



**WiCyS 2025**  
**Call for Presenters (CFP)**  
**Supplementary Information**

# CALL FOR PROPOSAL (CFP)

## Tracks

The 2025 WiCyS annual conference will have five different tracks. CFP submissions can be related to anything within the five tracks that would be valuable to WiCyS attendees.

- **Technical Skill Building** - (technical skill development in all areas of security and/or privacy)
- **Education & Workforce Development** - (all levels of cybersecurity education and training programs, strategies and initiatives for current and upcoming job demand)
- **Research & Innovation** - (includes research, entrepreneurship and trends in emerging technologies)
- **Career Advancement & Management** - (includes internships, apprenticeships and being hired, leadership, career development/growth, and work-life balance)
- **Community EcoSystem & Outreach** - (includes collaborations/partnerships and diversity, equality, inclusion & accessibility (DEIA) efforts)

# CFP Timeline

**Submissions Open:** September 9, 2024

**Submission Deadline:** November 4, 2024

(Student posters are open until January 6, 2025)

Both close at 5:00 CT of date noted above.

**Notification of Status:** December 16, 2024

(Student research posters will be sent January 17, 2025)

# CFP Categories

- **Birds of a Feather (BoaF)** (45 minutes)
- **Lightning Talks** (5 minutes)
- **Panels** (45 minutes)
- **Presentations** (45 minutes)
- **Workshops** (120 minutes)
- **Student Posters**

# Proposal Content

## **Abstract (Required):**

- Overview that describes the offering
- Published in conference program
- Limited to 250 words

## **Outline (Required):**

- Additional relevant information
- Articulates plan/outline of presentation
- NOT to be published
- Limited to 500 words

## **Author Information (Blind):**

- Author experience/qualification related to the topic
- CANNOT mention name or company/affiliation of author(s)

# **Submissions must be submitted through the WiCyS CFP platform.**

- Submitters need to identify the type of submission: Birds of a Feather, Lightning Talk, Panel, Presentation, Workshop, or Student Research Poster.
- Submitters also must identify which tracks: Technical Skill Building, Education & Workforce Development, Research & Innovation, Career Advancement & Management, and Community EcoSystem & Outreach. Multiple tracks can be selected. No track is required for Student Research Poster.
- Please do not include ANY names or affiliations in the abstract since all reviews are anonymized.
- An abstract is limited to 250 words that highlight the proposed session.
- An outline of the proposed session should also be submitted for review but will not be published.

# General Tips for Proposal Submissions

## Relevant and Specific

- To topics in cybersecurity and privacy
- Matched to one or more tracks and tailored to the category
- To career development/advancement of cyber professionals
- Not everything needs to apply to females in cybersecurity
- No “vendor” pitch

## To the point (Not lengthy)

- Describe specifically what the presentation will address
- Try to be within 250 words for overview/abstract (to be published in the conference program)
- May provide additional information about presentation outline
- Absolutely NO information about author(s)/presenter(s) identity (name or affiliation/association of institution/company) in the body of proposal (may talk about experience/qualifications)

## Written in Third-person

- Example:
  - Don't say: I will talk about it
  - Do say: This talk will present/discuss

# Tips for Competitive Proposals

- Timely
- Innovative
- Unique perspective
- Clear, specific and concise description of presentation
- No author bio/information



# Workshops



## WORKSHOPS

Workshops are free hands-on sessions (technical / professional development) on any topic related to cybersecurity. Hands-on workshops in any cybersecurity area are welcome. Workshops are 2 hours long.

### **Your 1st Time at WiCyS? Join Us For Insiders' Tips for Navigating WiCyS!**

#### **TRACK: BEST PRACTICES**

Elizabeth K Hawthorne, *Rider University*; Kim Huynh, *Microsoft*; Felicia Jackson, *Raytheon*; Marena Soulet, *Tennessee Technological University*; Laura Sturgeon, *Smoothstack/Bloomberg*; Comfort Uduebholo, *Amazon Web Services*

Attending a WiCyS conference for the first time can be both exciting and daunting. There is just so much to navigate through in little time! Join us in this session, if this is your 1st time at the WiCyS conference. As panelists from various backgrounds and interests, we will share our experiences of what we found useful, what matters, and most importantly how you can get the most out of this experience as a first-time WiCyS attendee.

