Protecting the Public from Catastrophic Software Failure -- The Professional:

experience, education, examination

System & Software Integration Certification Committee

Cate Richards
Director, Federal Programs
CRichards@Sonatype.com

Dr. Ben Amaba, Professional Engineer, CPIM®, LEED®AP BD+C
Fellow, Industrial and Systems Engineering
BAmaba@Sonatype.com

Agenda

> **Who We Are**

> **What Are We Doing**

> **Why Are We Doing It**
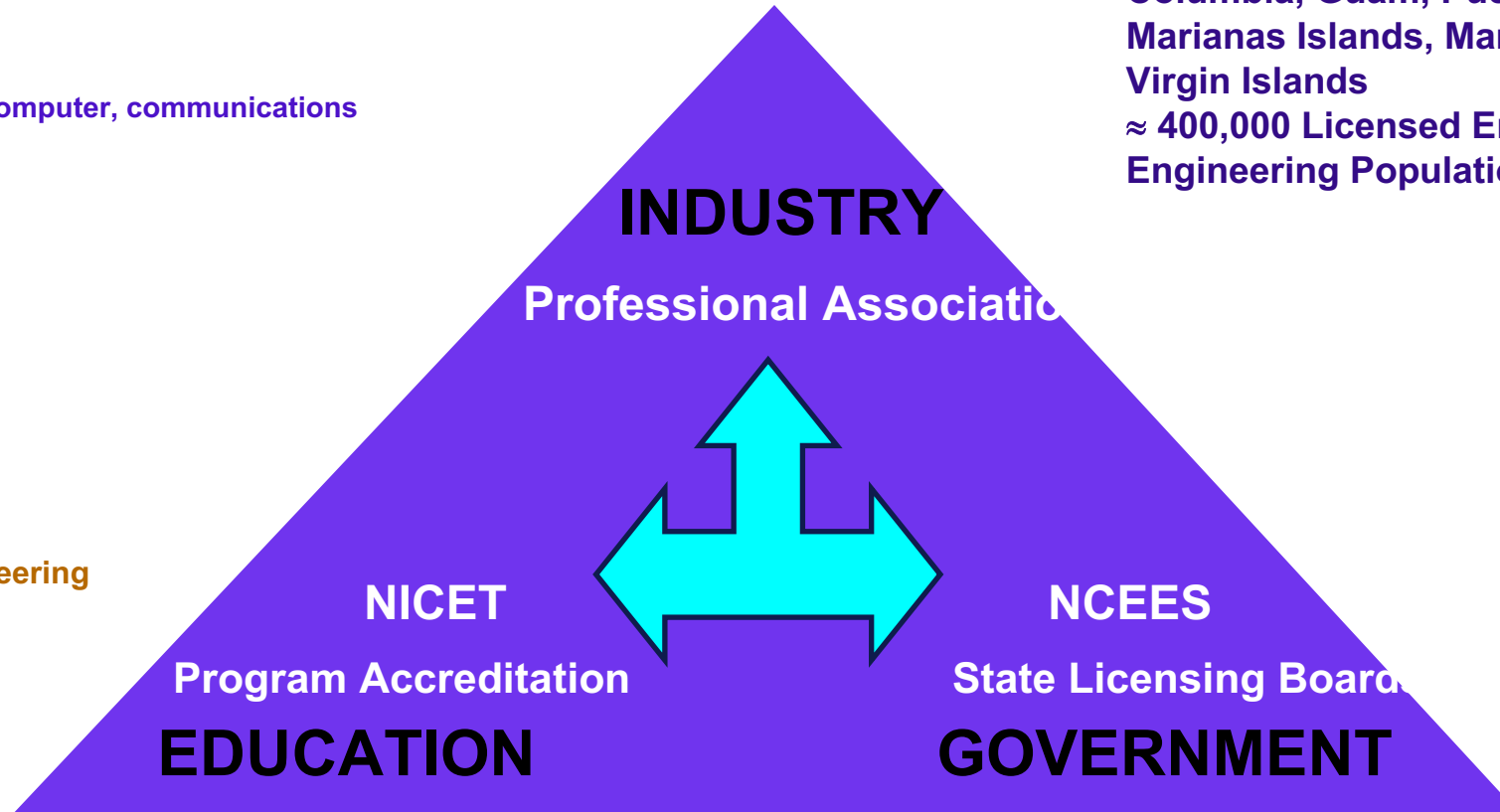
> **Where Are We Now**

