



Introduction to Carnegie Mellon University Software Engineering Institute (CMU SEI)

Anita Carleton, Director, Software Solutions Division

MIT Lincoln Laboratory Meeting

October 20, 2022

Copyright 2022 Carnegie Mellon University.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

DM22-0959

CMU SEI is a DoD R&D Federally Funded Research and Development Center



Established in 1984 at Carnegie Mellon University (CMU)

Charged to improve the state of the practice of software engineering and cybersecurity

Added AI Engineering in 2018

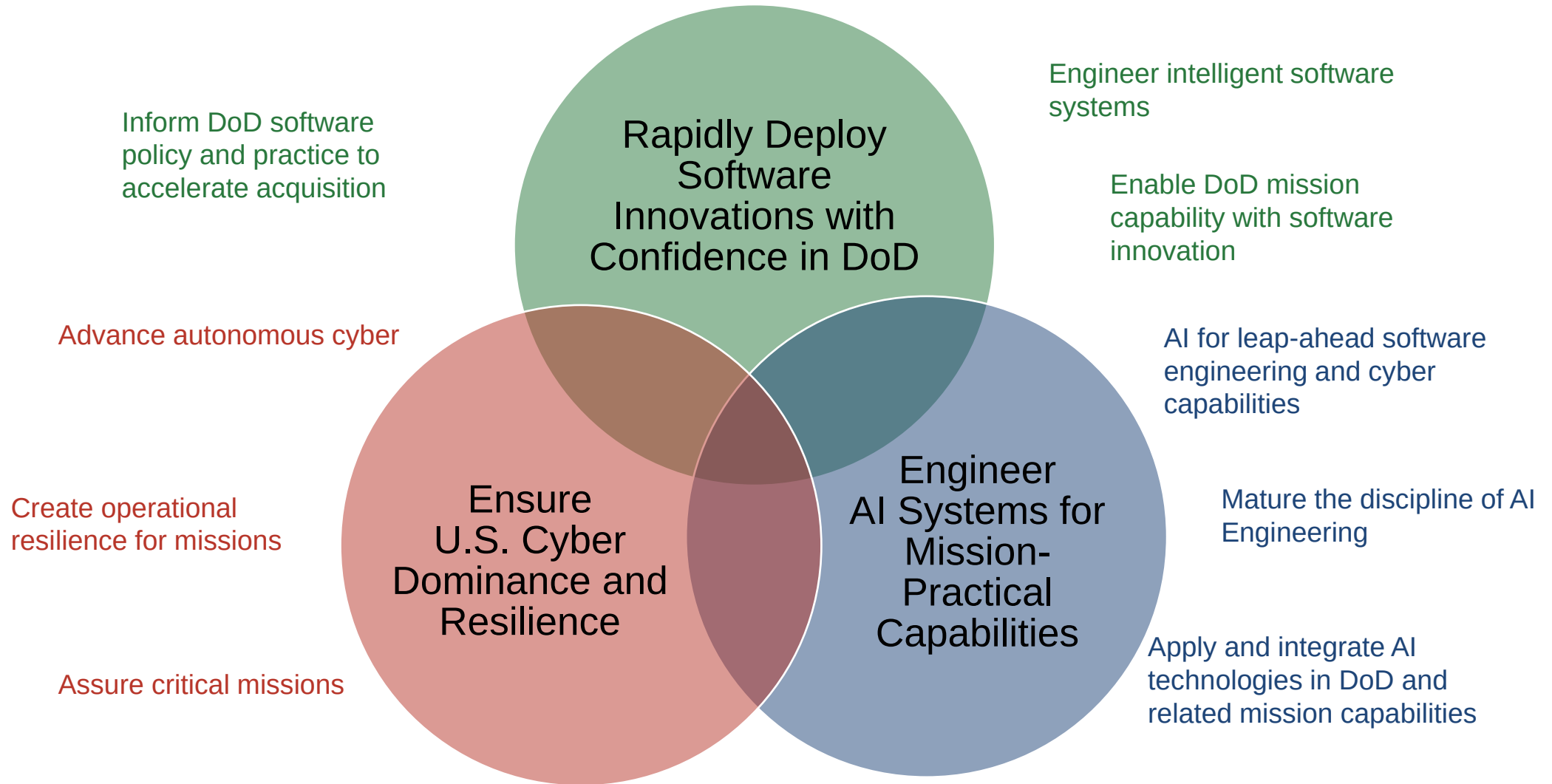
Collaborates with CMU and broadly in academia, government, and industry

