Headquarters U.S. Air Force

I n t e g r i t y - S e r v i c e - E x c e l l e n c e

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
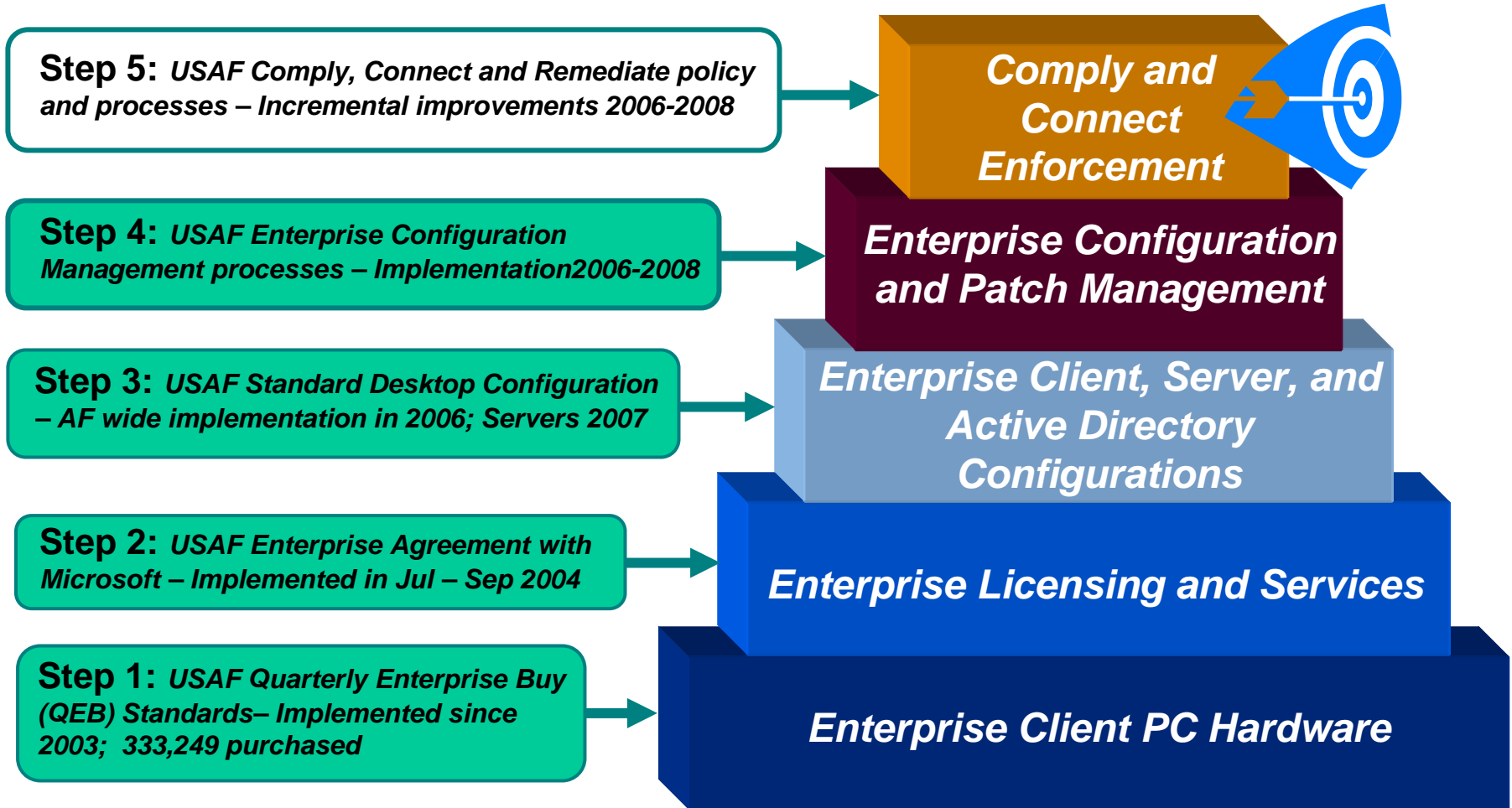**Air Force Office of Warfighting Integration and CIO**

Overview

- **Background**
- **Air Force XP Standard Configuration**
- **Plans for DoD Vista Standard Configuration**

