

*Federal CIO Council*

# Federal Desktop Core Configuration

## FDCC Technical Overview

Ms. Shelly Bird  
Microsoft Desktop Architect

*FDCC*

# Agenda

- History
- Deliverables
- Configuration Details
- Testing FDCC
- Preparing for FDCC

# *History*

## Federal Desktop Core Configuration (FDCC)

This slide represents the views of the presenter and not the Federal Government

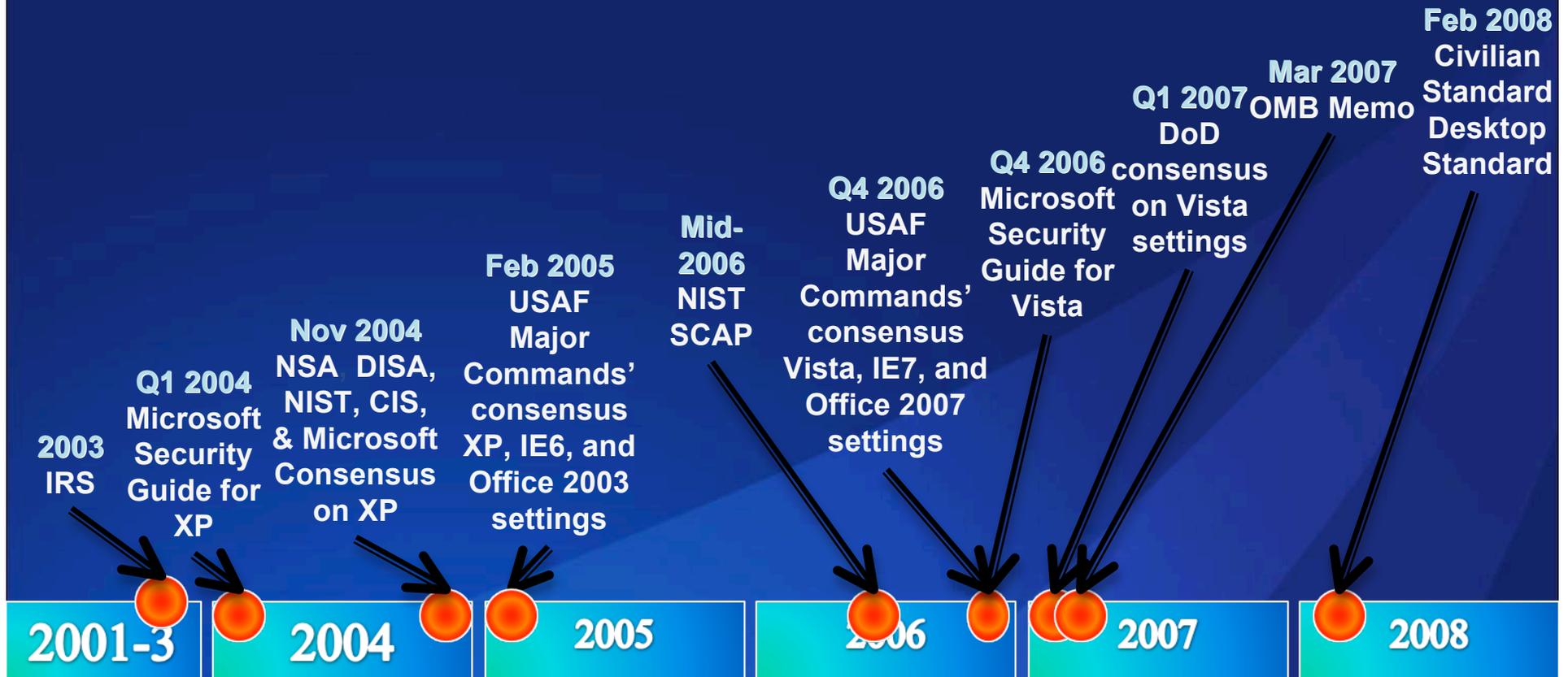


# Implementation Oriented

- **Standard Settings Review** – introduce and solidify security and configuration decisions
- **Image Build Session** – apply those decisions in an Agency standard baseline
- **Application Compatibility** – educate on tools and methods to solve issues

