

Enterprise Directory Services and Authentication Consolidation

What is it?

Enterprise Directory Services and Authentication (EDSA) provides secure user authentication and access to the Army's Network. Currently, the Army uses multiple Microsoft Active Directory® network operating environments, called forests, to authenticate to the Network and access IT resources, such as documents, presentations, spreadsheets and other files. Under the command and control of Army Cyber Command, the Army is standardizing and consolidating these multiple forests, and integrating disparate groups of users and accounts into a global EDSA architecture for both the Non-secure and Secret Internet Protocol Router Networks (NIPRNet and SIPRNet, respectively).

Why is it important to the Army and to individual Soldiers?

A standardized, centrally managed EDSA environment significantly enhances mobility, command and control, network security and the overall defense posture. In today's localized environment, the mobile Soldier and civilian transitioning from one location to the next, via permanent change of station, temporary duty or base realignment and closure, often are unable to access their IT resources physically located elsewhere. This includes units moving from home station to forward deployed locations. The new enterprise environment will enable secure, assured access to global IT resources, regardless of location, and support workforce mobility across theaters.

What has the Army done?

The EDSA forest architecture is built around five theaters: the continental United States, Southwest Asia, Europe, Korea and the Pacific. Army Cyber Command has developed detailed plans of action and milestones for each phase of implementation and migration; the Army Cyber Command EDSA execute order (EXORD) will articulate the details.

What does the Army have planned for the future?

Army Cyber Command will publish the EDSA EXORD in fiscal year 2011, which will establish policy and tasks to guide Army stakeholders and functional commands operating Microsoft Active Directory® environments through forest consolidation. Among those activities, the Army will upgrade the EDSA infrastructure (hardware and software) in the near future, and migrate most functional users around the world from the current numerous and varied account structures to the standardized EDSA environment. ■

Reference in this website/information paper to any specific commercial products, processes or services, or the use of any trade, firm or corporation name, is for the information and convenience of the public and does not constitute endorsement, recommendation or favoring by the U.S. Army. Contact CIOG6StratComm@conus.army.mil

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

ARMY CIO/G-6

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. ■

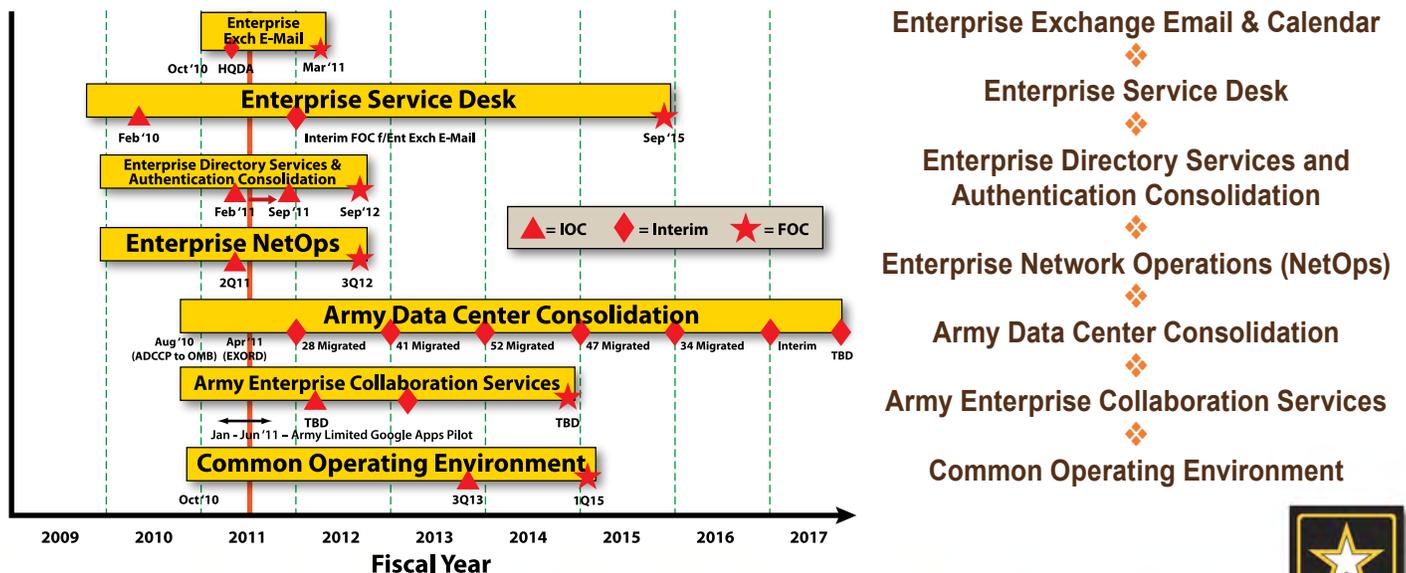
Why is LandWarNet important to the warfighter?

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