Security & Capability Roadmap

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

Step 4: *USAF Enterprise Configuration Management processes – Implementation 2006-2008*

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

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

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

Comply and Connect Enforcement

Enterprise Configuration and Patch Management

Enterprise Client, Server, and Active Directory Configurations

Enterprise Licensing and Services

Enterprise Client PC Hardware

U.S. AIR FORCE

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
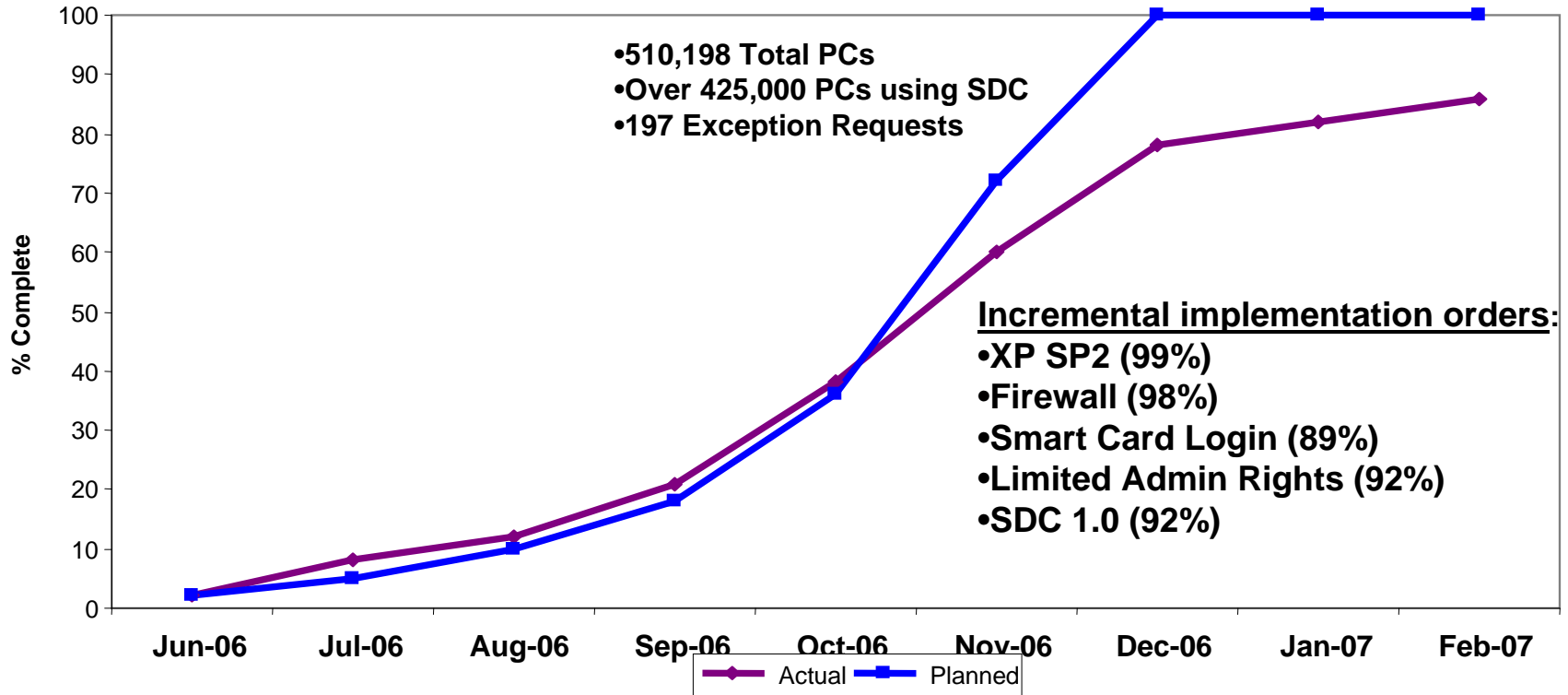
SDC 1.x AF Wide NIPRNET Metrics
Goal: 100% by 31 Dec 06

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%)

Y-axis: % Complete (0–100)

X-axis: Jun-06, Jul-06, Aug-06, Sep-06, Oct-06, Nov-06, Dec-06, Jan-07, Feb-07

Legend: Actual ▬ Planned ▬

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)