*Typically delivered  
in six to eight weeks*

# Steady Building of Consensus



Std Config  
Work at Civilian  
and Military  
Agencies

This slide represents the views of the presenter and not the Federal Government

FDCC

# FDCC Benefits

- Standardize security and configuration
  - Improve security
  - Cut costs
  - Simplify deployments
  - Focus audits
- Revise on a quarterly basis
- Clear target for government developers
- Drive vendor development decisions

# Hitting the Mark

- Flexible
- Responsive
- Informative
- Transparent
- Trusted authorities making decisions
- Easy deployment
- Accountable
  - Utilize NIST Security Content Automation Program (SCAP) to monitor final results

# Definitions and Terms

- **Image** – Bit Copy or File Copy format, that “wipes and loads” a partition or disk with a master configuration, including OS, Applications, settings, and default profile.
- **Configuration** – Specific settings, registry changes, file permissions, dictated in guidance and/or incorporated into scripts or Group Policies for implementation
- **Virtual PC** – Microsoft’s Virtualization software allows running a complete “virtual machine” inside your XP or Vista desktop

# How Did FDCC Evolve?

- Started out with US Air Force settings
  - Tested on 435,000 desktops
- Settings drawn from Microsoft XP and Vista Security Guides, NSA guidance for IE7
  - Represents consensus between NIST, NSA, DISA, and Microsoft
- USAF security and operations personnel decisions landed somewhere between:
  - **Enterprise Configuration (EC)** and
  - **Specialized Security – Limited Functionality (SSLF)** in the Microsoft Security Guides
- USAF included many other settings as well

# How Did FDCC Evolve?

- NIST reviewed the USAF settings, made necessary adjustments:
  - Changes to accommodate the wider scale
  - Normalized XP and Vista settings (consistency)
  - Accelerated Security Content Authentication Program (SCAP), to handle FDCC
- NSA, DISA, and USAF feedback solicited and incorporated
- Department of Homeland Security assigned to threat and patch information

# Zeroing in on the Deliverables

- **Virtual PCs** for application compatibility and development testing
  - Why not an image? *Hardware and Licensing*
- **Group Policy Objects** for enforcement and domain application of settings
- **SCAP Files** for measurement of compliance
- **Supporting Documentation**
- **For future maintenance:**
  - FDCC ISO download from Microsoft Volume Licensing Agreement (MVLA) site
  - Microsoft Security Update (MSU)