Capable of conducting both fundamental research and classified work

~610 staff members

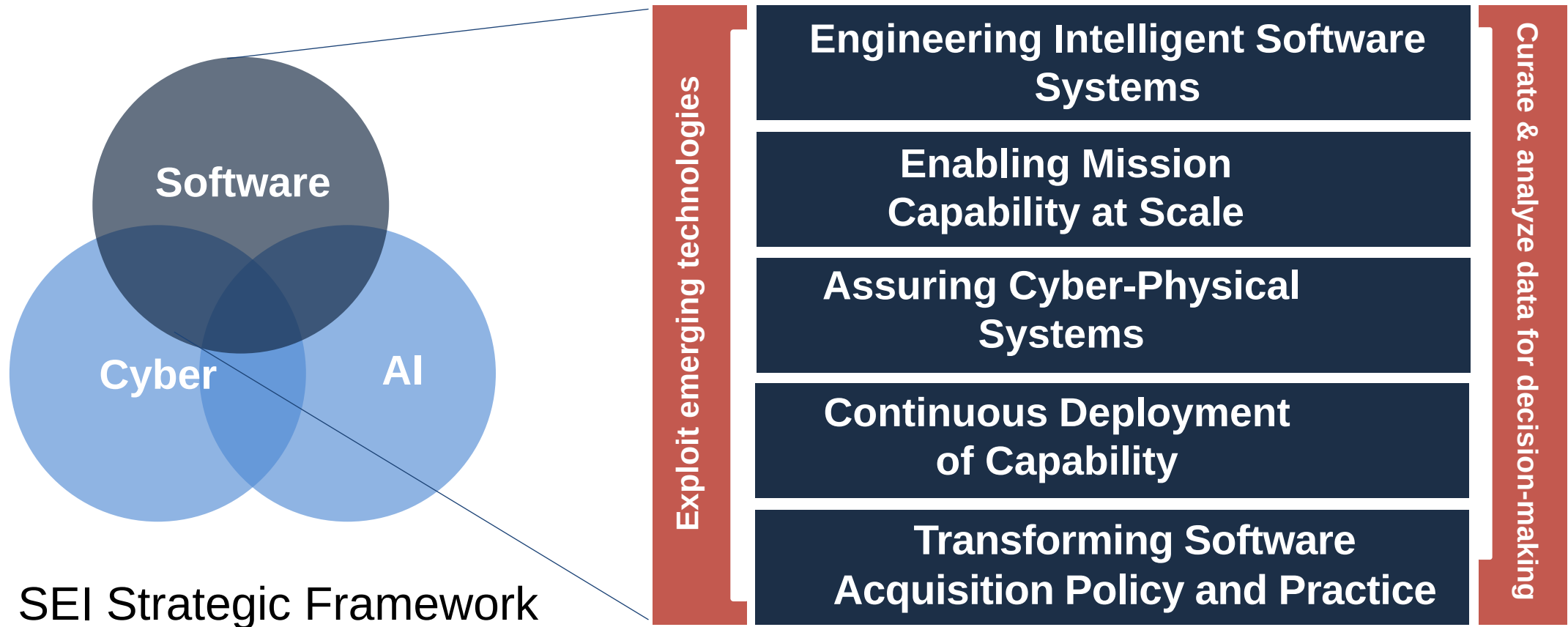
FY20 total funding ~\$140M Offices in Pittsburgh and DC, with locations near customer facilities in MA, TX, and CA

Our technical work portfolio connects software, cyber, and AI strategies for greater impact



Software Engineering Strategy:

Rapidly Deploying Software Innovations with Confidence in DoD



SSD Leadership Team



Harold Ennulat
Associate Director of
Client Integration and
Program Development



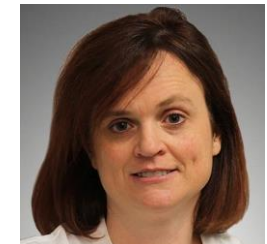
John Robert
Deputy Director



Anita Carleton
Director



Mark Klein
Principal Technical
Advisor



Erin Harper
Strategic
Communications
Manager

Technical Directors



Dionisio de Niz
Assuring Cyber-
Physical Systems



Ipek Ozkaya
Engineering Intelligent
Software Systems



Daniel Plakosh
Enabling Mission
Capability at Scale



Eileen Wrubel
Transforming Software
Acquisition Policy &
Practice



Hasan Yasar
Continuous Deployment
of Capability

SSD Technical Directorates and Initiatives

Technical Directorate/ Director	Initiative Name and Lead	Initiative Description
Engineering Intelligent Software Systems Ipek Ozkaya	Architecture Design, Analysis, & Automation	Applying AI to automate architecture design and analysis activities; applying and accelerating adoption of architecture practices
	Tactical and AI-enabled Systems	Developing software engineering principles and practices for tactical and AI-enabled systems; advanced prototyping of the application of principles and practices
Enabling Mission Capability at Scale Daniel Plakosh	Systems and Software Development & Analysis	Scaling software development and deployment through AI/ML and automation for large, complex, real-time mission systems
	Resilient Critical Software Systems	Leveraging threat information and real-time software techniques to drive resilient solutions for mission critical embedded systems
	Advanced Deterrents	Contribute to the development of America's new 21st century deterrent platforms and weapons which will serve as the backbone of our nation's national security
Assuring Cyber-Physical Systems Dionisio De Niz	Formal Verification of Cyber-Physical Systems	Rapid and scalable automatic verification of cyber-physical systems built from verified and unverified components, ensuring outputs with the right value, at the right time, and with the right physical reaction (e.g., stop a crash)
	Model-Based Software Engineering	Virtual integration to discover flaws before implementation
Transforming Software Acquisition Policy and Practice Eileen Wrubel	Software Acquisition Pathways	Assembling modern software acquisition/development approaches to inform policy and practice
	Software Engineering Measurement & Analysis	Data analytics to drive software acquisition policy and priorities
Continuous Deployment of Capability Hasan Yasar	Agile Transformation	Modernizing software development and acquisition with Agile methods
	DevSecOps Innovations	Engineering for automated secure deployment and operations pipeline

National Agenda for Software Engineering R & D Study Update



Study released November 2021

Available online at

<https://www.sei.cmu.edu/go/national-agenda>

Focus of National Agenda for Software Engineering

Software is vital to America's **global competitiveness**, **innovation**, and **national security**. The economy, the nation's infrastructure, education, and healthcare all depend on software.



Lead a community effort to:

1. **Identify future challenges** in engineering software-reliant systems.
2. Develop a **research roadmap** that will drive advances in **foundational software engineering principles** across system types such as intelligent, autonomous, safety-critical, and data intensive systems.
3. Raise the **visibility** of software to the point where it receives the sustained recognition commensurate with its importance to national security and competitiveness.
4. Enable strategic partnerships and collaborations to **drive innovation among industry, academia, and government**.

