CyberCorps Scholarship for Service: Developing The Next-generation Cyber Workforce

Assefaw Gebremedhin
Washington State University

What is CyberCorps: Scholarship for Service (SFS)?

Created in 2000 under the Federal Cyber Service Training and Education Initiative

Today, the SFS program is managed by the National science Foundation (NSF) in collaboration with the Office of Personnel Management (OPM) and the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA)

Relevant Acts:

Cybersecurity Enhancement Act of 2014

National Defense Authorization Acts for 2018 and 2021

CHIPS and Science Act of 2022

What is CyberCorps: Scholarship for Service (SFS)?

The SFS program educates high-caliber scholarship recipients from institutions with strong existing academic program in cybersecurity

SFS scholars receive full scholarship support for up to three years

Upon completing their education, recipients are obliged to work for a Federal, State, Local, Tribal, or Territorial Government agency for a period equivalent to the length of the scholarship

OPM administers the program by providing placement assistance, coordinating recipient compliance, and tracking recipients through all phases of the program

Goals of the SFS Program

Enhance the security of critical information infrastructure

Increase national capacity of educating IT specialists in cybersecurity disciplines

Produce new entrants into the Government cybersecurity workforce

Increase national R&D capabilities in cybersecurity

Strengthen partnerships between institutions of higher learning and relevant employment sectors

Benefits

- Up to three years of scholarship support for undergraduate and graduate education including the following:
  - Tuition paid by the program
  - Stipend of $27,000 per year for undergraduate students
  - Stipend of $37,000 per year for graduate students
  - Professional allowance of up to $6,000 per year for travel to annual SFS Job Fair and other travel, certifications, etc
- Access to SFS-specific virtual and in-person job fairs in Washington DC

Commitment

- **Before graduating**
  - Maintain full-time enrollment
  - Maintain good academic standing
  - Respond to requests for information from the SFS Program Office
    - E.g., surveys, questions regarding program participation
  - Complete at least one internship opportunity within government
  - Participate in experiential learning opportunities offered by the WSU SFS program
  - Begin searching for employment to meet the post-graduation service requirement

Commitment

- **After graduating:**
  - Work full-time in qualifying position at an approved agency for a period commensurate with the length of the scholarship
  - Provide documentation to the SFS Program Office and WSU verifying employment annually
  - Ensure contact information is up to date in your SFS profile
  - Complete periodic surveys as requested by the SFS Program Office
  - Respond to all requests from SFS Program Office and WSU for information concerning the SFS program and your status

Examples of Qualifying Agencies

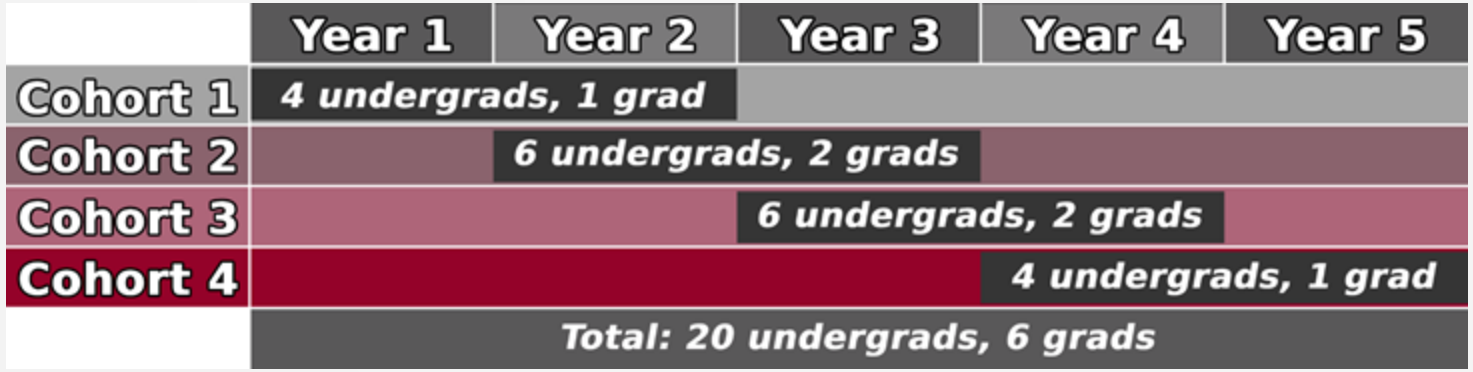
Federal Executive Agency
Congress, including any agency, entity, office, or commission established in the legislative branch
An interstate agency
State, local, or Tribal government
State, local, or Tribal government-affiliated non-profit that is critical infrastructure as defined in section 1016(e) of the USA Patriot Act