# ***Deliverables***

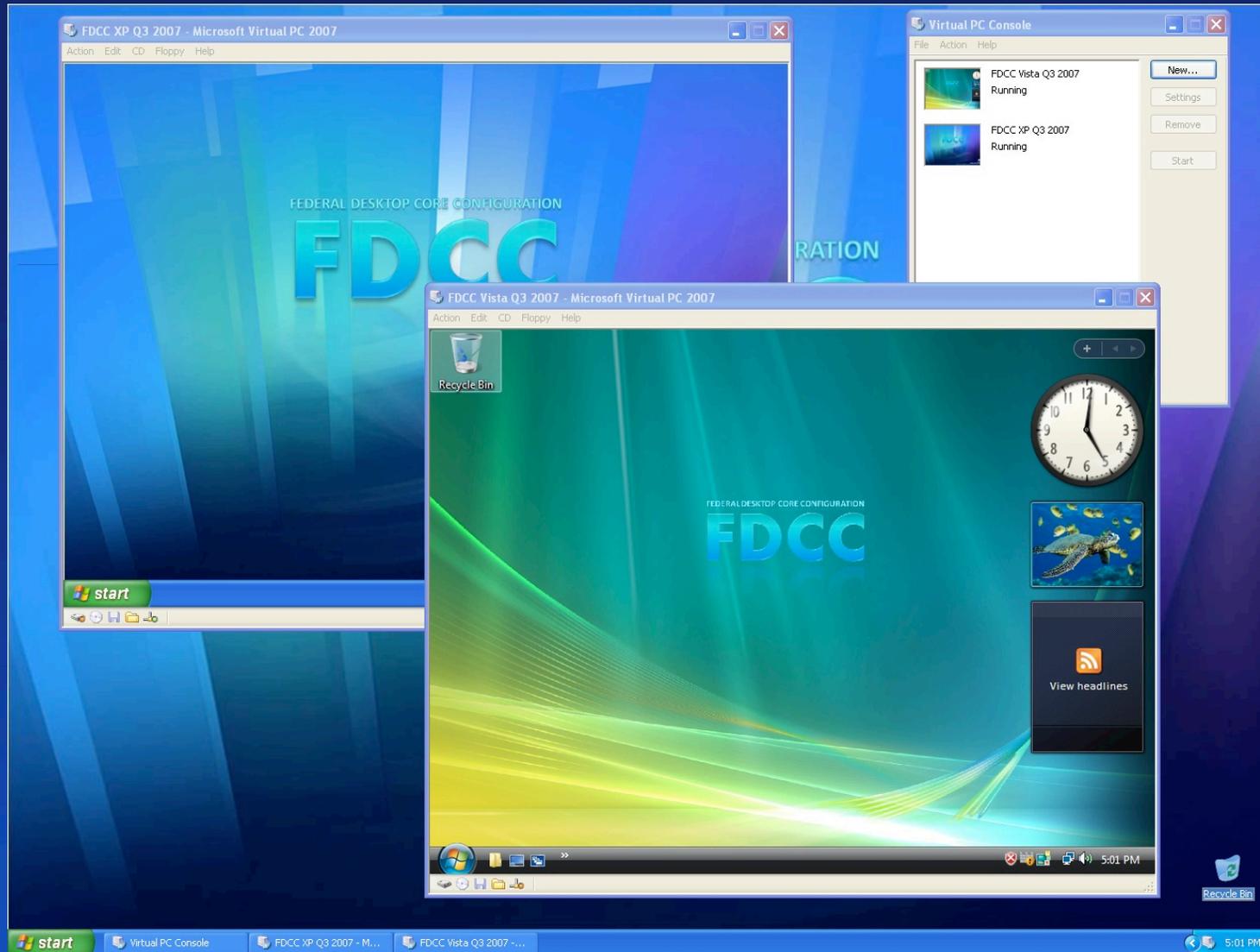
Federal Desktop Core Configuration (FDCC)

This slide represents the views of the presenter and not the Federal Government

# Deliverable: Two Virtual PC Files

- **FDCC Q3 2007 XP** = includes IE7 Settings, XP Security Settings, Additional Settings, Additional XP-Specific Settings
- **FDCC Q3 2007 Vista** = includes IE7, XP Security Settings, Additional Settings, Additional Vista-Specific Settings

# VPCs



This slide represents the views of the presenter and not the Federal Government

FDCC

# Deliverable: Group Policy Objects

- **Both** operating systems
  - FDCC Q3 2007 Account Policy
  - FDCC Q3 2007 Additional Settings
  - FDCC Q3 2007 IE7 Settings
- **Windows XP SP2**
  - FDCC Q3 2007 XP Firewall Settings
  - FDCC Q3 2007 XP Security Settings
  - FDCC Q3 2007 XP-Specific Additional Settings
- **Windows Vista**
  - FDCC Q3 2007 Vista Firewall Settings
  - FDCC Q3 2007 Vista Security Settings
  - FDCC Q3 2007 Vista-Specific Additional Settings

# Deliverable: SCAP Content

- **Windows XP SCAP content covers:**
  - FDCC Q3 2007 Account Policy
  - FDCC Q3 2007 Additional Settings
  - FDCC Q3 2007 XP Security Settings
  - FDCC Q3 2007 XP-Specific Additional Settings
- **Windows XP Firewall SCAP content**
  - FDCC Q3 2007 XP Firewall Settings
- **Windows Vista Firewall SCAP content**
  - FDCC Q3 2007 Vista Firewall Settings
- **Windows Vista SCAP content covers:**
  - FDCC Q3 2007 Account Policy
  - FDCC Q3 2007 Additional Settings
  - FDCC Q3 2007 Vista Security Settings
  - FDCC Q3 2007 Vista-Specific Additional Settings
- **IE7 SCAP content**
  - FDCC Q3 2007 IE7 Settings (use on both XP and Vista)