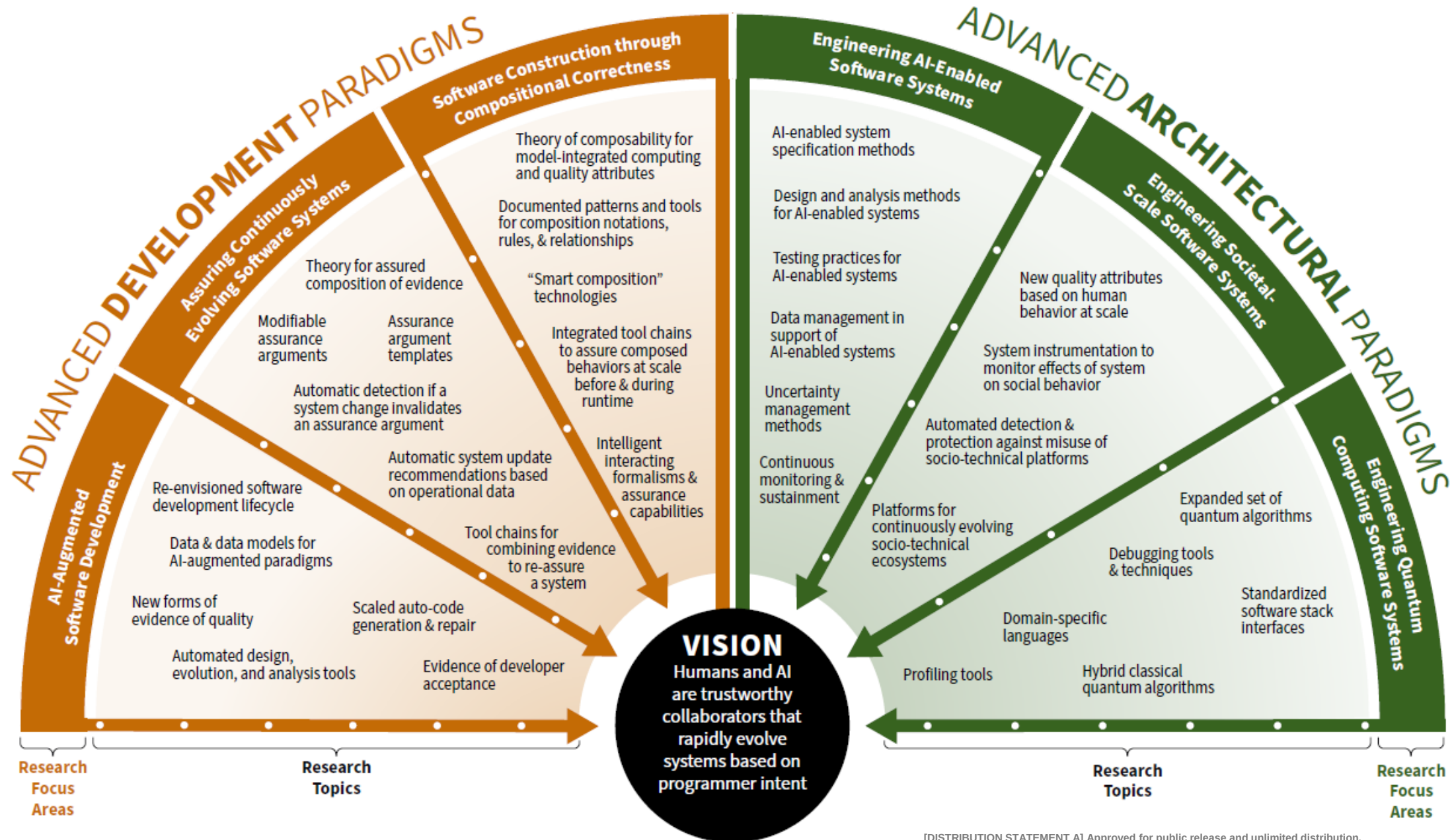
Foreword, National Agenda for Software Engineering

