DEFENSE INFORMATION SYSTEMS AGENCY
The IT Combat Support Agency

Secure Host Baseline

Windows 10 Migration

21 April 2016

Presentation Disclaimer

"The information provided in this briefing is for general information purposes only. It does not constitute a commitment on behalf of the United States Government to provide any of the capabilities, systems or equipment presented and in no way obligates the United States Government to enter into any future agreements with regard to the same. The information presented may not be disseminated without the express consent of the United States Government. This brief may also contain references to Unite States Government future plans and projected system capabilities. Mention of these plans or capabilities in no way guarantees that the U.S. Government will follow these plans or that any of the associated system capabilities will be available or releasable to foreign governments."

Panel Member Introductions

Terri Parks, NSA

Ed Zick, DoD CIO

Ray Perry, AFECMO

Rick Munck, AFECMO

Chris McKinney, DISA RME

Mike Hayes, DISA ID

Overview

- **Task:** DoD CIO priority to migrate IT systems running MS Windows operating systems to Win10 by 31 January 2017; tasked DISA to lead rollout

- **Methodology:** Services implement DoD Win10 Secure Host Baseline as a security hardened, STIG compliant "build from" capability
  - Leveraging refined NSA and Air Force standard desktop process
  - New paradigm for continuous updates and patching; will be available on Information Assurance Support Environment (IASE) portal
  - Will include commonly used and mandated applications (i.e., Google Chrome)

- **Benefits**: Win10 security enhancements, fewer configurations, improved interoperability, enterprise licensing, apps rationalization

Background

- Apr 2009 efforts began with Standard Desktop Configuration (SDC)/DoD Server Core Configuration (DSCC) “images”
- Oct 2010 CENTCOM Unified Golden Master (UGM) for AOR urgent needs
- Oct 2011 MilDep CIO buy-in for Unified Master Gold Disk (UMGD) concept
- Dec 2012 Request from Dep DoD CIO for Cyber Security to Create PMO
- Oct 2013 Rebranded to Secure Host Baseline (SHB) “build from”
- May 2014 released first SHB for Win 7 on DISA IASE web site
- Sept 2015 DoD CIO request for Win 10 SHB rapid rollout across DoD

Leveraged AF’s standard desktop image experience to develop current methodology

Joint Secure Host Baseline Working Group*

Lead by NSA and DISA

Partnership

- DoD CIO
- AF Enterprise Configuration Management Office (AFECMO)

Lead Integrators

- Government
  - NSA
  - DISA
  - DoD CIO
  - AFECMO
  - OSD
  - USMC
- Industry
  - Microsoft
  - Apple
  - Red Hat
  - Other vendors