### **SEED Labs: Hands-on Labs for Cybersecurity Education**

Wenliang (Kevin) Du, *Syracuse University*

#### **TRACK: TODAY'S TECHNOLOGY AND CHALLENGES CPE**

#### **CREDITS: 2**

To improve students' hands-on skills in cybersecurity, over the last 20 years this presenter has developed roughly 40 labs called SEED labs. Today, over 1,000 institutes worldwide are using them in their cybersecurity curricula. Many companies also are using the labs for their internal training and interviews. In this workshop, the presenter will give an overview and demonstrate several labs before guiding participants through some. Participants need to download the provided SEED VM beforehand, as all labs will be conducted inside the VM. Educators, students, professionals and researchers are welcome to attend this workshop.

# Tips for Workshop Sessions

- 26 slots available
- 2 hours long
- Maximum 4 presenters
- Assume that audience will bring their own laptops
  - Any additional hardware needs to be provided at the venue
  - Any additional software needs to be provided before the conference
- Assumptions about participants must be articulated
  - Pre-reg knowledge/skill
  - Certain groups

The first listed presenter receives complimentary registration and two nights of complimentary lodging.

The second listed presenter receives complimentary registration and does not receive complimentary lodging.

Other listed presenters do not receive complimentary registration or lodging; they receive early registration.

Only presenters in attendance will be listed for the session.

# Birds of a Feather (BoaF)



## BIRDS OF A FEATHER (BoaF)

Birds of a Feather are informal discussion sessions on just about any topic related to cybersecurity, that elicit participant discussions. These sessions can be a great way to share ideas and be introduced to current issues or trends. BoaF sessions are 45 minutes long.

### **Cultivating Women as Leaders - The Role of Allyship**

Kip Bates, *University of California, Santa Barbara*; Reema Moussa, *University of Southern California, Gould School of Law*

#### **TRACK: BEST PRACTICES**

Everyone has heard the stats -- with only 25% representation, there simply aren't enough women in cybersecurity. Another dominant problem often overlooked is women's retention and leadership in cyber, which contributes significantly to the disparity between the prevalence of women and men in the cybersecurity field. Join Reema Moussa and Kip Bates for this roundtable discussion on the importance of male allyship in fostering women's leadership in the cybersecurity sphere. In this Birds-of-a-Feather session, participants will be encouraged to discuss their experiences and perspectives on how to instill in their organizations the mission of promoting women in cybersecurity and how it isn't solely a women's issue but a priority for everyone in the cybersecurity field.

### **Cybersecurity Academic Integration Through Outreach**

Joan Labay-Marquez, *University of the Incarnate Word*

#### **TRACK: BEST PRACTICES**

This Birds-of-a-Feather session will discuss how to integrate cybersecurity awareness through outreach programs that include additional degree programs within the institution to support a department's CAE-CD application for designation as a National Center of Academic Excellence in Cybersecurity. Presenters will discuss CAE-CDE program eligibility requirements and demonstrate how to incorporate a cybersecurity awareness community outreach program with a service-learning focus to support the submission of an application for the Program of Study validation component, part one of a two-part process for designation. The CAE-CDE Program is open to current regionally accredited four-year colleges and graduate-level universities; its goal is to promote and support quality academic programs of higher learning that help produce the nation's cyber workforce.

# Tips for BoaF Sessions

- 5 slots available
- 45 minutes long
- Maximum 2 presenters
- Must be interactive
- Must assume audience interaction throughout the whole session

The first listed presenter received complimentary registration and does not receive complimentary lodging.

Other listed presenters do not receive complimentary registration or lodging.

Only presenters in attendance will be listed for the session.

# Presentations



## PRESENTATIONS

Presentations highlight innovations, research & development projects, internships/ co-ops experiences, service learning and outreach projects, or other experience related to cybersecurity. Presentations are 45 minutes long, including time for Q&A.