# Deliverable: Documentation

- **Settings:** a master database generates a spreadsheet:
  - Group Policy Path
  - Setting Name
  - Setting for XP
  - Setting for Vista
  - Group Policy File Name
  - Registry Key related to the group policy setting
  - SCAP CCE numbers for testing
- **Frequently Asked Questions**
  - Guidance on how to load VPCs and GPOs
  - Address common questions about FDCC
- **Where SCAP content gives false negatives**

# *Configuration Details*

Federal Desktop Core Configuration (FDCC)

This slide represents the views of the presenter and not the Federal Government

# Key Takeaways

- Typical user must run as **User**
  - **Not** Power User, **Not** Administrator
- Firewall (inbound) **On**
  - Local Admins **cannot** edit firewall settings
- File and Print Sharing **Off**
- IE7 Protected Mode **On** (Vista only)
- Password Length set to **12 characters**
- “Challenge” Settings
  - FIPS 140-2 turned **On**
  - Driver Signing turned **On** (XP only)

This slide represents the views of the presenter and not the Federal Government

FDCC

# What May Cause Concern

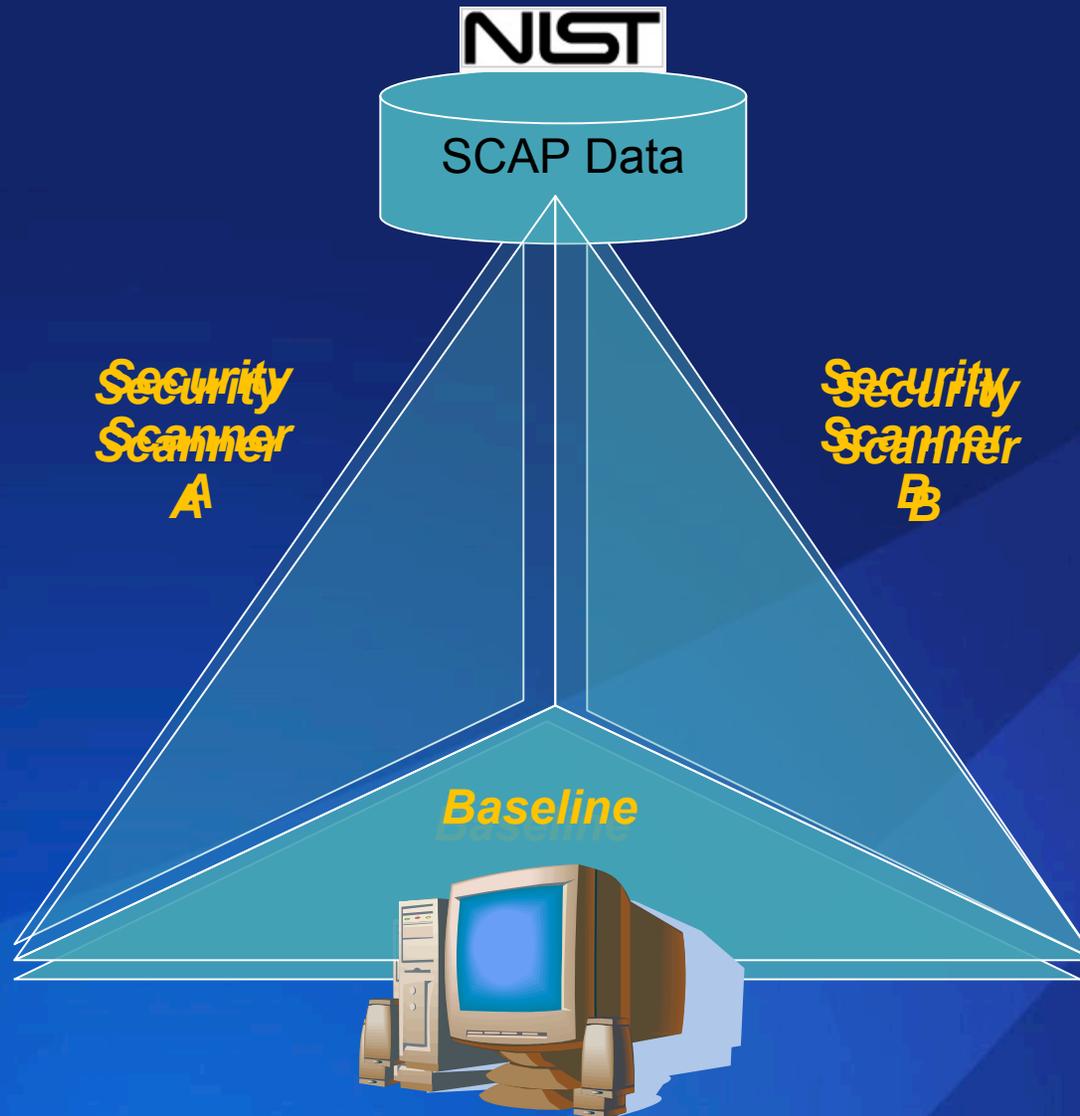
- Java in IE7 settings **Disabled**
  - But don't worry: this only applies to *Microsoft's* defunct Java (not Sun Java Runtime Environment or JRE)
- ActiveX Controls cannot be loaded by Normal Users
  - But Vista has ActiveX Install Service