**Formerly call the Joint Consensus Working Group*

Development Team

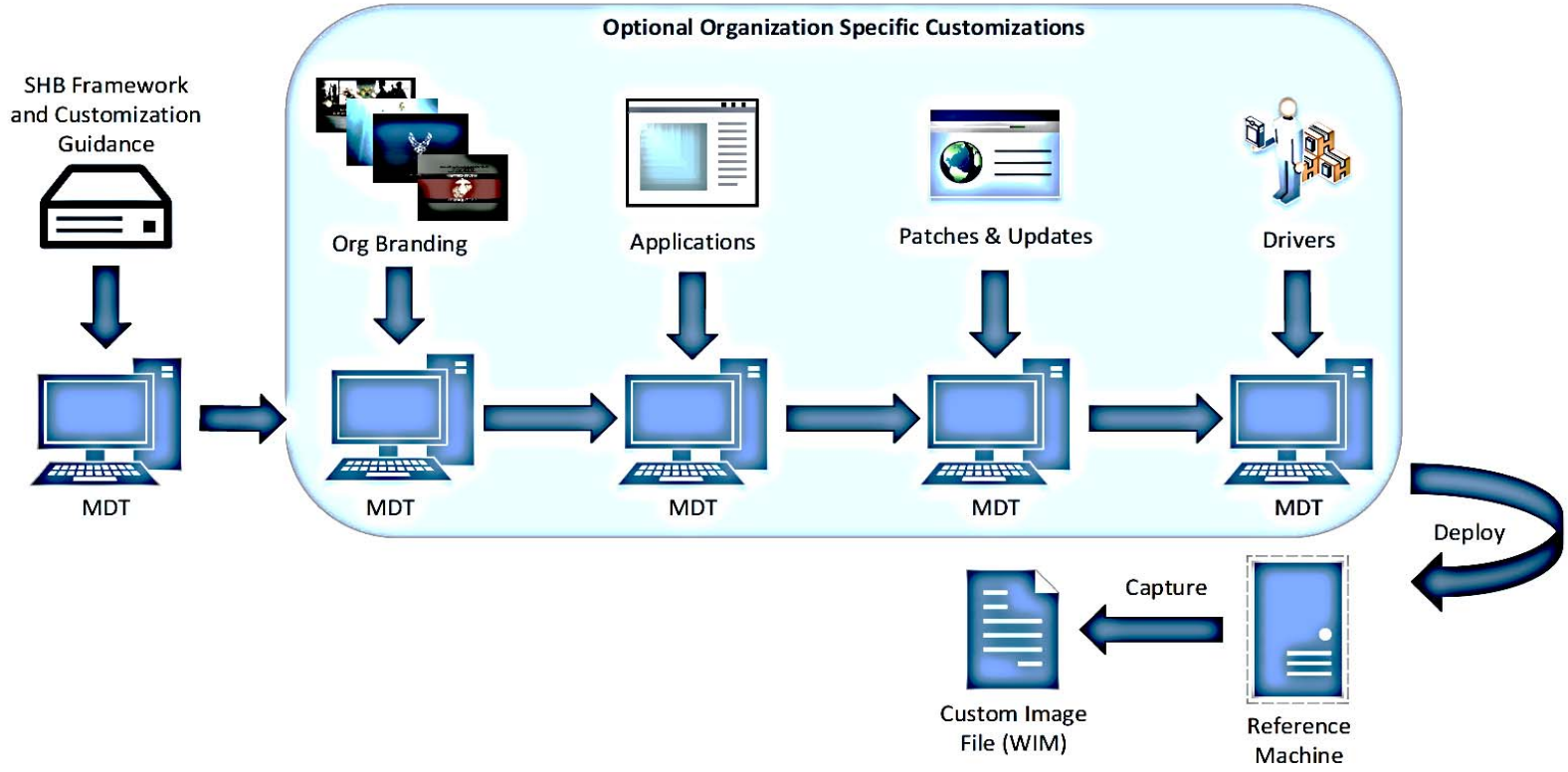
DoD joint initiative and validation

- Security Technical Implementation Guides (STIG) worked thru Security Settings Reviews (SSR)
- Hardened baselines
  - Windows
  - Apple
  - Linux
  - Various applications
- Inheritance and reciprocity
- .mil