	Total Available Settings	Microsoft Security Guide SSLF Settings	NSA/DISA Security Guide SSLF Settings	Air Force Baseline Settings (Nov 9)	Navy Baseline Settings (Dec 8)	Army Baseline Settings (Feb 7)	DoD SDC (9 Apr 2007)
Vista (Security Only)	217	217	0	279	251	293	217
Vista (other GPO settings)	1258	36	14	244	268	244	244
Office 2007	173	NA	-	173	173	173	173
Internet Explorer 7	1192	99	32	162	162	162	162
Major Delta's from NSA/DISA	-	46	-	7	9	6	-

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

Recommendations to DoD CIO Executive Board for OMB Memo

- **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 IE7at 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**
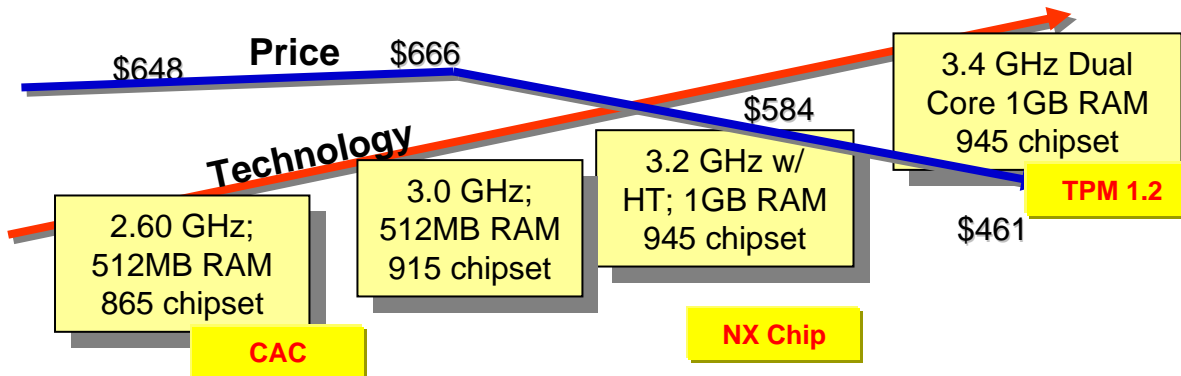- ■ **Jan 09 - Earliest timeframe for mandatory USAF Vista use**

OMB: Test configurations to identify adverse effects on system functionality

What About Hardware for Vista?

U.S. AIR FORCE

FY03 Q4 OEM: Dell	FY04 Q4 OEM: HP	FY05 Q4 OEM: Dell & HP	FY06 Q4 OEM: HP

Price $648 $666 $584

Technology

- 2.60 GHz; 512MB RAM 865 chipset
- 3.0 GHz; 512MB RAM 915 chipset
- 3.2 GHz w/ HT; 1GB RAM 945 chipset
- 3.4 GHz Dual Core 1GB RAM 945 chipset

TPM 1.2 $461

CAC   NX Chip

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

QEB Market Share

Gateway 5%   Lenovo 7%   Dell 39%   HP 49%
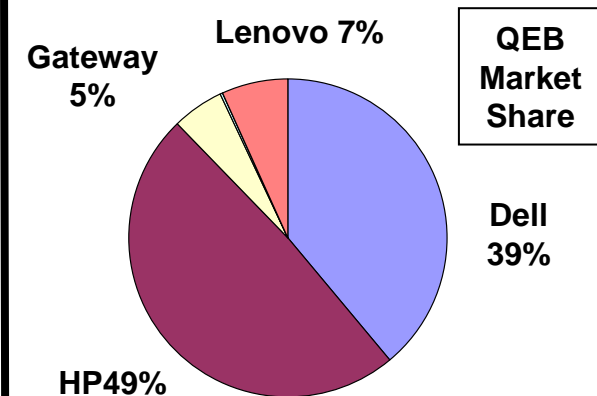
* **As of QEB 0702 (May 07)**