> **Where Are We Headed**

Industry and Academia's Role in Licensing Engineers with the National Society of Professional Engineers (NSPE)

Licensed Professional Engineers are:

Agricultural
Chemical
Civil
Control systems
Electrical, electronic, computer, communications
Environmental
Fire protection
Industrial
Mechanical
Mining/mineral
Metallurgical
Manufacturing
Nuclear
Petroleum
Structural
NEW Software Engineering

All 50 states plus the District of Columbia, Guam, Puerto Rico, Northern Marianas Islands, Marshall Islands and Virgin Islands
≈ 400,000 Licensed Engineers   (U.S. Engineering Population ≈ 2,000,000)

INDUSTRY
Professional Association

NICET
Program Accreditation
EDUCATION

NCEES
State Licensing Board
GOVERNMENT

NSPE Software Professional Certification Task Force is our opportunity

NICET - National Institute for Certification in Engineering Technologies
ABET - Accreditation Board for Engineering and Technology
NCEES - National Council of Examiners for Engineering and Surveying

WHY WAS THE TASK FORCE FORMED?

- NSPE's Value Number 1 is "Protection of the public health, safety, and welfare above all other considerations."
  - Autonomous vehicle software failures in 2018 and 2019 – deaths and damage.
  - Boeing 737 Max software failures in Indonesia and Ethiopia in 2018 and 2019 – 346 deaths and $100 billion damages.
  - Washington State Amtrak failure – December 18, 2017
- There is substantial risk to the public health, safety, and welfare caused by using software and software-based devices designed or developed by others without a similar commitment.
  - Widespread use of Open-Source Code to speed development
  - Thousands of attacks and breaches on private and government infrastructure daily – deaths, ransom, and trillions of dollars in financial impacts annually.
  - 96 percent of this vulnerability and risk is avoidable.

BACKGROUND

- Software Engineering Licensure Consortium (2006-2013)

- P&P Exam Development (2011-2013)

- P&P Exam Discontinued by NCEES (2018)

- SPCTF Formed by President Martini (2020)

- Outreach to Intel, IISE, IBM, SAE, Insurers, NIST, NFPA, ASEE, ASME, Lockheed Martin, Railroad Associations, SAME, Federal Government (2020-2023)

- Executive Order 14028 (May 21, 2021)