Eligibility Requirement

- Must be a citizen or lawful permanent resident of the United States
- In addition, a student must be one of the following:
  - A full-time student within two years of completing their bachelor's or three years completing their master's degree in a coherent, formal program focused on cybersecurity
  - A research-based doctoral student
- Prospective students will also need to meet any other university-specific eligibility requirements **and** meet the criteria for Federal employment, including the ability to obtain a security clearance, if required

WSU SFS Program

- Aims to recruit and train **20 undergraduate and 6 graduate students** over the course of five-years
- Provide excellent academic experience to SFS scholars through *integrated research*, *career mentoring*, *experiential learning*, and *internship* opportunities
- First cohort will begin in **Fall 2025**
- **To apply visit:** https://cyser.wsu.edu/sfs

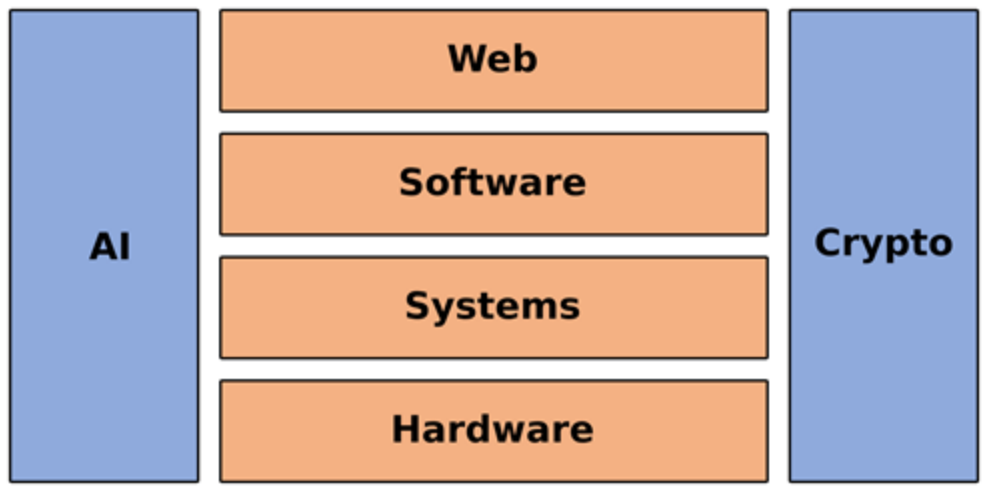


Eligibility Requirements for WSU SFS Program

- Must be a citizen or lawful permanent resident of the United States
- Must be a full-time student at WSU with an overall GPA of 3.0 or above and accepted into one of the following undergraduate or graduate programs:
  - Undergraduate programs
    - BS in Cybersecurity
    - BS in Computer Science, Computer Engineering, or Software Engineering and pursuing the coursework requirements for the CySER CAE-CO Fundamentals certificate
  - Graduate programs
    - MS or PhD in Computer Science, Software Engineering, or Electrical Engineering with research focused on cybersecurity and a program of study that includes at least four 400 or 500-level cybersecurity courses
- Must commit to working for a Federal, State, Local, Tribal, or Territorial Government agency after graduation for as many years as you received scholarship through the SFS program

WSU SFS Program Research Areas and Team

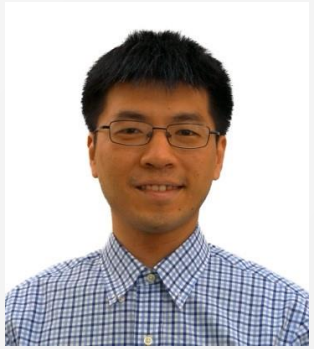
1. Artificial intelligence and Security
2. Cyber-physical Systems Security
3. Cryptography and Post-Quantum Security
4. Software Supply Chain Security
5. Hardware Security
6. Web Security



