

Armament Cyber Engineering (ACE) Laboratories

The Armament Cyber Engineering (ACE) Labs enable the Armament Cyber Engineering & Cybersecurity Assessment (ACE & CA) Branch to evaluate armament systems and other information systems for their resistance to security threats across all project phases.

The ACE Labs were created to satisfy the needs of clients who employ the ACE & CA Branch to secure both new and existing information systems, assess information systems for compliance with DoD and U.S. Army Cybersecurity & Information Assurance (IA) requirements and regulations, assist with IA & Cybersecurity problems, answer IA & Cybersecurity questions, assist legacy DoD Information Assurance Certification & Accreditation Process (DIACAP) systems transition to Risk Management Framework (RMF) For DoD Information Technology (IT), create RMF Security Authorization Packages (SAP) and other Cybersecurity & IA related documentation, and assist with customer Cybersecurity & IA related requirements. The ACE Labs are designed to be reconfigurable, and are being constantly updated and expanding to meet the needs of our clients in an ever evolving threat environment. When necessary, new equipment or software is added to the labs to ensure that customer needs and employee training needs can be met.

The ACE Labs reconfigurable environment is housed within a quarantined enclosure, allowing ACE Engineers to thoroughly evaluate cyber products without the risk of contaminating external networks or non-target system. They offer a unique opportunity to work with target systems, under highly controlled conditions, before working in a client's operating environment. These labs are also available for training and evaluation of vulnerability detection software, such as Assured Compliance Assessment Solution (ACAS), Security Content Automation Protocol (SCAP) Scanner, Flying Squirrel and other tools.

The Quarantined environment of the ACE Labs consist of both networked & standalone systems. Equipment in the ACE Labs include the following:

- Cisco Network Equipment
- Microsoft Windows Servers
- Microsoft Windows Workstations/Laptops
- Linux Workstations/Laptops
- Legacy Systems
- Flexible workstations not connected to the network for training and testing purposes. These workstations can have various operating systems and software installed and can be used for testing new products and for training in less-often used Operating Systems and Software.
- Workstations connected to the DREN for research purposes and for downloading patches, antivirus signatures, etc.

Point of Contact

Armament SEC Business Planning and Development
usarmy.armamentsec@mail.mil
<http://www.ardec.army.mil/armamentsec>

(973) 724-ASEC (2732)
DSN 880-ASEC (2732)