### **Protecting America's Defense Industrial Base with Cybersecurity Services**

*Kristina Walter, National Security Agency*

#### **TRACKS: LOOKING AHEAD, BEST PRACTICES**

**CPE CREDITS: 1**

For the better half of a century, the National Security Agency/ Central Security Service (NSA/CSS) has led the U.S. government in cryptology and signals intelligence (SIGINT) missions. In partnership with the Department of Defense (DoD) Chief Information Officer (CIO), NSA is actively engaged in lending its technical expertise to identify, mitigate and eradicate threats to the U.S. Defense Industrial Base (DIB). The DIB represents a large and diverse target set for America's key global adversaries who thrive on the theft of intellectual proprietary, defense information and program insights. This presentation will present the compelling story behind NSA's burgeoning DIB cybersecurity mission, one that involves actively collaborating and sharing cyber threat information to disrupt adversaries' attempts to steal critical information and protect industry partners. It also will explain how a new model of provisioning cybersecurity services to DIB companies at scale dramatically expands DoD's security umbrella and the near-term strategy plans for NSA's newest mission focus.

### **Diversity is a Result of Inclusive Cultures**

*Deidre Diamond, CyberSN and Secure Diversity*

#### **TRACKS: TODAY'S TECHNOLOGY AND CHALLENGES, BEST PRACTICES, SMART ABOUT "SMART" THINGS**

**CPE CREDITS: 1**

An advanced society requires complex human interactions. Teamwork skills are needed at a greater scale than ever before. This means emotional intelligence or "EQ skills" need strengthening. Developing EQ starts with the desire to learn combined with the right tools to do so! This talk centers on a nine- piece framework, the Standards of Inclusive Behavior, to help participants create inclusive cultures that will result in diverse workplaces. The presenter will explore how each of the nine standards for interactions impact professional environments and how to use this framework to create equality and diversity of thought. Security, privacy, economic well-being and mental health depend on the ability to engage others positively, yet this is a skill that employers rarely teach. When establishing a baseline of standards for human interactions that are framed through the window of cybersecurity, teams and organizations can excel because expectations are clear and fair.

# Tips for Presentation Sessions

- 34 slots available (includes 8 Career Talks)
- 45 minutes long
- Maximum 2 presenters
- Audience interaction is limited to 10 min Q&A

The first listed presenter will receive complimentary registration with two nights of lodging.

Second listed presenter receives complimentary registration and does not receive complimentary lodging.

Only presenters in attendance will be listed for the session.

# Lightning Talks



## LIGHTNING TALKS

Lightning talks highlight fresh ideas, unique perspectives, valuable experiences, and emerging trends in cybersecurity. Lightning Talks are 5-minute presentations that aim to jump-start discussions and collaborations while soliciting feedback from the community.

### **Economics and Ethics Behind Successful Free and Open Source Security Projects**

*Olivia Gallucci, Rochester Institute of Technology*

Many organizations use Free and Open Source Software (FOSS) to build products and implement procedures. Yet, there is a lack of understanding, acknowledgment and support of the FOSS community in the cybersecurity industry, creating gaps in security knowledge. This presentation by Olivia Gallucci and professor Stephen Jacobs explores the relationship between FOSS and closed-source vulnerabilities, FOSS lifecycles, and FOSS security trends in projects including and excluding Freedom 3 (i.e., the ability to redistribute modified programs). It also examines the social workings and economic development behind successful FOSS projects and communities. The goal of this research was to document the history of FOSS projects, illustrate how organizations use FOSS projects, and determine effective security practices. The research highlights the importance of FOSS in cybersecurity, including things like documentation, collaboration and human rights. Research methods include an extensive reading of published research, journal articles, statistics, CVEs, and press articles on security threats and mitigations.

