology-agnostic client guidance — and joined the firm's weekly "Cybersecurity Circle," a community forum she now plans to open to her students.
- **Doug Hampton (Sinclair CC)** — At Tenet3 in Dayton, he explored digital-twin system modeling and the Metra cloud platform within AWS and AWS GovCloud, and secured free student access to Tenet3's software for his Securing a Microsoft Network course — where students will now protect a real legacy Windows XP sock-knitting machine mapped in a simulated enterprise network.
- **M. Ajmal Khan (Ohio Northern)** — Conducted a comprehensive network vulnerability assessment in an industrial setting using Nessus and Nmap, demonstrated the risk of unpatched legacy systems through controlled exploitation, and developed segmentation and firewall mitigation strategies he will now convert into scenario-based labs.
- **Andrew Leiren (South Puget Sound CC)** — At Intelligent Technical Solutions, an MSP, he investigated skills students need to stand out after graduation and identified classroom-ready tools including the any.run malware sandbox, the Wazuh open-source SIEM/XDR platform, and Dataiku for teaching AI concepts.
- **Adeoye Olaoluwa (Prince George's CC)** — Explored virtual Security Operations Center (SOC) concepts and SIEM integration — including proposals for real-world SOC practices supporting public-sector modernization in Africa — and is now building an open-source home SOC lab as a model for a cost-effective student training environment; he has also arranged a second externship with apiphani.com to deepen tool exposure.
- **Michael Olaolu-Arowolo (Xavier University of Louisiana)** — Completed his externship with Idaho National Laboratory, gaining exposure to data protection strategy, cloud-based security, and threat intelligence, and broadening his perspective on how health informatics intersects with cybersecurity.

What the Cohort Learned

- Cross-Cutting Themes -

Analysis of the final reports surfaced remarkably consistent themes across participants, regardless of host sector. Five stand out:

- **Workforce Readiness Over Test Preparation** — Participants are shifting from certification-driven instruction to a practice-focused model that blends technical learning with reasoning and ethical judgment, helping students think like practitioners.
- **Documentation and Communication Are Foundational** — Across every site, strong documentation and direct cross-team communication emerged as foundational professional skills — in one participant's words, a contractor identified documentation as the single most critical skill in the field. Several faculty will now grade documentation and reporting as core competencies.
- **Governance Mindset, Not Just Tooling** — Exposure to CISO-level strategy clarified that cybersecurity is as much about policy, risk, and oversight as it is about technology. Faculty plan structured integration of governance, frameworks (NIST, MITRE ATT&CK, ITIL, CIS Controls), and decision-making exercises into coursework.
- **AI and Automation Are Reshaping Operations** — Participants observed AI adoption ranging from department-wide initiatives to skepticism, but agreed that AI and automation are transforming productivity expectations — underscoring the need for responsible-AI instruction and continual upskilling.
- **Applied, Hands-on Learning Drives Job Readiness** — Project-based work with clear, actionable reporting emerged as the clearest marker of job readiness. New labs and simulations will integrate AI-driven tools, automation, open-source platforms, and cloud systems so coursework mirrors current industry practice.

Challenges Identified

Participants reported few barriers during the externships themselves, but several practical challenges affect classroom integration: limited time on site to observe operations in depth; the difficulty of finding industry hosts willing to sponsor an externship; a technology gap between academic lab tools and professional-grade platforms; tight course schedules that make it hard to layer in new labs, case studies, and guest speakers; students who enroll primarily to pass certification exams; low student engagement in clubs and competitions outside class; and inconsistent ethics coverage across programs. Faculty responses include modular course redesign (pairing each core topic with a lecture, lab, and applied component), advocating for software licenses and cloud credits, and pushing for dedicated ethics modules or courses.

Classroom Integration: Challenges vs. Responses

	CHALLENGES (PRE- & POST-EXTERNSHIP)	STRATEGIC FACULTY ACTIONS
STRUCTURAL & SCHEDULING	• **LIMITED SITE TIME** — Short duration restricts deep operational insight • **TIGHT COURSE SCHEDULES** — Difficult to integrate new labs, cases, and guest speakers	→ **MODULAR COURSE REDESIGN** — Pairing each core topic with Lecture, Lab, and Applied components to maximize efficiency
RESOURCES & PARTNERSHIPS	• **TECHNOLOGY GAP** — Disparity between academic tools and professional-grade platforms • **DIFFICULTY FINDING HOSTS** — Fewer industry partners willing to sponsor externships	→ **RESOURCE ADVOCACY** — Pushing for corporate software licenses, cloud credits, and institutional resource support
STUDENT ENGAGEMENT	• **CERTIFICATION FOCUS** — Students enroll primarily to pass exams • **LOW CLUB PARTICIPATION** — Minimal extra-curricular involvement	→ **CURRICULUM REALIGNMENT** — Shifting focus from test-prep to highly applied, workforce-ready project competencies
PROGRAM ETHICS	• **INCONSISTENT ETHICS COVERAGE** — Variations across academic programs	→ **TARGETED ETHICS MODULES** — Developing and integrating dedicated, standardized ethics content and courses

