Air Force Progress in Implementing Standard Desktop Configurations

Information Security and Advisory Board
June 7th, 2007

Ken Heitkamp
Associate Director, Life Cycle Management (SAF/XCD)
and Director, USAF IT Commodity Council
Air Force Office of Warfighting Integration and CIO
Overview

- Background
- Air Force XP Standard Configuration
- Plans for DoD Vista Standard Configuration
Enterprise Client PC Hardware

Step 1: USAF Quarterly Enterprise Buy (QEB) Standards– Implemented since 2003; 333,249 purchased

Enterprise Licensing and Services

Step 2: USAF Enterprise Agreement with Microsoft – Implemented in Jul – Sep 2004

Enterprise Client, Server, and Active Directory Configurations

Step 3: USAF Standard Desktop Configuration – AF wide implementation in 2006; Servers 2007

Enterprise Configuration and Patch Management


Comply and Connect Enforcement

Step 5: USAF Comply, Connect and RemEDIATE policy and processes – Incremental improvements 2006-2008

Security & Capability Roadmap
Standard Desktop Configuration

- Windows XP SP2/Office 2003/IE7 (SDC 1) and Vista/Office 2007/IE 7 (SDC 2)
  - Security, performance, feature, compatibility & usability baseline settings
  - Developed by NSA, DISA, DHS, NIST, Microsoft, Air Force Army, Navy, and Marines (security, operators, software developers)
  - Air Force core applications preinstalled (e.g., Acrobat, Anti-Virus)
  - No Administrative Rights for normal users
  - Firewall Enabled
  - Updated Quarterly (patches, drivers, updates)
  - Preinstalled by hardware vendors on new computers
  - Current image supports well over 75 desktop & laptop platforms

- Active Directory Group Policy Enforcement
  - Allows the Network commander to enforce the configuration and rapidly change settings for operational needs

OMB: By 1 May 2007, agencies using Microsoft Windows XP and Vista must develop plans for using security configurations by Feb 2008
SDC 1.x AF Wide NIPRNET Metrics

Goal: 100% by 31 Dec 06

Standard Desktop Configuration

- 510,198 Total PCs
- Over 425,000 PCs using SDC
- 197 Exception Requests

Incremental implementation orders:
- XP SP2 (99%)
- Firewall (98%)
- Smart Card Login (89%)
- Limited Admin Rights (92%)
- SDC 1.0 (92%)

As of 10 Apr 2007

OMB: Secure configurations; restrict administration to authorized professionals
Major Reasons for Incompatibility

- 197 Exception requests; only a small number approved that affect over 50,000 PCs
- Major causes of over 75% of application incompatibilities:
  - Requires normal end users to run with local system admin rights
  - Write to restricted Windows areas (e.g., Registry)

OMB: By July 2007, ensure new acquisitions use these configurations and certify their products operate effectively using these configurations
A narrow “WINDOW” Of Opportunity for a Federal Desktop Common Configuration with Vista
SDC 2.0 Benefits
(Vista, Office 2007, IE 7)

■ Security
  ■ User Account Control to limit privileged system access
  ■ IE 7 runs in “protected mode” on Vista
  ■ Windows Services Hardening and Memory Randomization
  ■ Firewall (inbound and outbound) that can be controlled by group policy
  ■ Data encryption capabilities
  ■ “Comply and Connect” Network Access Protection Client

■ Manageability
  ■ 600+ new network group policy settings
  ■ Power management controls

■ Other Improvements
  ■ Integrated search integrated into user interface
  ■ User Interface -- ease of use
  ■ Native IPv6 foundation that can be consistently installed AF and DoD wide
  ■ New file formats; less storage required
**DoD SDC Progress**
(For the Image and Group Policies)