# *Testing Making it Accountable*

Federal Desktop Core Configuration (FDCC)

This slide represents the views of the presenter and not the Federal Government

# Checks and Balances



This slide represents the views of the presenter and not the Federal Government

FDCC

# Manual Checks

- Discover false positive-positives and false negative-negatives
- NIST, DISA, and NSA participate
- Opportunity to review the actual decisions and reconsider if necessary

# Extending SCAP to the Field

- Final build step for Agencies: confirm the settings haven't changed
- Security auditors can use the same SCAP data to confirm compliance repeatedly
- Manufacturer independent baseline file
- Single point of reference for interpretation of the security guidance

# *Prepare for FDCC*

Federal Desktop Core Configuration (FDCC)

This slide represents the views of the presenter and not the Federal Government

# Lay the Groundwork

- Users **log on as Normal User**--therefore:
  - Management systems (examples: SMS, Tivoli, Altiris, Remote Desktop capabilities) will be critical to success
  - Must have mature help desks/remote support
  - Developers must code so software runs as User
  - Log in as User now to flag problem applications
- Capture data about hardware and software
  - SMS Queries, Tivoli queries, etc.
  - Application Compatibility Toolkit (ACT) 5.0
  - Windows Vista Hardware Assessment (WVHA)
- Gather information on firewall exceptions

# Step One: Test and Certify

## 1. Build To/Test to/Certify that Agency Applications will run on the FDCC

- FDCC draws a starting line in the sand with:
  - Virtual PCs pre-configured with FDCC settings
  - Group Policy Objects (GPOs)
  - Guidance Documents
  - Validation Tools: SCAP
- Agencies will do early Application Compatibility testing using the **Test Evaluation Virtual PCs**

# Step Two: Agency Standard Image

## 2. FDCC Configuration will form the foundation for an Agency Image

- Microsoft Volume Licensing Site: FDCC ISO
- Base Agency custom image on that ISO
- Testing yields a reasonable Agency standard
- Variations from FDCC noted and plans put in place to remediate in the long term
- OMB can work on improving applications
- Written in the FAR to meet FDCC

# Step Three: Update

## 3. Stay Current with FDCC Standard

- Options may include
  - Windows Update utilizing Windows Software Update Server (WSUS )
  - Systems Management Server (SMS) and other deployment tools chosen by each agency

# Ongoing FDCC Tasks

- Governance board for final decisions
- Program Office that will host quarterly builds (a Center of Excellence)
- FDCC ISO for download from MVLS
- FDCC Microsoft Security Update (MSU)
- Office 2007 GPOs, SCAP
- (TBD 2.0) Data at Rest: software must run well with encrypted user data
  - Pointing to EFS Assistant
  - Requires enterprise recovery methods (AD)
  - Volume level encryption (BitLocker) and FIPS

# FDCC Feedback Channels

- NIST FDCC web site:  
<http://csrc.nist.gov/fdcc>
- Microsoft blog:  
<http://blogs.technet.com/fdcc/>
- Send e-mail to [fdcc@nist.gov](mailto:fdcc@nist.gov)
- FDCC Education/Status LiveMeetings will be run on a bi-weekly basis