

Engage Our Experts

Software-reliant systems and networks are vital to Air Force operations. When designed using the best architecture, development, and security practices, these systems provide improved lethality, better situational awareness, secure operation, high reliability, and increased maintainability.

The SEI is a Department of Defense federally funded research and development center (DoD FFRDC) operating as part of Carnegie Mellon University (CMU). We are the only FFRDC focusing specifically on software-related security and engineering issues.

Our mission is to support the Nation's defense by advancing the science, technologies, and practices needed to acquire, develop, operate, and sustain software systems that are innovative, affordable, trustworthy, and enduring. We serve as a value-added broker of R&D, working with Government, academia, and industry to customize, develop, and adapt software and cybersecurity technologies for the measurable benefit of the DoD.

For the Air Force, the SEI is positioned on the front lines of software and cybersecurity R&D, providing credible, independent advice and applying technologies to enable programs to overcome significant challenges across the acquisition and sustainment process.



The Carnegie Mellon University Software Engineering Institute (CMU SEI) serves the nation as a Federally Funded Research and Development Center (FFRDC) sponsored by the U.S. Department of Defense (DoD) and based at Carnegie Mellon University.

Contact Us

CARNEGIE MELLON UNIVERSITY
SOFTWARE ENGINEERING INSTITUTE
4500 FIFTH AVENUE, PITTSBURGH, PA 15213
sei.cmu.edu | info@sei.cmu.edu
412.268.5800 | 888.201.4479

Building Software Engineering Capabilities for the Air Force

What Our Air Force Customers Are Saying About Us

"The SEI provides crucial domain expertise for [Global Hawk] tech reviews, CDRL reviews, proposals, engineering change proposal evaluation and contractor audits."

"I agree with your team's findings and recommendations. You've identified several key gaps that I need to get my arms around."

"We're already implementing your recommendations and addressing SEI's observations—it's critical to continued success in steering the GPS Enterprise."

"SEI is adding a lot of value [for F-22 modernization], and a lot of people are saying this."





New Solutions for Verifying Critical Systems

The DoD faces an overwhelming challenge when developing complex systems: how to verify that the software will do the right thing at the right time—which is especially important when the work is safety or mission critical. Working with the Air Force Research Laboratory at Wright-Patterson Air Force Base, SEI researchers continue to make significant advances in software model checking and timing verification that can be applied earlier in the development lifecycle to reduce the cost of assurance.



Video Summarization and Search

The DoD is developing object detectors that apply foundational computer vision and machine learning technology for object recognition in aerial surveillance images. While existing object detectors can indicate the presence of people, vehicles, and other things, they neither provide information about object significance and actions in context nor recognize and interpret more complex patterns of people, objects, and interactions over time and space. The SEI is building tools that use machine learning and other techniques to recognize and alert analysts when complex patterns are detected.



Enabling Agile Adoption in the DoD

Commercial organizations have reported the benefits of using the iterative, incremental software development methods known as Agile—and the DoD would like to obtain similar results. The SEI has created a range of resources to help the DoD reap the benefits of Agile and lean-based approaches while adhering to DoD acquisition policy. The SEI Agile team has trained more than 1700 practitioners, provided expert information to senior leaders and policymakers, and is directly supporting a range of DoD and AF programs to include: DCGS-AF, F-22, AF/A4, AEHF, AMPD, and PEO Digital.

Photo courtesy of the U.S. Air Force.



Technology and Know-How to Prepare the Cyber Mission Force

The SEI Simulation Training and Exercise Platform (STEP) enables cyber operators and analysts to train-as-they-fight. USCYBERCOM uses this technology to support Cyber Flag and Cyber Guard tactical exercises and as the basis for its Persistent Training Environment. In addition, AFCYBER, ARCYBER, MARFORCYBER, and others choose SEI platforms for their cyber capabilities exercises.



Securely Integrating IoT Devices in Mission Environments

The use of Internet of Things (IoT) devices in DoD systems expands the attack surface on the battlefield and in other resource-constrained and adversarial environments. Existing IoT security approaches focused on the home and industry are inadequate in these situations. The SEI is working to ensure IoT devices are resilient to high-priority threats and able to achieve their missions even in disconnected, intermittent, and limited environments. We are moving the burden of security from the device to the network, which will drastically reduce the time to deploy IoT devices in a DoD setting.



New Technologies Fusion in Dynamic Network Defense Platform

Dynamic network defense hinges on creating unpredictable conditions for cyber attackers. The SEI is bringing together new technologies to create a reference implementation for a dynamic network defense platform. The platform will have a rich data model for advanced planning, “human-in-the-loop” support, and extensibility.