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Vista (Security Only)</td>
<td>217</td>
<td>217</td>
<td>0</td>
<td>279</td>
<td>251</td>
<td>293</td>
<td>217</td>
</tr>
<tr>
<td>Vista (other GPO settings)</td>
<td>1258</td>
<td>36</td>
<td>14</td>
<td>244</td>
<td>268</td>
<td>244</td>
<td>244</td>
</tr>
<tr>
<td>Office 2007</td>
<td>173</td>
<td>NA</td>
<td>-</td>
<td>173</td>
<td>173</td>
<td>173</td>
<td>173</td>
</tr>
<tr>
<td>Internet Explorer 7</td>
<td>1192</td>
<td>99</td>
<td>32</td>
<td>162</td>
<td>162</td>
<td>162</td>
<td>162</td>
</tr>
<tr>
<td>Major Delta's from NSA/DISA</td>
<td>-</td>
<td>46</td>
<td>-</td>
<td>7</td>
<td>9</td>
<td>6</td>
<td>-</td>
</tr>
</tbody>
</table>

Notes:

1. DoD SDC settings will be reviewed again after each military service evaluations in an operational test
2. Each military agency is evaluating variations of some settings to obtain feedback for DoD
3. DoD and Service settings include other settings (e.g., performance, usability, compatibility, and features)
4. The Air Force used SSLF security settings (35 were lower, 6 higher out 352)

Over 5,000 man-hours in Joint Meetings to arrive at consensus
Contingent upon successful test and evaluation within DoD

- Support DoD Standard Desktop Configuration (SDC) and Group Policies for DoD certification and use
- Require applications software to function properly with the DoD SDC by a specified date
USAF SDC 2.0
(Vista/Office 2007/IE 7) Plan

- Nov 06 - Establish USAF baseline configuration
- Jan 07 - Build initial USAF test configuration
- Feb 07 - Configuration Testing/Validation
- Feb 07 - Hardware Testing
- Mar 07 - Test XP with IE7 at 8 lead bases (SDC 1.3)
- Apr 07 - DoD Standard Desktop Configuration
  - Apr 07 - Test software applications for compatibility
  - May 07 - Test XP with Office 2007 at 8 lead bases for (SDC 1.5)
  - Jul 07 - Test Vista, Office 2007, IE 7 at 8 lead bases (SDC 2.0)
  - Sep 07 - Earliest timeframe for approved USAF use
  - Jan 09 - Earliest timeframe for mandatory USAF Vista use

OMB: Test configurations to identify adverse effects on system functionality
What About Hardware for Vista?

<table>
<thead>
<tr>
<th>FY03 Q4</th>
<th>FY04 Q4</th>
<th>FY05 Q4</th>
<th>FY06 Q4</th>
</tr>
</thead>
<tbody>
<tr>
<td>OEM: Dell</td>
<td>OEM: HP</td>
<td>OEM: Dell &amp; HP</td>
<td>OEM: HP</td>
</tr>
<tr>
<td>Price</td>
<td>$648</td>
<td>$666</td>
<td>$584</td>
</tr>
<tr>
<td>Technology</td>
<td>2.60 GHz; 512MB RAM 865 chipset</td>
<td>3.0 GHz; 512MB RAM 915 chipset</td>
<td>3.2 GHz w/ HT; 1GB RAM 945 chipset</td>
</tr>
<tr>
<td>$461</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**FY04 Q4**

OEM: HP

- Price: $666
- Technology: 3.0 GHz; 512MB RAM 915 chipset
- 945 chipset

**FY05 Q4**

OEM: Dell & HP

- Price: $584
- Technology: 3.2 GHz w/ HT; 1GB RAM 945 chipset
- 945 chipset
- 3.0 GHz; 512MB RAM 915 chipset

**FY06 Q4**

OEM: HP

- Price: $584
- Technology: 3.4 GHz Dual Core 1GB RAM 945 chipset
- TPM 1.2

**Take Aways**

- Security, Savings, Standardization
- Quarterly Buys
- Buying/Operating Standards
- Standard Desktop Configuration
- Regression Testing for SDC
- 200K support Vista; 100K need .5GB memory upgrade