- Shift in the reception to our message and proposed SSI Certification

- Mandates passing to Critical Infrastructure companies need to be addressed through education and certification
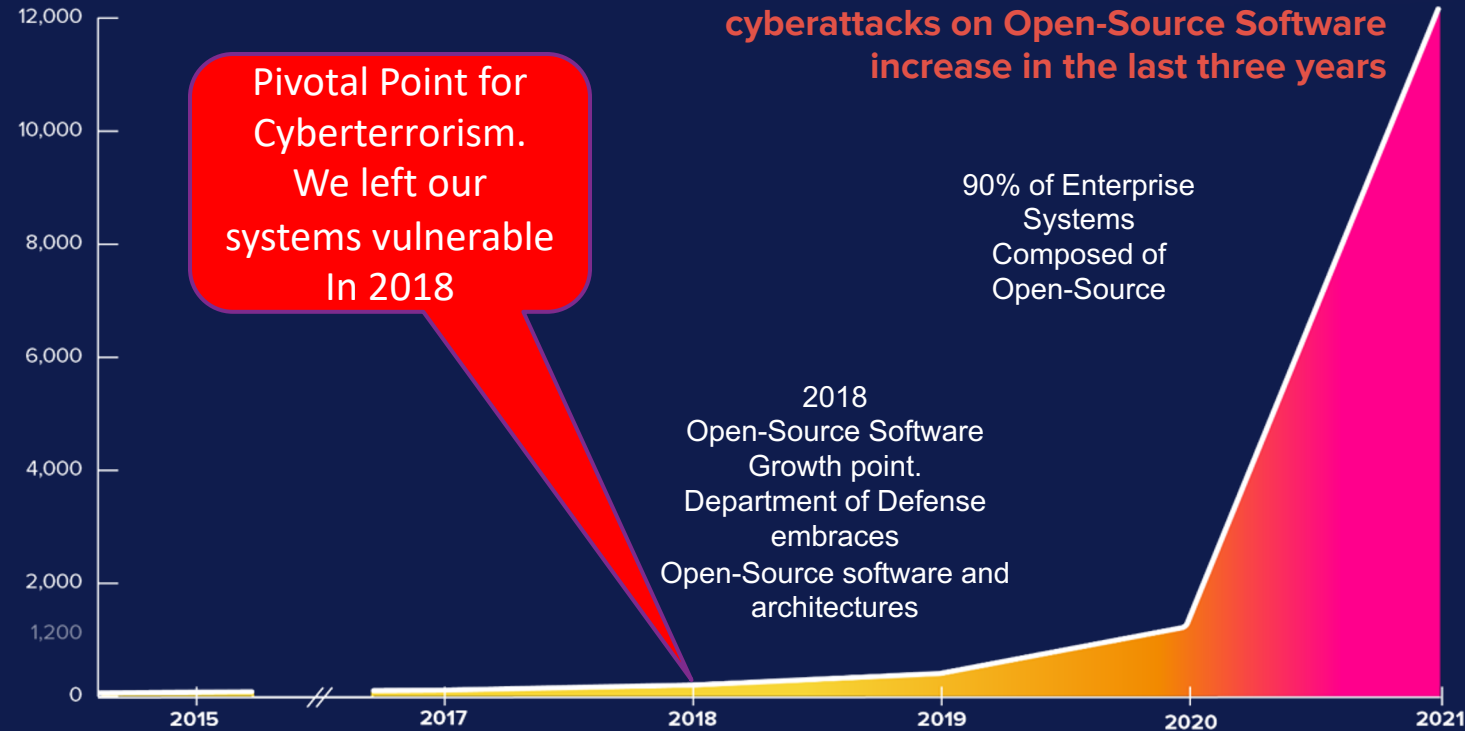
Why Software Supply Chain as the First Certification?
Open-Source Software Supply Chain Attacks | *2015 – 2023*

742%
year over year
cyberattacks on Open-Source Software
increase in the last three years

Pivotal Point for Cyberterrorism. We left our systems vulnerable In 2018

90% of Enterprise Systems Composed of Open-Source

2018
Open-Source Software Growth point.
Department of Defense embraces Open-Source software and architectures

12,000

10,000

8,000

6,000

4,000

2,000

1,200

0

2015   2017   2018   2019   2020   2021

Late 1990s
IEEE, ACM,
Canada states
Software
Engineering,
Branch of
Engineering

2006
NSPE, IEEE,
TBPE, NCEES
Launched
Software
Licensing

2013 - 2018
Software PE
License
Protect the
Public

2018
Software PE
Sunset by NCEES

sonatype
https://www.sonatype.com/ssc

WHAT ISSUES WILL THE PROPOSED SSI CREDENTIAL ADDRESS?

- Address concerns addressed by E.O. 14028.
- Common development processes throughout the supply chain.
- Standard credential review.
- Common reliability and interoperability testing.
- Fewer failures of infrastructure attributed to software failures.
- Improved coordination between the software developers and the engineering team.
- Reduced risk and vulnerability to cyber-attacks
- Baseline certification common to all industry sectors – First Certification
- Industry-specific certification applicable to specific industry (e.g., Automotive, Aerospace, Energy, Electronics, Petrochemical, Pharmaceutical, and Railroads) - Second Certification
- Establish a commonly accepted standard of care.