### **Ditch the Dichotomy: Embrace the Rainbow**

*Kaitlyn Bestenheider, RSM US, LLP*

While new to the field, novice cyber professionals are constantly taught in dichotomies: Red Team vs. Blue Team. Black Hat vs. White Hat. These dichotomies divide people and are not truly reflective of the various roles and mindsets it takes to address the robust cybersecurity landscape. Using basic color theory and the NIST NICE Framework, Kaitlyn will present a better model to show the full spectrum of career options within the cybersecurity rainbow.

# Tips for Lightning Talk Sessions

- 16 slots available
- 2 sessions of 8
- Must be within 5 minutes
- Maximum 1 presenter
- Great for new speakers
- Can be about work-in-progress
- Concurrent with other sessions

The first listed presenter receives complimentary registration and does not receive complimentary lodging.

Only presenters in attendance will be listed for the session.



# Panels



## PANELS

Panels provide opportunities to discuss a current relevant topic in cybersecurity. Panel organizers are responsible for selecting appropriate panelists to participate. In addition to the moderator, there can be up to 4 panelists, and each panel is 45 minutes long.

### **The Power of Six: Creating Cyber Experiences and Building a Talent Workforce Pathway for Women and Underrepresented Students**

Laura Freeman, *Virginia Tech National Security Institute*;  
Sharon Hamilton and Lauren Provost, *Norwich University*;  
Linda Riedel, *The Citadel*

#### **TRACK: BEST PRACTICES**

In 2017, six universities joined together (Power of Six) to establish a pilot program to demonstrate their ability to develop cybersecurity talent pathways for women and underrepresented students for civilian and military positions in the Department of Defense (DoD). Norwich University, University of North Georgia, The Citadel, Texas A&M, Virginia Tech and Virginia Military Institute share a common identity as senior military colleges but had never previously teamed up to create and fund academic, experiential and research opportunities for cybersecurity students. In 2018, the Power of Six built bipartisan federal support of senators and congresspersons to insert language in the 2019 National Defense Authorization Act to establish DoD Cyber Institutes.

### **The Skills Gap Wish List: Students, Industry and Academia**

Dr Brandy Harris, Pam Rowland, Niya Patterson, and Irene Vallalabos  
*Grand Canyon University*; Tamyria Williams, *TWC CORE Consulting, LLC*

#### **TRACK: BEST PRACTICES**

I wish you knew....” This conversation started at the 2021 WiCyS conference with industry partners sharing the gaps they have experienced when hiring students as interns or new hires. Students also have been asking, “What can I do to prepare myself for a career that will set me apart?” Academia is eager to help fill the skills gap and educate students to be prepared professionals. This panel will discuss specific needs, strategies and opportunities for student success. INDUSTRY - this is the time to share with academia and students the key skills and knowledge needed to fill the gaps seen in new hires and interns. ACADEMIA - this is the time to hear from students and industry on how to better prepare students for success. STUDENTS - share what to do and learn how to set themselves apart and become better prepared for a career in this exciting field. Together, key takeaways will be produced that can be shared with the entire community. Students will walk away with creative ideas on how to position themselves for success. Industry will provide specific ways that students can prepare for the field and make connections with some of the brightest and most engaged students. Academia will take away strategies as the conduit between students and industry.

# Tips for Panels

- 5 slots available
- 45 minutes long
- Maximum 4 panelists and 1 moderator
- Panelists with different backgrounds and viewpoints on the topic
- Clear takeaways from the panel discussion

Moderator receives complimentary registration and does not receive complimentary lodging.

Up to three panelists receive reduced rate conference registration (\$300) and do not receive complimentary lodging.

Only presenters in attendance will be listed for the session.

# Student Posters



## POSTERS

Student posters will be judged in two categories: Undergraduate and Graduate. Winners in each category will be awarded a student travel grant for a future security conference and Runners Up will be awarded a tech prize.