ITCC's Vista Hardware Planning Assumptions

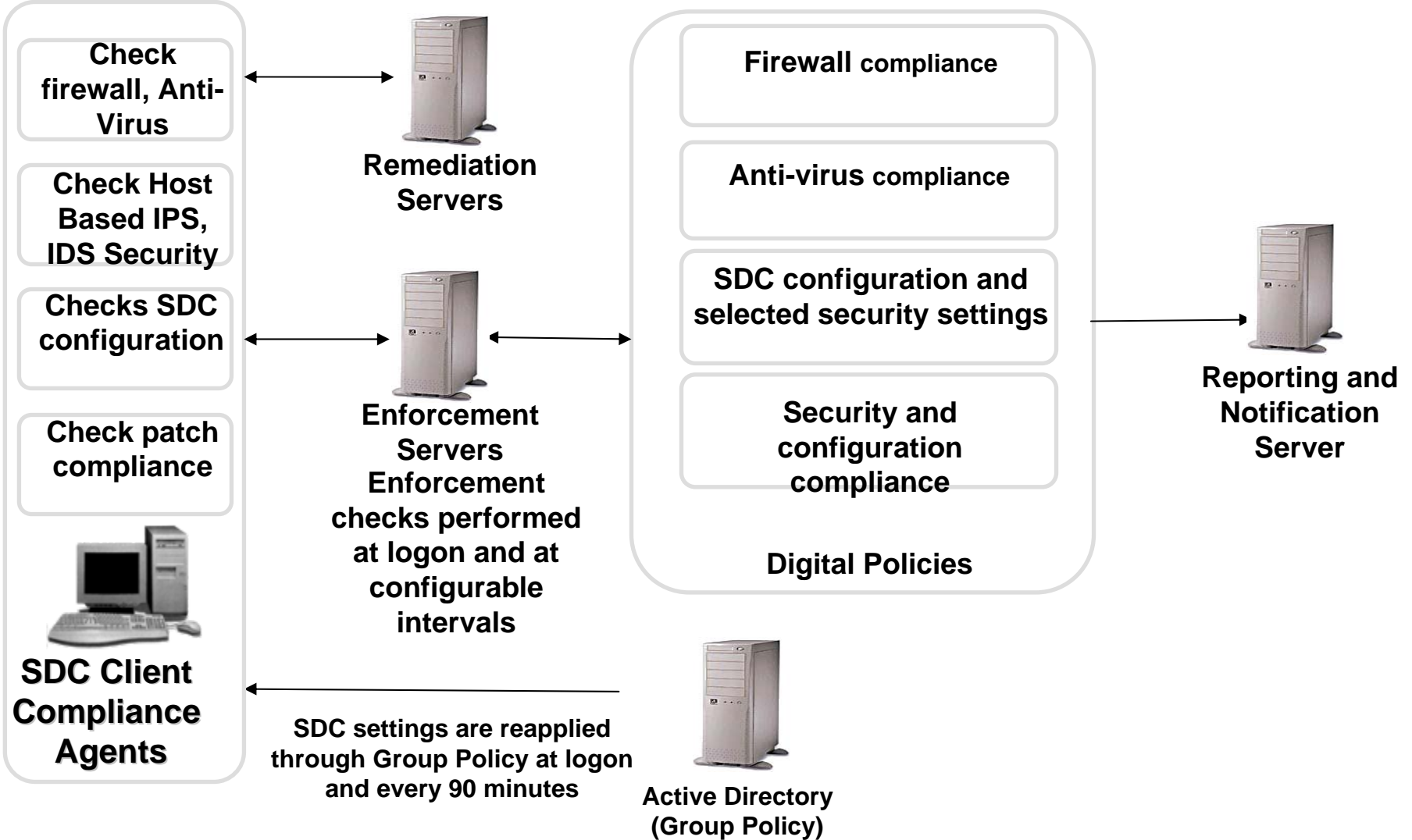|	Windows Vista Capable	Windows Vista Premium	Current USAF Buying Standard
GP	A modern processor (at least 800MHz)	1 GHz 32-bit (x86) or 64-bit (x64) processor)	Dual Core, 2.13 GHz
System Memory	512 MB of system memory	1 GB of system memory	2 GB of system memory
GPU	A graphics processor that is DirectX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

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

Integrity – Service – Excellence

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

Enforcement Servers Enforcement checks performed at logon and at configurable intervals

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

Active Directory (Group Policy)

Firewall compliance

Anti-virus compliance

SDC configuration and selected security settings

Security and configuration compliance

Digital Policies

Reporting and Notification Server

OMB: Implement and automate enforcement of these configurations

14

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**

Questions?