Assefaw Gebremedhin
(PI)

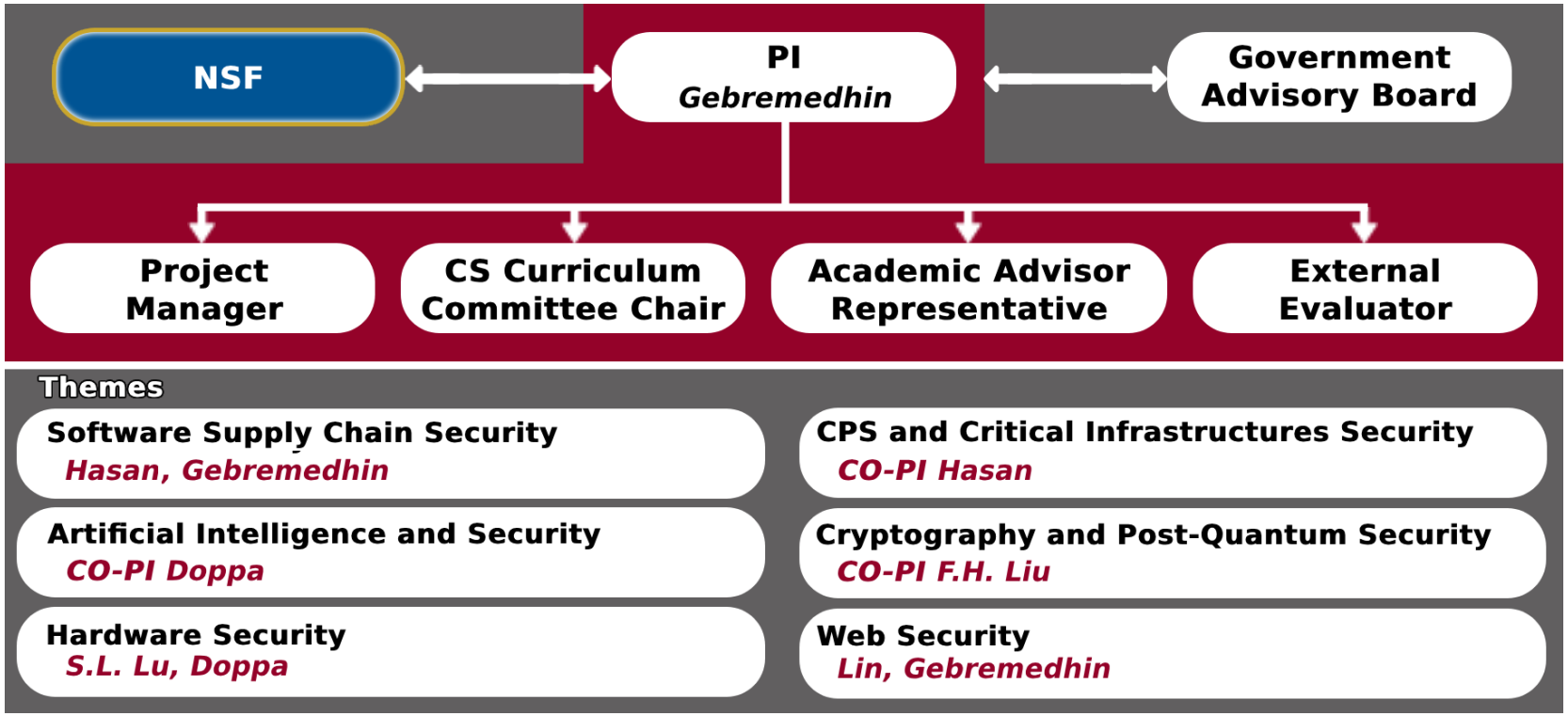
Jana Doppa
(Co-PI)

Monowar Hasan
(Co-PI)



Feng-Hao Liu
(Co-PI)

