Carnegie Mellon University
Software Engineering Institute

Making Software a Strategic Advantage

OUR NATION'S MILITARY AND CIVILIAN GOVERNMENT ORGANIZATIONS increasingly rely on complex, software-based systems and networks. At the Carnegie Mellon University Software Engineering Institute (SEI), a federally funded research and development center, we objectively research complex software engineering, cybersecurity, and artificial intelligence (AI), mature solutions, and facilitate their transition into practice.

The SEI supports organizations that need

- **software to do more** with capability that gives the U.S. an edge over competitors or adversaries
- **software to be deployed rapidly** with timely response to warfighter needs
- **software cost to be affordable** with predictable cost, reduced where possible
- **software to be secure** and free from exploitable defects

Combining strengths in technology research, development, and application, we invent the possible and facilitate deployment of the practical by supporting both fundamental research and classified work to

- innovate the rapid, secure delivery of software capabilities
- drive cyber and software workforce readiness
- improve cyber operations to defend and secure systems and networks at the speed of relevance
- leverage AI and other emerging technologies to assure enduring advantage

Impactful Results: Faster, More Secure, Better Quality Software

- The SEI established the **first Artificial Intelligence Security Incident Response Team (AISIRT)**. This initiative builds on decades of SEI leadership in computer security, from establishing CERT/CC to identify, analyze, and report on vulnerabilities. CERT/CC provided the model for US-CERT. In 2023, CISA integrated US-CERT functions.
- The SEI contributed analysis of pilot results and decades of evidence-based software research for DoD's creation of **DoDI 5000.87: Software Acquisition Pathway (SWP)**. SWP **reduces bureaucracy** to deliver software capabilities to the warfighter faster. All SWP-adopting programs are delivering software within the one-year benchmark established by Congress.
- The SEI applied decades of expertise in cybersecurity and capability modeling to co-develop the Cybersecurity Maturity Model Certification (CMMC) to **assess the cybersecurity capabilities** of 220,000 DoD contractors.
- The Office of the Director of National Intelligence selected the SEI to **lead a national initiative in engineering AI for defense and national security.**
- Microsoft GitHub **adopted the SEI C and C++ Security Coding Standards** into its CodeQL service, which is used by tens of thousands of open-source projects.
- The Office of the Under Secretary of Defense for Research and Engineering and the SEI launched the **Center for Calibrated Trust Measurement and Evaluation (CaTE) to assure that AI systems for defense are safe, reliable, and trustworthy before being fielded.**
- A commercial aircraft industry consortium (Boeing, Airbus, and others) confirmed the ROI of 26 percent **cost avoidance** from using **SEI architectural modeling technology**.

More Impactful Results

- **A pioneer in technical debt research,** the SEI delivered the **first-ever independent review of technical debt** in DoD programs to Congress.
- With the Defense Innovation Unit, **the SEI co-authored *Responsible AI Guidelines in Practice*** as a framework for developing AI systems in a way that aligns with the DoD AI Ethical Principles
- Innovative SEI processes **shortened authority-to-operate approval** from months to a single day for the Joint Improvised-Threat.
- The SEI provided on-site independent verification and validation to help the Navy and industry team **quickly resolve software challenges** on a critical software subsystem.
- **SEI-developed technology cut system integration costs by 7x** in the Army's Joint Multi-Role Technology Demonstrator project through the use of its architecture-led incremental system assurance method.
- Using its **expertise and rapid response capability,** the **SEI provided feedback to the Long Range Stand Off (LRSO) Weapon** to ensure faster iterations of a highly complex software baseline.
- The SEI's **AI technological and domain expertise** supported aligning acquisition with mission goals for nearly $150 million in prototype to production funding.
- Army Cyber Protection Teams, Multi-Domain Task Forces, and NETCOM Regional Cyber Centers use the SEI's Fortress platform for **cyber training, exercises, and mission rehearsals.**
- The SEI **trained thousands of acquisition professionals** on modern software practices through curriculum it developed and **facilitated that curriculum's transition to the DAU DevSecOps Academy and Service-specific initiatives.**
- SEI cybersecurity expertise assisted the Department of State in implementing cyber capacity and capability building in 40 countries with the aim of **securing and protecting the integrity of cyber infrastructure.**
- Using its software, data, AI, and cybersecurity engineering expertise, the SEI enabled the NETCOM Data Science Directorate to create an **ML-enabled analytic framework** deployed to the recently launched NETCOM Edge platform that facilitates data-driven innovation.

Distinctively SEI

We are shaping the future of software for a better world through our work in AI engineering, software engineering, and cybersecurity research. The SEI

- is part of CMU, a world leading university in software engineering, cybersecurity, and AI
- offers in-depth technical knowledge of software development practices and processes and cyber protection that includes capabilities in modern techniques
- collaborates with industry to provide the DoD with an effective mechanism to discover and access technologies for possible DoD use
- applies advances in technology and new research outcomes to the most critical ongoing needs
- provides government organizations with insights to anticipate future needs before they become critical issues
- integrates research in AI, software, and cyber to provide solutions for DoD capabilities, acquisition, integration, and delivery of software

Trusted, Long-Term DoD Partner for Innovation and Invention

Examples include the following:

- invented the first-of-its-kind **DevSecOps Platform Independent Model** to help organizations in highly regulated environments implement DevSecOps securely
- **applied analytical methods to insider threat** cases, to create tools for government programs to detect, mitigate, and prevent insider threats
- adapted its **vulnerability research** to help develop the DoD Vulnerability Disclosure Program (VDP)
- codified the **CERT Resilience Management Model** to improve operational resilience
- invented tools to **automatically detect and repair** two critical software-coding errors
- innovated the **Pharos Binary Static Analysis Framework** to automate the reverse engineering of malicious software. Pharos is built on the Rose compiler infrastructure developed by Lawrence Livermore National Laboratory.

About the SEI

Always focused on the future, the Software Engineering Institute (SEI) advances software as a strategic advantage for national security. We lead research and direct transition of software engineering, cybersecurity, and artificial intelligence technologies at the intersection of academia, industry, and government. We serve the nation as a federally funded research and development center (FFRDC) sponsored by the U.S. Department of Defense (DoD) and are based at Carnegie Mellon University, a global research university annually rated among the best for its programs in computer science and engineering.

Contact Us

CARNEGIE MELLON UNIVERSITY
SOFTWARE ENGINEERING INSTITUTE
4500 FIFTH AVENUE
PITTSBURGH, PA 15213-2612

sei.cmu.edu
412.268.5800 | 888.201.4479
info@sei.cmu.edu

Scan the QR code with your smartphone camera for a digital version of this fact sheet.

insights.sei.cmu.edu/library/making-software-the-strategic-advantage/