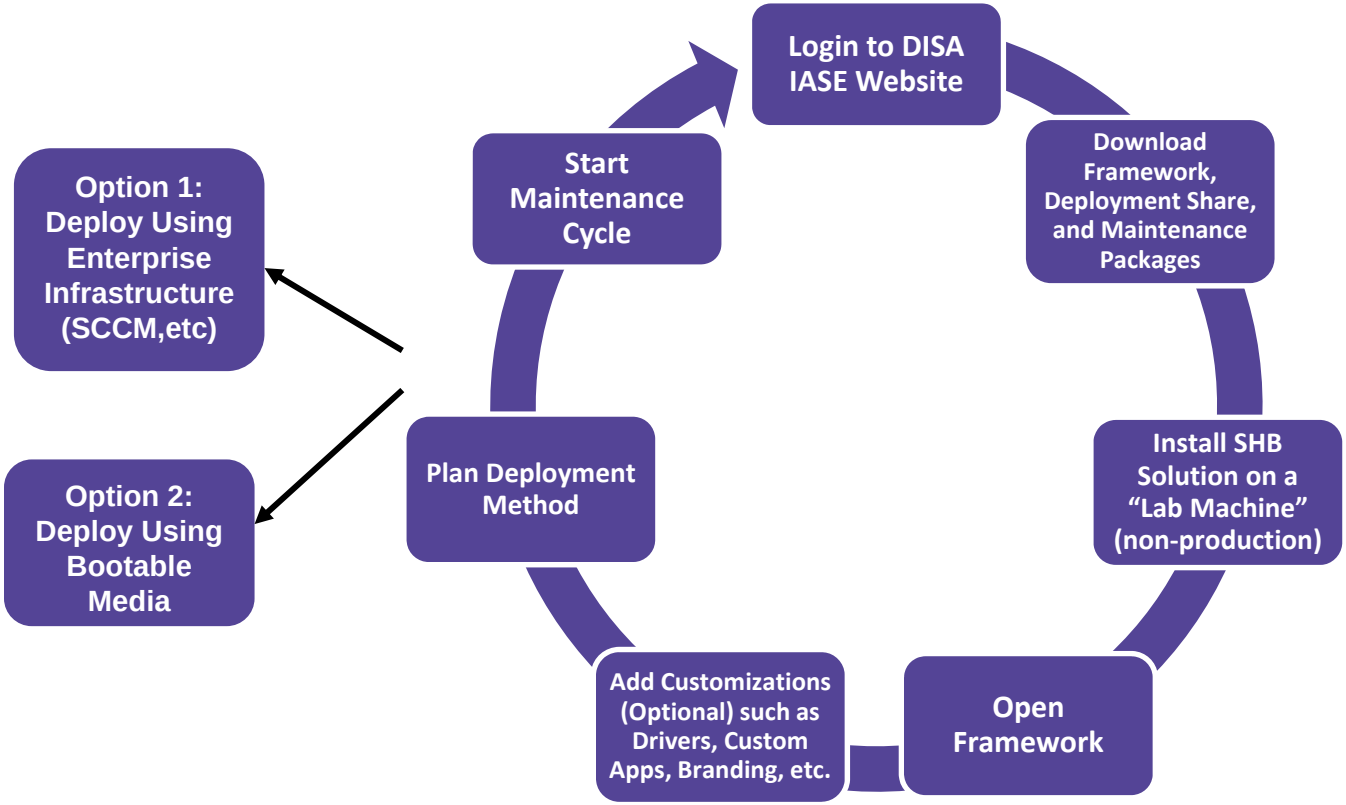
AFECMO

- Tasked by NSA/Joint SHB WG to develop Windows baselines
- On-going effort since 2009 with several “published” OS baselines
- Funded by NSA to develop for the DoD

Solution Overview



End-to-End Process



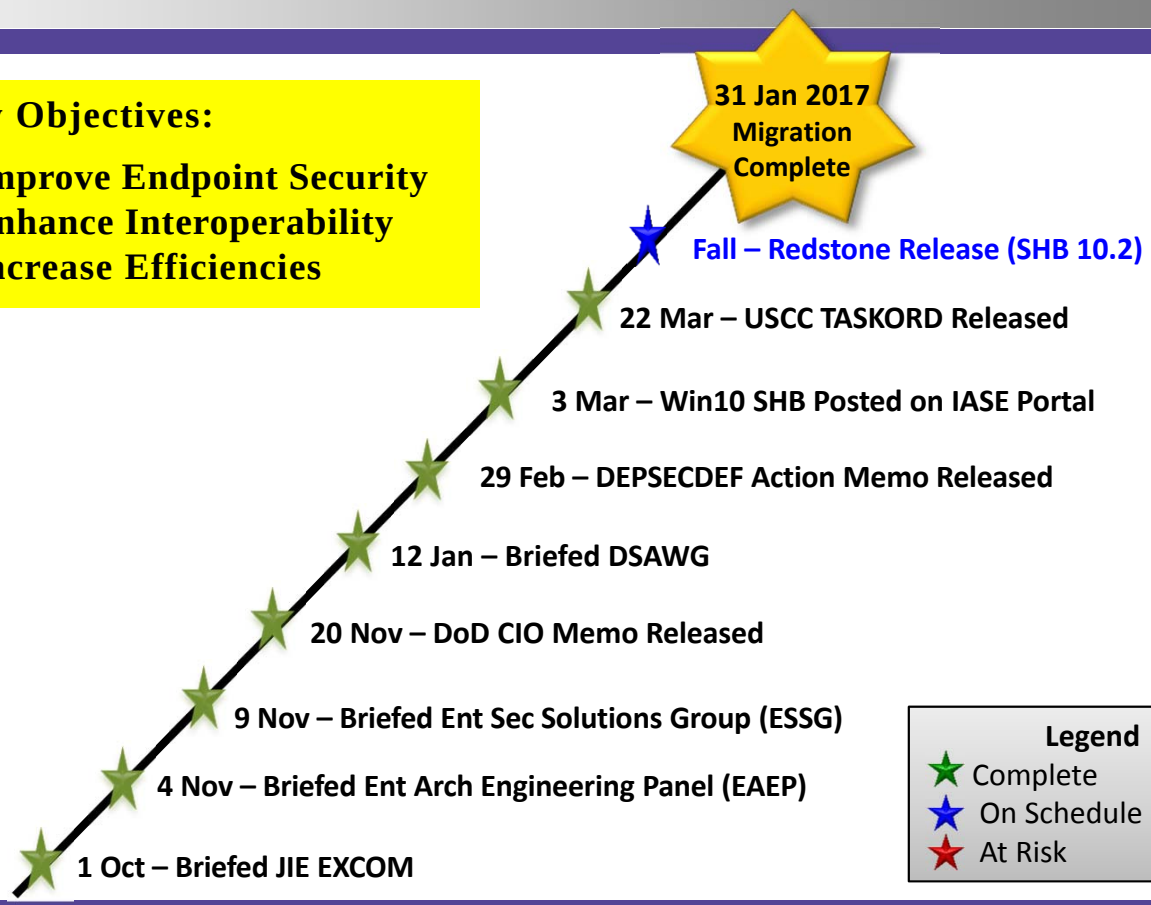
Windows 10 Secure Host Baseline Milestones