SFS Program: Project Management



WSU SFS Program: Project Evaluation

- External evaluation led by **Dr. Olusola Adesope** of the *Learning and Performance Research Center* (LPRC)
- The LPRC team will evaluate the effectiveness of the educational components derived from
  - Experiential learning opportunities
  - Cybersecurity seminar series
  - Internships and government engagement
  - Research and career mentoring
  - Professional development activities
- The LPRC team will also evaluate
  - Faculty development
  - Institutional partnerships
  - Broadening participation activities

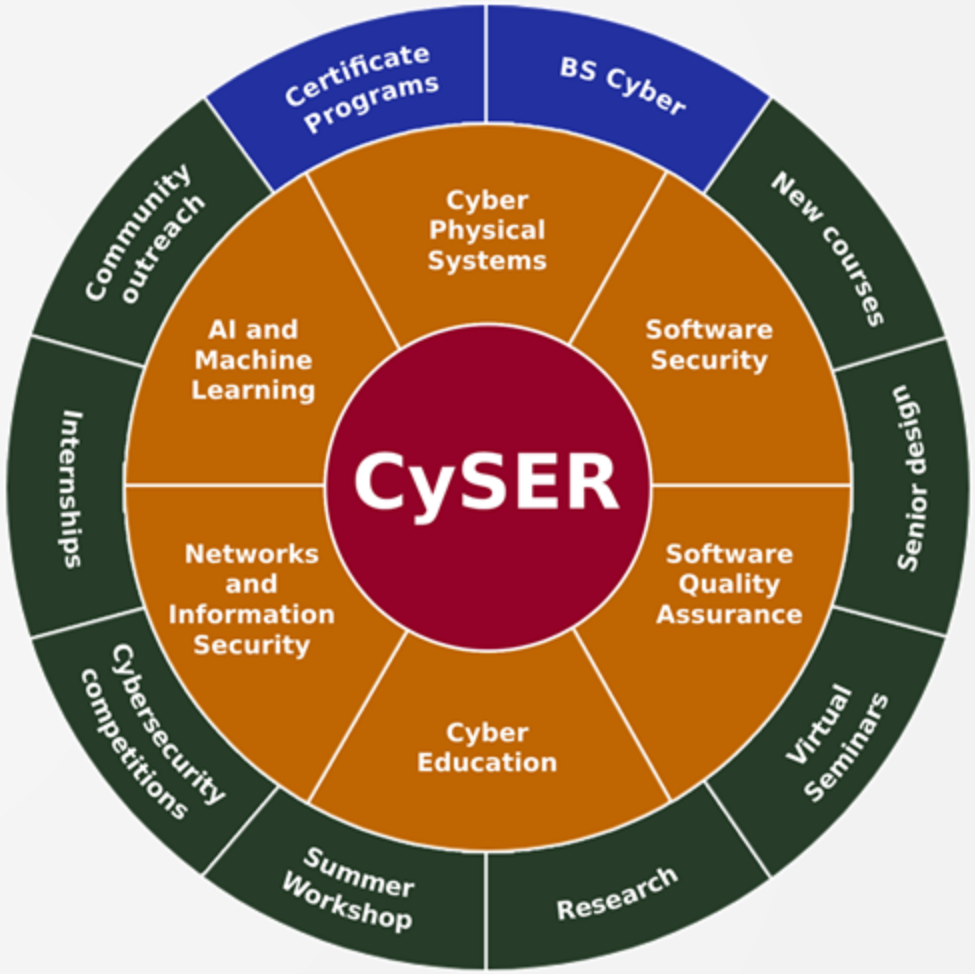
Foundations of our SFS Program

- **VICEROY Institute for Cybersecurity Education and Research (CySER)**
  - Established in June 2021, with support from DoD (OUSD R&E)
- **New BS in Cybersecurity degree program**
  - Launched in Fall 2023, with support from Washington state government
- **Existing broader institutional capacity and support**
  - Five thriving BS programs at EECS
    - Computer Sci., Software Eng., *Cybersecurity*, Computer Eng., Electrical Eng.,
    - ABET Accredited (CS, SE, CE, EE)
    - Cybersecurity in preparation for next ABET cycle
  - Strong and growing core cybersecurity faculty
  - Strong interdisciplinary research programs in several areas, including AI, data science, design automation, power engineering, security & privacy, and software engineering
  - Cybersecurity is a key priority area for the university