NATIONAL CYBERSECURITY STRATEGY: SOFTWARE LIABILITY CHANGES

"We must begin to shift liability onto those entities that fail to take reasonable precautions to secure their software while recognizing that even the most advanced software security programs cannot prevent all vulnerabilities. Companies that make software must have the freedom to innovate, but they must also be held liable when they fail to live up to the duty of care they owe consumers, businesses, or critical infrastructure providers. Responsibility must be placed on the stakeholders most capable of taking action to prevent bad outcomes, not on the end-users that often bear the consequences of insecure software nor on the open-source developer of a component that is integrated into a commercial product."

EVERYBODY PANIC!

HOW DOES CERTIFYING SOFTWARE AND SOFTWARE PROFESSIONALS HELP?

- Raising the level of professionalism

- Creating a system of accountability

- Creating trust and confidence in the public

- Lowering insurance

- Addressing public concerns

- But …. We need to start with certification

WHO: ...the connections to safer software supply chains through collaboration
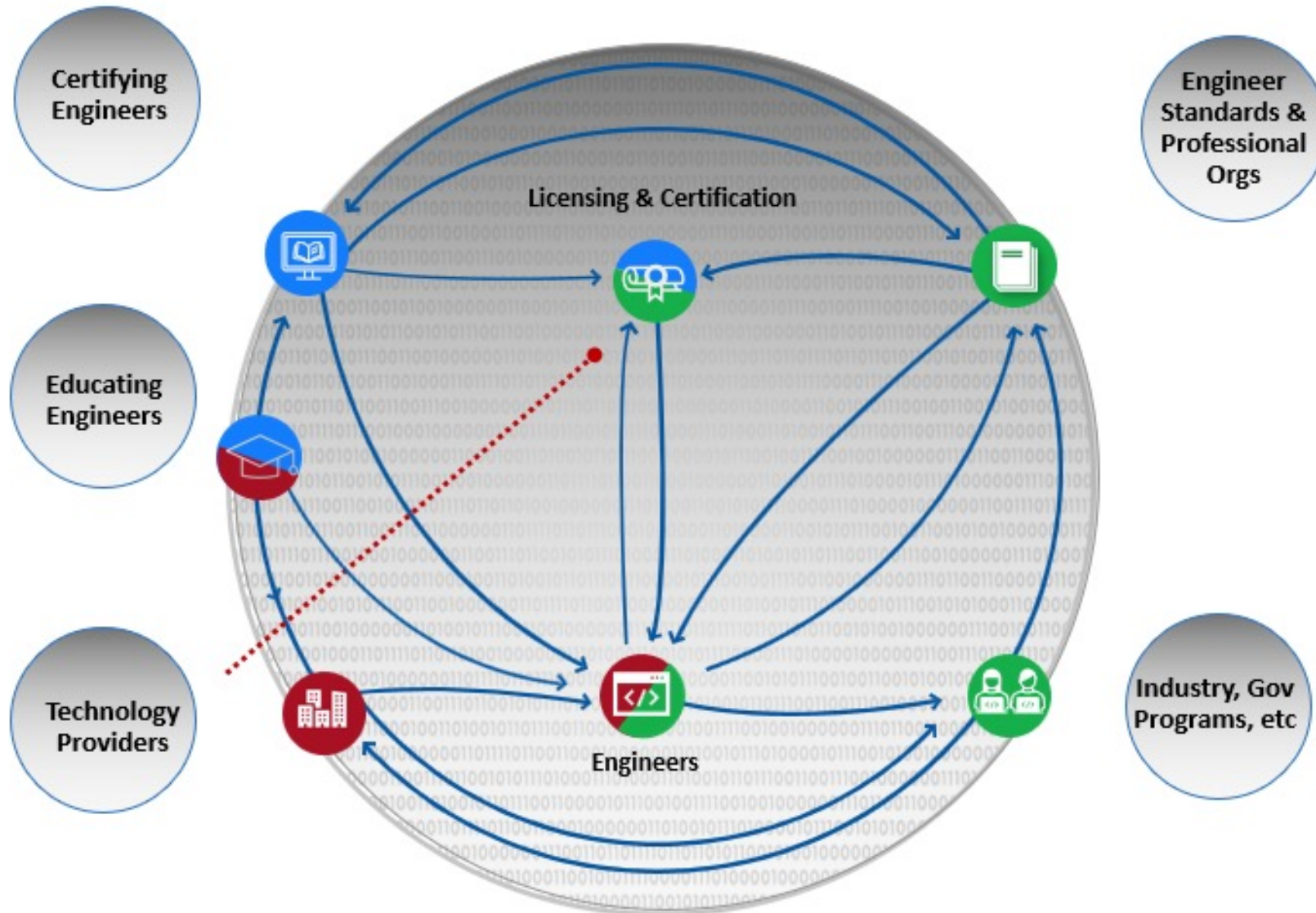
ACADEMIA PARTNERS TO LAUNCH TRAINING
UCF AS THE FOUNDING UNIVERSITY

