ARMY CIO/G-6

Common Operating Environment

What is it?

The Common Operating Environment (COE) is an approved set of computing standards and technologies to which the Network and all applications and systems riding the Network must adhere. The COE defines minimum configurations for the Army's computing environments, from the enterprise server to mobile small handheld devices.

The COE fulfills one objective of Army Software Transformation (AST), which aims to alter the way the Army defines, develops, tests, certifies and delivers software applications to the Soldier. AST calls for standardized end-user environments and software development toolkits; a streamlined end-to-end enterprise software process; and creation of an Army Software Marketplace.

Why is it important to the Army?

By establishing a uniform architecture, the COE will enable quicker, and potentially cheaper, development and fielding of secure interoperable applications and systems that satisfy current operational requirements. Industry will know in advance the standards to which it must build solutions, cutting acquisition timelines and possibly cost. The COE also will reduce the complexities of configuration, support and training, making integration of new capabilities with existing technology much easier and faster.

In addition, by adopting certain industry norms, such as Everything over Internet Protocol, the Army will open the door to using more commercial-off-the-shelf or near-COTS equipment and applications.

What has the Army done?

In October 2010, the Army released the initial COE architecture guidance document. Alignment with the COE is mandatory for new systems and capabilities; the Army is in the process of bringing existing programs of record and non-PORs into compliance, as well. The current COE architecture and additional COE information can be found at:
http://ciog6.army.mil/ToBeArchitecture.aspx

What does the Army have planned for the future?

The Assistant Secretary of the Army (Acquisition, Logistics and Technology) will publish a COE Implementation Plan, outlining a governance structure for compliance enforcement and independent validation and verification of program-of-record migration and adherence to the COE. The Army Acquisition Executive will reinforce the implementation plan through an acquisition decision memorandum that identifies the conditions and schedule by which the PEO community must implement the COE.

In parallel, the CIO/G-6 will establish a compliance framework for program of record (POR) and non-POR transition to the COE. The framework will address all aspects of COE compliance, to include pre-deployment test and certification; operational testing; and post-deployment COE compliance assessments. The G-3/5/7 also will publish guidance for Army-wide compliance enforcement. ■

Continue to visit http://CIOG6.Army.mil for further information.

The Network of 2020: Powering America's Army

The individual warfighter and the collective Army rely more heavily than ever before on information technology to execute the mission. The data and capabilities Soldiers need – among them intelligence, surveillance, reconnaissance, communications and command and control – are all obtained through the Network.

Today's versatile mix of tailorable, linked organizations operates on a rotational cycle and conducts wide-ranging, full-spectrum operations. For the Network to fulfill the requirements of this dynamic force – securely, on demand and as far as the tactical edge reaches – it must become a unified, global system.

The Army is laying the foundation for this global Network by standardizing the underlying architecture; consolidating and centralizing Network operation, defense and services; and reforming development, acquisition and fielding processes. Ultimately, these changes will produce a seamless, technologically modern Network that is always available and always trusted, regardless of location or environment. ■

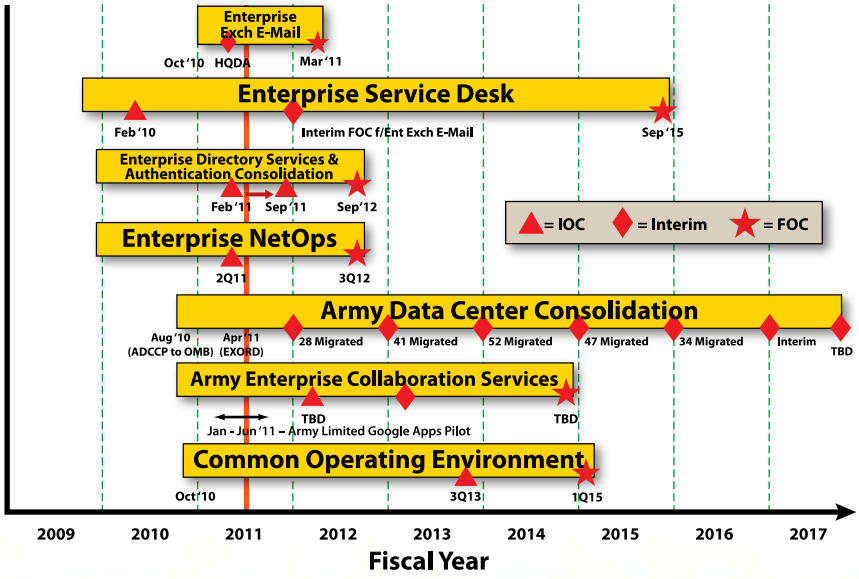
Why is LandWarNet important to the warfighter?

The ability to fight upon arrival is critical to enabling the predominantly CONUS-based Army to respond effectively to any threat in any environment. The Army's current networks, information systems and resources are not sufficient to support a true fight-upon-arrival capacity. Access to the Network and information technology resources is inconsistent; units must deal with numerous IT-related changes as they move from one physical location to another and one phase of the Army Force Generation cycle to another. However, by providing all warfighters universal access to their applications, data and collaboration and training resources, as well as one email address and telephone number, the Army will achieve this essential fight-upon-arrival capability.

Where Are We Now?

Over the past year, the Army has adopted standards and protocols, based on those of the commercial sector, for the Network's architecture and transmission means. The goal is to accelerate software development and increase network security. The Army also began to centralize Network management and services through initiatives such as enterprise email, collaboration, directory services and authentication, and data center consolidation. Additionally, the new Army Cyber Command assumed responsibility for operation and defense of the Network. With fiscal reality and the always adapting enemy in mind, the Army will continue to define and refine Network doctrine, tactics, techniques and procedures, and to incorporate technological advances, customer demands, national strategic objectives and process improvements. ■

Top Strategic Initiatives and Implementation Timeline



Enterprise Exchange Email & Calendar

Enterprise Service Desk

Enterprise Directory Services and Authentication Consolidation

Enterprise Network Operations (NetOps)

Army Data Center Consolidation

Army Enterprise Collaboration Services

Common Operating Environment

Contact: CIOG6StratComm@conus.army.mil

U.S. ARMY