**20-May-2007**

<table>
<thead>
<tr>
<th>Totals</th>
<th>% to SB</th>
<th># of Computers</th>
<th>QEB Total Cost</th>
<th>Est. Cost Avoidance</th>
</tr>
</thead>
<tbody>
<tr>
<td>FY03 Total</td>
<td>6.5%</td>
<td>29,027</td>
<td>$22,372,599</td>
<td>$6,394,449</td>
</tr>
<tr>
<td>FY04 Total</td>
<td>9.1%</td>
<td>66,827</td>
<td>$61,848,534</td>
<td>$13,938,133</td>
</tr>
<tr>
<td>FY05 Total</td>
<td>15.5%</td>
<td>108,541</td>
<td>$95,140,007</td>
<td>$32,796,574</td>
</tr>
<tr>
<td>FY06 Total</td>
<td>12.9%</td>
<td>106,885</td>
<td>$71,977,291</td>
<td>$36,052,959</td>
</tr>
<tr>
<td>FY07 Total*</td>
<td>6.8%</td>
<td>21,969</td>
<td>$19,250,858</td>
<td>$6,178,636</td>
</tr>
<tr>
<td>Grand Totals</td>
<td>12.0%</td>
<td>333,249</td>
<td>$270,589,289</td>
<td>$95,360,751</td>
</tr>
</tbody>
</table>

* As of QEB 0702 (May 07)
## ITCC’s Vista Hardware Planning Assumptions

<table>
<thead>
<tr>
<th></th>
<th>Windows Vista Capable</th>
<th>Windows Vista Premium</th>
<th>Current USAF Buying Standard</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>GP</strong></td>
<td>A modern processor (at least 800MHz)</td>
<td>1 GHz 32-bit (x86) or 64-bit (x64) processor</td>
<td>Dual Core, 2.13 GHz</td>
</tr>
<tr>
<td><strong>System Memory</strong></td>
<td>512 MB of system memory</td>
<td>1 GB of system memory</td>
<td>2 GB of system memory</td>
</tr>
<tr>
<td><strong>GPU</strong></td>
<td>A graphics processor that is DirectX 9 capable</td>
<td>Support for DirectX 9 graphics with a WDDM driver, Pixel Shader 2.0 and 32 bits per pixel</td>
<td>Support for DirectX 9 graphics with a WDDM driver, Pixel Shader 2.0 and 32 bits per pixel</td>
</tr>
<tr>
<td><strong>Graphics Memory</strong></td>
<td>128 MB (minimum)</td>
<td>256 MB</td>
<td></td>
</tr>
<tr>
<td><strong>HDD</strong></td>
<td>40 GB</td>
<td>160 GB (7200 RPM)</td>
<td></td>
</tr>
<tr>
<td><strong>HDD Free Space</strong></td>
<td>15 GB</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Optical Drive</strong></td>
<td>DVD-ROM Drive</td>
<td>16X DVD-RW/CD-RW</td>
<td></td>
</tr>
<tr>
<td><strong>Audio</strong></td>
<td>Yes</td>
<td>Integrated</td>
<td></td>
</tr>
</tbody>
</table>

2 Processor speed/memory are indicators; AFECMO evaluated each ITCC Quarterly Enterprise Buy Configurations and provided recommendations for each which will be validated at lead bases; also a Vista assessment utility will be provided to run via SMS.
Vision 2008: “Comply and Connect” (Security and Configuration Mgt Process)

Check firewall, Anti-Virus

Check Host Based IPS, IDS Security

Checks SDC configuration

Check patch compliance

SDC Client Compliance Agents

Remediation Servers

Firewall compliance

Anti-virus compliance

SDC configuration and selected security settings

Security and configuration compliance

Digital Policies

Enforcement Servers

Enforcement checks performed at logon and at configurable intervals

Reporting and Notification Server

SDC settings are reapplied through Group Policy at logon and every 90 minutes

Active Directory (Group Policy)

OMB: Implement and automate enforcement of these configurations
USAF Governance

- General Officer Steering Group
- Air Force wide Network Command and Control
- Enterprise Configuration Control Board
- Standard Settings Review
- CIO Policy
- Enterprise Configuration Management Processes
- Enterprise Program Office
- Exception/Waiver Process
- Metrics and measurement

Integrity – Service – Excellence
Questions?