VICEROY CySER Institute

WSU

- Established in June 2021, in the first cycle of the VICEROY program
- VICEROY = Virtual Institutes for Cyber and Electromagnetic Spectrum Research and Employ
- Trains DoD-aligned civilian workforce and ROTC in cybersecurity
- Integrates cybersecurity research and education with professional skills in teamwork, communication, leadership, and lifelong learning
- A strong consortium in the Pacific Northwest for cybersecurity education and research
  - WSU (lead), Montana State University, Univ of Idaho, and Central Washington Univ



CySER Curriculum: Encapsulated via 3 Certificate Offerings at WSU

CySER CAE-CO Fundamentals

- Targeted for BS in Computer Science (or Software Eng.) students interested in specializing in cybersecurity
- Or students in the BS in Cybersecurity program
- Led by the School of EECS

CySER Basic

- Targeted for non-CS majors interested in cybersecurity
- Led by the Department of MISE in the College of Business

CySER CAE-CO Advanced

- Targeted for MS and PhD students (in CS, CE, EE, ME, ChE, MISE) whose research focuses on cybersecurity
- Mentor CySER undergraduate participants on research projects
- Led by the School of EECS

CySER CAE-CO Fundamentals Certificate

Required coursework

- CptS 327: Fundamentals of Cybersecurity and Cryptography
- CptS 427: Cybersecurity of Wireless and Distributed Systems
- CptS 428: Software Security and Software Reverse Eng.
- CptS 421 and 423 (Senior Design) with cybersecurity-related project
- **Four** electives from a pool of relevant CptS and EE courses

Internship
(VICEROY MAVEN or Industry)

Participation in mentored research

Summer workshop

Bi-weekly seminars

Foreign language recommended
(Examples: Russian, Chinese, Korean, Arabic, Persian)

New BS in Cybersecurity Program at WSU

- Independent degree program (major)
- Focuses on cyber operations
- Emphasizes hands-on coursework, experiential learning
- Credits Required: 120 (4-year)
  - 74 Comp Sci/Cyber, 16 Math/Stat, 30 General
- First two years like BS in Comp Sci; last two years heavy on cyber courses

Cybersecurity Courses in the New Degree

Required

- CptS 327: Fundamentals of Cybersecurity and Cryptography
- CptS 427: Cybersecurity of Wireless and Distributed Systems
- CptS 428: Software Security and Software Reverse Engineering
- CptS 455: Introduction to Computer Networks and Security
- CptS 439: Cybersecurity of Critical Infrastructure Systems
- CptS 426: Hardware Security and Hardware Reverse Engineering
- CptS 432: Cybersecurity Capstone Project

Elective

- CptS 425: Cyber Forensics and Anti-Forensics
- CptS 424: Cyber Law, Ethics, Rights, and Policies
- CptS 429: Virtualization and Offensive Cyber Operations
- CptS 431: Security Analytics and DevSecOps

Courses and CAE-CO KUs

Cybersecurity course (each 3 credits)	**KUs covered**
CPTS 327: Fundamentals of Cyber Security and Cryptography	M7, M8, O4, O13
CPTS 427: Cyber Security of Wireless and Distributed Systems	M5, O2
CPTS 428/528: Software Security and Reverse Engineering	M2, M9, O8
CPTS 455: Introduction to Computer Networks and Security	M4, O11
CPTS 439: Cybersecurity of Critical Infrastructure Systems	O1, O14
CPTS 426: Hardware, Firmware Security and Reverse Engineering	M1, O1, O10, O17
CPTS 424: Cyber Law, Ethics, Rights, and Policies	M10
CPTS 425: Cyber Forensics and Anti-forensics	O11
CPTS 429: Virtualization and Offensive Cyber Operations	O3, O16
CPTS 431: Security Analytics and DevSecOps	O5, O8
CPTS 432: Cybersecurity Capstone Project	O9

Thanks!

Questions