Challenges

- Third-party driver compatibility issues
- VDI compatibility with Credential Guard
- Hardware upgrades (legacy systems)

Key Objectives:

- **Improve Endpoint Security**
- **Enhance Interoperability**
- **Increase Efficiencies**



Backup Slides

PREPARE HBSS ECOSYSTEM PRIOR TO SHB DEPLOYMENT

- **Prior to deploying Windows 10, site HBSS ecosystem must be prepared to support Windows 10. SHB requires specific modules and patches that have been updated to support the DoD Windows 10 SHB framework.**

- **Site Administrators will have to verify the applicable modules and patches are configured in the local ePO for deployment to new Windows 10 clients. Failure to use the correct versions of modules and patches will result in a catastrophic failure at the endpoint.**

- **The HBSS Windows 10 information is located on the DISA IASE web portal under the Windows 10 SHB section:**
  - **https://disa.deps.mil/ext/cop/iase/dod-images/Pages/Win10.aspx**
  - **https://disa.deps.mil/ext/cop/mae/CyberDefense/HBSS/SitePages/win10updates.aspx**

- **DISA and USAF team have coordinate a Software Forge site where administrators can collaborate on both the Windows 10 (USAF) and HBSS (DISA) aspects of the SHB deployment.**

Win10 SHB Applications – "First Release"

Application	Install Default
AppLocker Whitelist Starter Policy	Mandatory
Group Policy	Mandatory
Image Branding	Mandatory
McAfee VirusScan Enterprise	Mandatory
Microsoft NetBanner	Mandatory
NIPRNet DoD Root Certificates	Mandatory
Windows 10 Enterprise (CBB)	Mandatory

All apps (both mandatory and optional) have STIGs or meet NSA security specs; common DoD-wide apps

Application	Install Default
ActiveClient	Optional
Adobe Acrobat Reader	Optional
Adobe Flash Player Plugin-based browser	Optional
Adobe Shockwave Player	Optional
Axway Desktop Validator	Optional
DoD Trusted Sites List	Optional
Google Chrome	Optional
Local Security Policies	Optional
Microsoft Office Professional (x86)	Optional
Oracle Java Runtime Engine	Optional
Oracle Java Runtime engine (x64)	Optional
SIPRNet 90meter	Optional
SIPRNet DoD Root Certificates	Optional

Win10 Security Improvements

Credential Guard	Counters pass-the-hash technique used in nearly all major Windows intrusions
Windows Defender	Malware protection
AppLocker	Seamlessly integrated; protection at the kernel level
Malicious Software Removal Tool	Provides a capability to specify which users or groups can run particular applications
Enhanced Mitigation Experience Toolkit	Anticipates most common actions and techniques adversaries might use in compromising a computer
SmartScreen	IDs malicious websites; scans for suspicious characteristics

Future ***potential*** to sunset existing duplicative security tools

Win10 Security Improvements

Credential Guard	Counters pass-the-hash technique used in nearly all major Windows intrusions
Windows Defender	Malware protection
AppLocker	Seamlessly integrated; protection at the kernel level
Malicious Software Removal Tool	Provides a capability to specify which users or groups can run particular applications
Enhanced Mitigation Experience Toolkit	Anticipates most common actions and techniques adversaries might use in compromising a computer
SmartScreen	IDs malicious websites; scans for suspicious characteristics

Future ***potential*** to sunset existing duplicative security tools