Curriculum Impact 2025-26

Every completing participant returned with specific, implementable curriculum plans. Representative commitments include:

- **Northwest State** will dedicate 25% of CYB220 Security Auditing to policy and administrative controls, add documentation templates to Microsoft Server Technology, and pilot labs using any.run, Wazuh, and MFA.
- **Forsyth Tech** will add a decision-making module, MSP-inspired scenario labs with peer critique, and LinkedIn/résumé exercises aligned with workforce expectations.
- **Houston Community College** will integrate GRC, policy, and ethics concepts into coursework, expand CTF activities using Raspberry Pi, pfSense, and IoT devices, and pursue a dedicated cybersecurity ethics course.
- **Sinclair College** will redesign its CIS 2630 project around digital-twin modeling and legacy-system risk management using Tenet3 software.
- **Ohio Northern** will enhance its network security course with vulnerability assessment, penetration testing, network segmentation, ransomware case studies, and an IoT security project.
- **Miami Dade** will launch a Canvas course covering soft skills, career preparation, certifications, and datacenter expectations, with assessments tracking student outcomes across eight campuses.
- **Prince George's** will develop virtual SOC and SIEM labs using Wazuh, add system hardening and endpoint monitoring exercises, and pursue funding for a college SOC lab.

Faculty will measure impact through evidence-based syllabus audits, pre- and post-assessments, student surveys and course evaluations, the quality of graded deliverables (lab reports, policy drafts, after-action reports, presentations), industry certification attainment, and ongoing advisory-board review — an intentional, data-informed approach to continuous improvement.

Partnerships & Networking

Beyond curriculum, the 2025 externships generated durable industry relationships with direct student benefits:

- **North Star BlueScope Steel** committed to classroom visits at Northwest State to discuss student internships, several employees volunteered as guest speakers, and the cybersecurity team leader will be invited to join the college's IT advisory committee.
- **Telefónica Tech's** Head of IT Services and Operations visited Miami Dade classes for live demonstrations, and students have been invited to the datacenter, with potential visits to the Boca Raton submarine cable landing station and Latin American facilities.
- **Tenet3** granted free software access for Sinclair students, effectively bringing a professional systems-modeling platform into the classroom at no cost.
- **Cyber Point Advisory's** weekly Cybersecurity Circle is now open to Houston Community College students as a standing mentorship and networking venue.
- **Advisory-board** ties deepened at Forsyth Tech, where the externship supervisor is helping refine new lesson plans, and internship pipelines and hiring pathways were strengthened at multiple sites.
- One participant is extending the experience through a second externship (apiphani.com) to broaden tool exposure for students — evidence that the program is seeding ongoing faculty-industry engagement rather than one-time visits.

Program Evolution & Future Directions

Operationally, 2025 brought a more structured review process (an eight-member ranking panel with standardized 1–5 scoring), consolidated letter templates, and milestone-based candidate tracking.

Planning conversations during the year identified several forward-looking opportunities:

- **Developing a pathway for adjunct faculty and aspiring instructors**
- **Converting cohort report outcomes into formal research documents under a dedicated part-time project manager**
- **A potential future model in which energy companies request placements and the program recruits faculty in their regions under Department of Energy funding, potentially widening eligibility beyond community colleges**

The 2025 results make a strong case for the program's continuation and growth. Applicant demand (39 applications for 10 seats) far exceeds capacity, completion quality was high, and participants described the experience in unambiguous terms—one calling it "something every faculty member should do" to remain current with industry expectations. With standardized processes now in place, the 2025 cohort provides both a playbook for future implementation and a benchmark for the 2026 program year.

NCyTE CENTER

National Cybersecurity Training & Education Center

The **National Cybersecurity Training and Education Center (NCyTE)** at Whatcom Community College, funded by the NSF, enhances U.S. cybersecurity education by supporting faculty, developing resources, and strengthening industry partnerships to build the cybersecurity workforce.

The National Cybersecurity Training and Education Center is funded by the National Science Foundation grant #2054724.