National Initiative for Cybersecurity Advancement (NI4CA)

Overview

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Document Markings

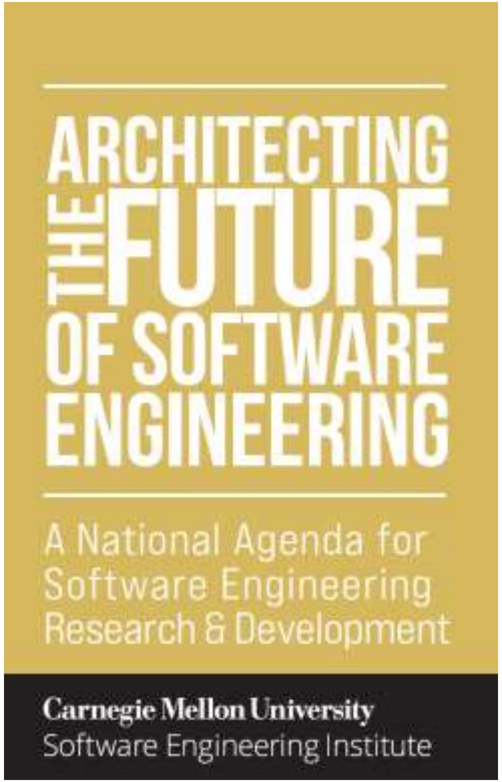
This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

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.

DM23-0045

Building on a Foundation of Transformative Research



ARCHITECTING THE FUTURE OF SOFTWARE ENGINEERING

A National Agenda for Software Engineering Research & Development

Carnegie Mellon University
Software Engineering Institute

Architecting the Future of Software Engineering: A National Agenda for Software Engineering Research & Development

This report is a multi-year research and development vision and roadmap for engineering next-generation, software-reliant systems.

- The report identified the most critical technologies and areas of research for enabling future software systems.
- The resulting technology roadmap is intended to guide the research efforts of the software engineering community toward future systems that are safe, predictable, and evolvable.

The National Initiative for Cybersecurity Advancement (2022-2023)

The National Initiative for Cybersecurity Advancement (NI4CA) is led by the CMU SEI.

Its goal is to define a multi-year research and development (R&D) vision and roadmap for securing next-generation, software-reliant systems in an effective, affordable, and timely way.

The recommendations it provides will:

- foster the development of technologies, methodologies, practices, and policies that advance cyber by design.
- enhance operational cyber resiliency.
- be applicable at scale across the cyber ecosystem.

The National Initiative for Cybersecurity Advancement (2022-2023)

We expect that the outcome of this initiative will:

- direct R&D to help realize new capabilities that improve and modernize current architectures and fielded systems and guide the development of future systems.
- inform the research community about the highest priority topics to refocus or influence its research and strategy.
- provide broad guidance for investment in cybersecurity engineering research by the Department of Defense (DoD) and across the U.S. government, as well as by critical infrastructure providers and academia.

How the NI4CA Fits with Other Initiatives

NI4CA is informed by activities such as:

- National Agenda for Resilient Digital Infrastructure (Aspen Cybersecurity Group, Dec 2020)
- Cyberspace Solarium Commission (Mar 2020)
- Federal Cybersecurity Research and Development Strategic Plan (National Science & Technology Council, Dec 2019)
- National Cyber Strategy of the United States (Sep 2018)
- Commission on Enhancing National Cybersecurity (Dec 2016)
- The Cybersecurity National Action Plan (Feb 2016)

NI4CA Proposed Framework: Outcome-Based Themes

Awareness

Improving aspects such as cyber hygiene, cyber education, workforce development, and awareness of both technological and human-centric risks

Usability

- Making technology more understandable and less complex for the average user

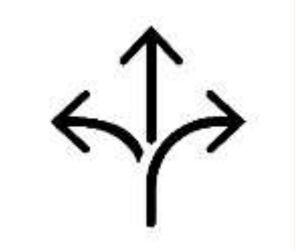
Capability

Focusing on how to engineer secure and trustworthy hardware and software systems

Visibility

Reducing barriers that hinder an organization's understanding of itself, its assets and their origins, and its adversaries and their capabilities

Flexibility



Exploring how to build resilient and adaptable systems – at scale - amidst emerging technologies and cybersecurity challenges

Identifying and Managing Risk