Army Win10 Transition

# Terms & Definitions

*Updated September 2016*

**AppLocker:** Provides seamlessly integrated protection at the kernel level.

**Credential Guard:** Hardware and virtualization-based security that better defends against advanced persistent threats. It protects user credentials by leveraging virtualization within Windows to isolate those credentials from the operating system, and counters the pass-the-hash technique used in nearly all major Windows intrusions..

**Deployment:** After a region completes the Early Adopter phase, it moves to deployment, migrating all technically suitable computers to Windows 10. Deployment will occur by organization (for instance, a division, a Command, a Program Executive Office) and may take several weeks to several months to complete, depending on the organization's number of computers.

**Early Adopters (EAs):** The first organizations to employ Windows 10. EAs are testing and evaluating Windows 10, on a limited number of computers, to discover general implementation issues and any challenges particular to their environment, and to help determine the best implementation practices and processes. The Army has selected multiple EAs by region (Europe, Southwest Asia, CONUS, Pacific/Korea).

**Enhanced Mitigation Experience Toolkit:** Anticipates most common actions and techniques adversaries might use in compromising a computer.

**Global Enterprise Fabric (GEF):** A global cluster of virtual machines, which are tightly integrated, connected, controlled and managed, that hosts Army network operations tools and capabilities, data analytics capabilities, installation processing needs and defensive cyber capabilities. The hub-and-spoke architecture includes components at the installation, regional and enterprise levels. The GEF merges physical and virtual environment silos into a single, enterprise-managed hosting environment.

**Host-Based Security System (HBSS):** A suite of commercial off-the-shelf software used to monitor, detect and defend Army and DoD networks and systems.

**Malicious Software Removal Tool:** Provides the capability to specify which users or groups can run particular applications.

**Peripherals:** Devices that connect to a computer or the network to add functionality, such as a mouse, keyboard, monitor, printer, scanner, CAC reader or webcam.

**Program of Record (PoR):** To be considered a PoR, a program must be included (and funded) in the current Future Years Defense Program. PoRs have a "line item record" in the official Army budget. Weapon systems and warfighting platforms, such as the Abrams tank, Paladin howitzer, Apache helicopter, Hellfire missile and Warfighter Information Network - Tactical, are PoRs.

*References to any 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 an endorsement, recommendation, or preferential treatment by the U.S. Army.*

# Terms & Definitions

**Secure Hash Algorithm (SHA):** Originally developed by the National Security Agency, a secure hash algorithm is a set of cryptographic functions used to digitally sign content, thereby validating its integrity. SHAs are a component of any digital certificate. Windows 10 requires SHA2 (also known as SHA-256).

**Secure Host Baseline (SHB):** An SHB is a pre-configured, security-hardened, machine-ready image that contains an organization's common operating systems and application software. The Windows 10 SHB requires specific modules and patches, including the Host-Based Security System (HBSS), Credential Guard and Device Guard. The Windows 10 SHB will make host security configuration management activities more uniform across the Army and DoD.

**Security Center Configuration Manager (SCCM):** Software that enables management of large groups of computers running the Windows operating system (as well as select other operating systems). It provides remote control, patch management, software distribution, operating system deployment, network access protection and hardware and software inventory. SCCM 2012 R2 is required to implement Windows 10 and its companion SHB.

**Security Implementation Technical Guide (STIG):** The configuration standards for DoD information assurance (IA) and IA-enabled devices and systems. The STIGs contain technical guidance to "lock down" information systems and software that might otherwise be vulnerable to a malicious computer attack.

**SmartScreen:** Identifies malicious websites and scans for suspicious characteristics.

**Trusted Platform Module (TPM):** A hardware module installed on the computer's motherboard that can be used to securely store items, such as keys and hashes. A hardware module is a more secure method of storing these items than software. DoD currently allows TPM 1.2 or 2.0. All new hardware purchases, however, must have TPM 2.0.

**Virtual Desktop Infrastructure (VDI):** With VDI, the desktop operating system is hosted within a virtual machine on a centralized server. VDI is sometimes labeled thin-client computing or server-based computing. The virtualization process separates the software aspects that define a user's personality from the operating system and applications, which are managed independently and applied to the desktop as needed without the requirement for scripting or roaming profiles.

**Windows Defender:** Malware protection that helps to defend against Zero Day attacks. Its configurable code integrity improves tamper resistance.

*References to any 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 an endorsement, recommendation, or preferential treatment by the U.S. Army.*