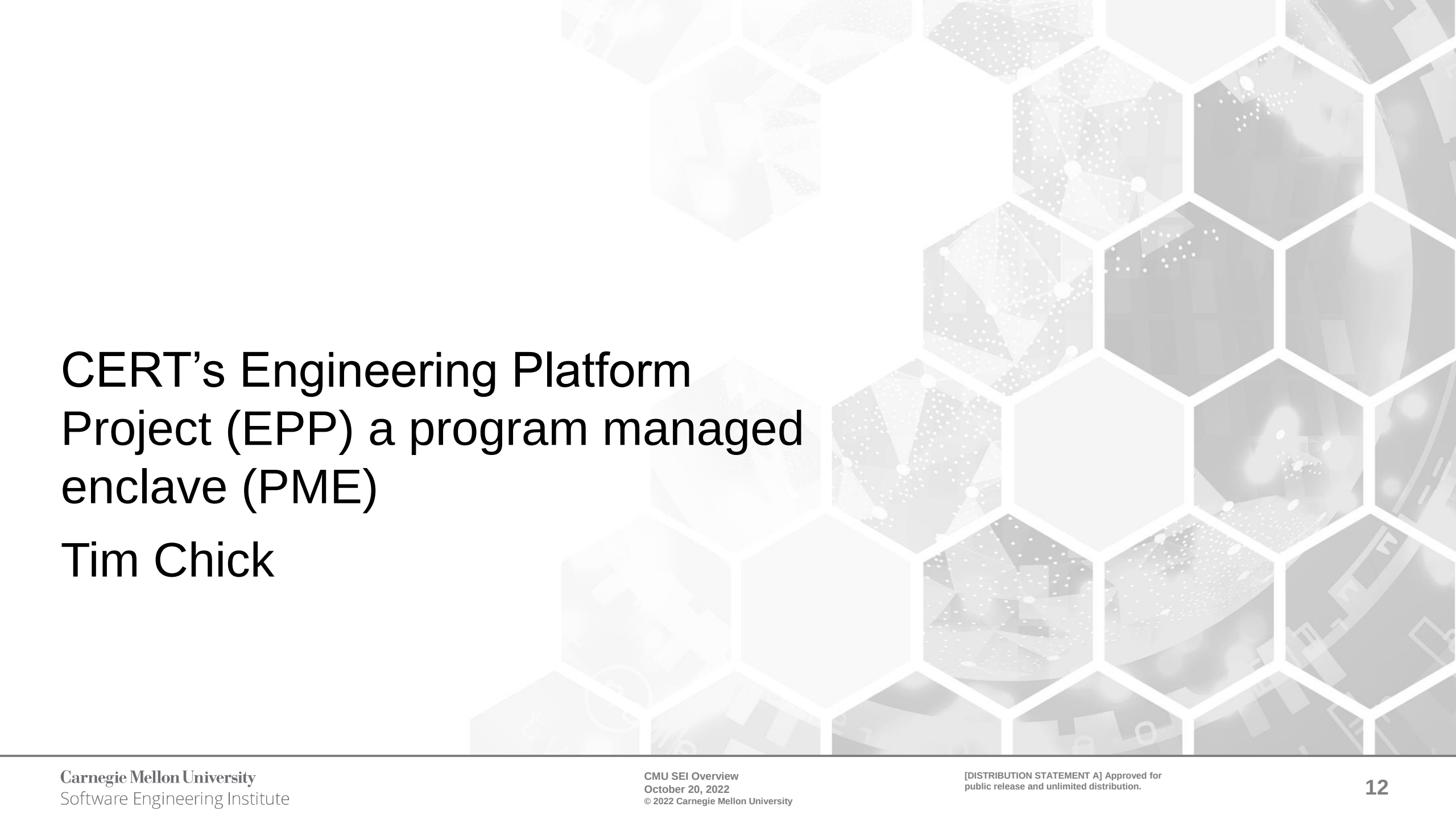
*"Software is an essential, if not the central, part of every Department of Defense (DoD) system. Our hardware has become increasingly programmable, and software has become ubiquitous. **Therefore, software engineering is a critical enabler for everything that we do in the DoD.** To remain competitive, our weapon systems acquisition must migrate away from the linear development and test cycle and evolve into a rapid continuous update and continuous assurance environment. **Consequently, this software engineering technology roadmap is a guide for our research and investment strategy that is vital for our national security.** As we develop new systems, we must go beyond model-based software engineering to enable us to rapidly develop systems while reducing re-assurance and sustainment costs. In the future, we will need rapid composition of new capabilities that can operate in a highly contested and denied environment. Integrating heterogeneous systems seamlessly and rapidly will enable us to stay ahead of threats. We will need to exploit the promise of artificial intelligence to increase capability not only in our fielded systems but also in our development systems. **This research roadmap should serve as the starting point for a sustained effort to improve software engineering.** The DoD will continue to look to the Carnegie Mellon University Software Engineering Institute as a leader in improving the state of the art and practice in software engineering."*

--The Honorable Heidi Shyu, Under Secretary of Defense
for Research and Engineering



Software Engineering Research Roadmap (10-15 Year Horizon)





CERT's Engineering Platform Project (EPP) a program managed enclave (PME)

Tim Chick

Engineering Platform Project (EPP) Mission

The mission of the EPP PME is to support engineering work and research at the SEI.

- The EPP is intended to be a forward-looking tool for teaching, training, experimentation, and research.
- The Systems Team works closely with developers, analysts, and researchers to provide specialized tooling as needed.
- The Systems Team leverages the expertise gained by the operation and use of the EPP to support efforts that fall outside the scope of the EPP.
- Systems Team personnel work closely with SEI IT personnel in order to deploy, configure, and operate applications which cannot feasibly be hosted in the EPP.

EPP Development Platform



- Tools for issue tracking, source code management, documentation, automated builds
- Highly configurable and customizable environment
- The EPP team will create custom projects and workflows and advise on DevSecOps CI/CD pipeline implementations

EPP Containerization



- Build, store, and access custom container images
- Run containerized applications on Docker-enabled virtual servers
- Create scalable, container based, cloud native applications in Kubernetes cluster
- Create and manage custom workloads
- Leverage GPU capabilities
- Containerization tools integrated with EPP software build tools

Researcher's Virtual Sandbox

- EPP provides virtual compute resources and data storage
- Custom virtual machines and/or virtual networks provided for:
 - Data analysis
 - LINE funded research
 - Software testing
 - PWP funded prototypes

Discussion