- Class Launch - Q4 2023
- In Final Peer Review by Industry, Academia, Government Committee Members
- Modularized to accommodate Practioners and Executive Briefing Needs in Industry
- Prerequisite to the first NICET certification
- Launched in Continuous Education
- Several ABET and Universities to partner
- Several State Regulation Bodies (ex Florida, Texas, New York)
- PDHs and CEUs

Table of Contents

Overview
Lesson 1: Defining Software Supply Chain Management
    Overview
    Objectives
    Available Resources
Lesson 2: A Growing Need for Management & Responsibility
    Overview
    Objectives
    Available Resources
Lesson 3: The Evolution of Software Supply Chain Attacks
    Overview
    Objectives
    Available Resources
Lesson 4: Best Practices for Software Supply Chain Management & Responsibility
    Overview
    Objectives
    Available Resources
Lab: Using a Next-Gen Platform to Secure Your Software Supply Chain
    Overview
    Prerequisites
    Objectives
    Process
    Available Resources
Knowledge Check

SSI GOES LIVE!

Contact Us

🌐 Website: https://www.nicet.org/ssi

✉️ Phone: (888) 476-4238

📞 Email: ssi@nicet.org

Technician Certification Programs

Civil Engineering Technology
- Construction Materials Testing (add-on Performance Examinations now available)
  - Asphalt / Concrete / Soils
- Transportation Construction Inspection
  - Highway Construction Inspection

Electrical and Mechanical Systems Engineering Technology
- Building Systems
  - In-Building Public Safety Communications
- Electrical Power
  - Electrical Power Testing
- Fire Protection
  - Fire Alarm Systems
  - Inspection and Testing of Fire Alarm Systems
  - Inspection and Testing of Water-Based Systems
  - Special Hazards Systems
  - Water-Based Systems Layout
- Security Systems
  - Video Security Systems Designer / Video Security Systems Technician

Systems Software Integrator (SSI) Certification
- Coming Soon! Learn more.

Next Steps

Check Out SSI

Check out the NICET SSI Site – Volunteer for the Committee

Provide Input

Reach out to Ben Amaba or Cate Richards with ideas/feedback

Connect on Linked In

Connect with Ben & Cate to receive notice of updates as the Committee progresses with implementation

Learn More

Links

1. NICET: https://www.nicet.org/certification-programs/systems-software-integrator-ssi-certification/

2. UCF: https://cdl.ucf.edu/support/student/

3. NSPE: https://pdh.nspe.org/products/professional-engineering-ethics-risk-and-liability-with-technology

4. Sonatype: https://www.sonatype.com/state-of-the-software-supply-chain/introduction

Connect

1. Cate Richards: https://www.linkedin.com/in/caterichards/

2. Ben Amaba: https://www.linkedin.com/in/benamaba/

Q&A

Any Questions?

sonatype