### **At What Age Should a Child Start Learning About Cybersecurity?**

*Georgia Tyner, SUNY Empire State College*

A, B, Cybersecurity...How early can a child start learning about cybersecurity? From the first time a child uses a cellphone, tablet or computer, they should be protected from cyberthreats. If their device is protected, that child is encountering cybersecurity. What should they know, when should they know it, and can they learn about cybersecurity at an early age? What is the best way for them to learn? In this paper, I will research what age children begin to learn about cybersecurity. I will research what type of cybersecurity education currently exists, online, in-person, through books, e-books, comic books or games, for children in pre-K to high school. I will look at the types of cybersecurity education and the success rate of the path of a cybersecurity career, if it has been around long enough to claim influence. There are many reasons we would want our children to know about cybersecurity. It could be a fruitful career, and the knowledge can protect them from predators, malware and malicious ads, to name a few. If parents don't understand cybersecurity basics, how can they teach their children? What help is out there? In this research, I will use systematic literature review as a research method as well as review existing programs and their effectiveness.

### **Exploring Side Channel Data for Detecting Malicious Software**

*Rebecca Clark and J Todd McDonald, University of South Alabama; Lee Hively, Oak Ridge Nat'l Lab (Retired)*

Rootkits are pernicious types of malware with administrative-level privileges that obtain access or control of a computer system. They often hide themselves effectively against detection mechanisms because they have the ability to alter system data and essentially lie to an end user. Side channel data such as CPU power and temperature, however, are outside the scope of a rootkit to alter. In this research, we use CPU power analyzed by a nonlinear phase space algorithm to detect rootkit execution. We collect CPU power measurements with a Data Acquisition System (DAQ) while test computers are in various states of activity (normal, stressed and manually controlled) and in either infected or uninfected states. We also compare results of our novel nonlinear phase space approach to common machine learning algorithms used in similar research. We train our algorithm using various phase space graph features that identify optimal threshold levels for graph dissimilarity and the optimal successive occurrences above threshold that produce the best detection accuracy. Our initial results demonstrate that certain rootkits can be detected through our phase space algorithm using low-frequency power signatures.

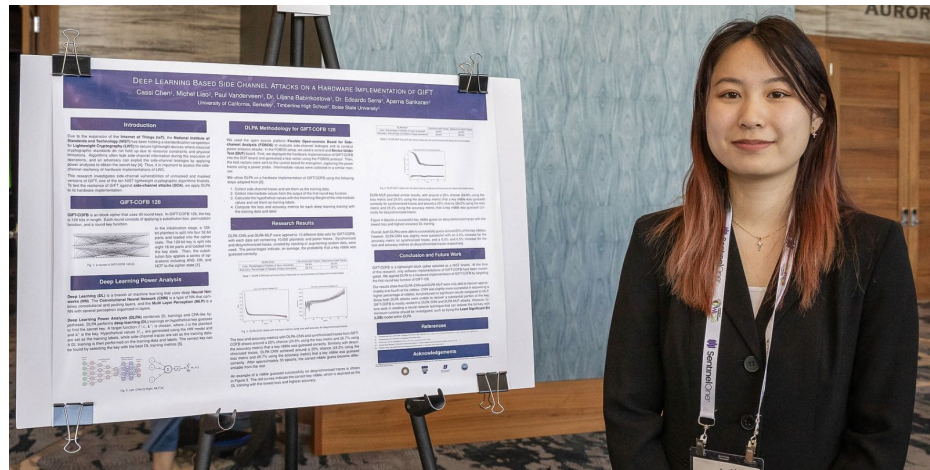
# Student Poster Competition

**Accepted poster presenters must become a student member if they are not already a student member.**

- Highlight major points of your research/work
  - Why is your work important?
  - What is your work about?
  - What approach do you use?
  - What is the outcome?
- Two categories
  - Undergraduate and Graduate
- Inclusions
  - The first listed student of accepted posters will receive an automatic scholarship.
  - Additional students listed on a poster must apply for a scholarship to attend and there is no automatic scholarship.
  - Submissions must be presented in person and the first listed presenter must be the lead presenter.



# Past Poster Presenters



## Gadgets of Gadgets in Industrial Control Systems: Return Oriented Programming Attacks on PLCs

Adeen Ayub<sup>1</sup>, Nauman Zubair<sup>2</sup>, Wooyeon Jo<sup>1</sup>, Hyunguk Yoo<sup>2</sup>, and Irfan Ahmed<sup>1</sup>

<sup>1</sup>Virginia Commonwealth University <sup>2</sup>The University of New Orleans

**VCU** College of Engineering **THE UNIVERSITY OF NEW ORLEANS**

### Motivation

- Programmable Logic Controllers (PLC) directly monitor and control physical processes such as nuclear plant, water treatment, and power grid via a control logic program
- Existing control logic injection attacks have some downsides
  - Can be detected by an IDS since they involve sending substantial malicious code to a PLC over the network
  - A strict firewall can prevent reading/writing to the control logic area of a PLC
- Return Oriented Programming (ROP) reuses existing instructions ending with a 'return' (called gadgets) in a target system, limiting or eliminating the need to transfer machine instructions over the network
- First attempt to fill the gap and explore challenges for a successful ROP attack on real-world PLCs and disrupt the underlying physical process

### Challenges

- Determining the location of the control logic program
- Deciding which gadgets are useful
- Overwriting the stack without buffer overflow vulnerability
- Executing an ROP gadget chain while ensuring normal PLC operations
- Maintaining a continuous attack cycle through ROP gadgets
- Persistent control of a compromised PLC

### Exploitable Features and Proposed Techniques

**Exploitable features**

- Predictable control logic location
- Using the mapping between CPU registers and I/O ports for searching gadgets
- Download and upload capability via ICS protocols
- No stack protection

**Proposed Techniques**

- Finding useful gadgets (FUG)
- Stack Modification Code (SMC) injection
- Stack Modification
- Persistent ROP Attack

### ROP 1

Add gadgets to existing control logic to make it malicious

Two variants

- Using one gadget (that modifies the register associated with the output port)
  - Limited to only a few output ports
  - Tested on an elevator model
- Using a gadget chain that gives an attacker more flexibility in manipulating the output ports
  - Tested on a conveyor belt model

**Performance evaluation on elevator model**

Scan time (us)	Program size (bytes)	Number of gadgets	Size of program (bytes)
120 - 122	600	1	3
121 - 122	670	1	3

**Performance evaluation on conveyor belt model**

Scan time (us)	Program size (bytes)	Number of gadgets	Size of program (bytes)
120 - 122	36	4	13
126 - 127	40	4	13

### ROP 2

- Construct a control logic from scratch using gadgets in a PLC's memory
- The kind of control logic that can be constructed is limited because of the limitation of the type of gadgets in the memory
- Tested on a compact traffic light model
- Toggle switch turns on blue lights

**Performance evaluation**

Number of gadgets - 2  
Gadget size - 3 bytes

### Conclusion

- Presented control logic attacks on PLCs using ROP
- Since ROP uses gadgets in memory to perform a malicious action, there is little to no need of transferring malicious control logic program to a PLC
- Unlike ROP in IT, we achieve a continuous (control logic) scan cycle through ROP gadgets
- Used M221 PLC as a case study
- Results show that an IDS for PLCs does not detect SMC

# Selection Process

- Submission scored by at least two reviewers.
- Authors can submit multiple proposals in different categories and tracks.
- Submissions will be peer reviewed with speaker name, email and affiliation blinded.
- Reviewers selected from WiCyS members who volunteered.
- Reviewers submit reviews using our CFP system.
- Sub-committee on each of the categories meets to discuss submissions with co-lead and select recommendations for program committee leadership.
- Program committee leadership meets to discuss all recommendations and finalize selections.
- Authors are notified and asked to register.

# Rubric

## **Fulfills general guidelines**

- **Content**
  - Is compelling/timely
  - Is technically sound
  - Is relevant to the tracks
- **Title**
  - Provides good indication of content of session
- **Description**
  - Is well articulated and written
  - Provides good view of session content, activities and outcomes



**Submission Deadline:**

**November 4, 2024**

(Student posters are open until  
January 6, 2025)

Both close at 5:00 CT of date noted  
above.

<https://www.globauxsourceevents.com/WICYS2024/CallForProposals>