

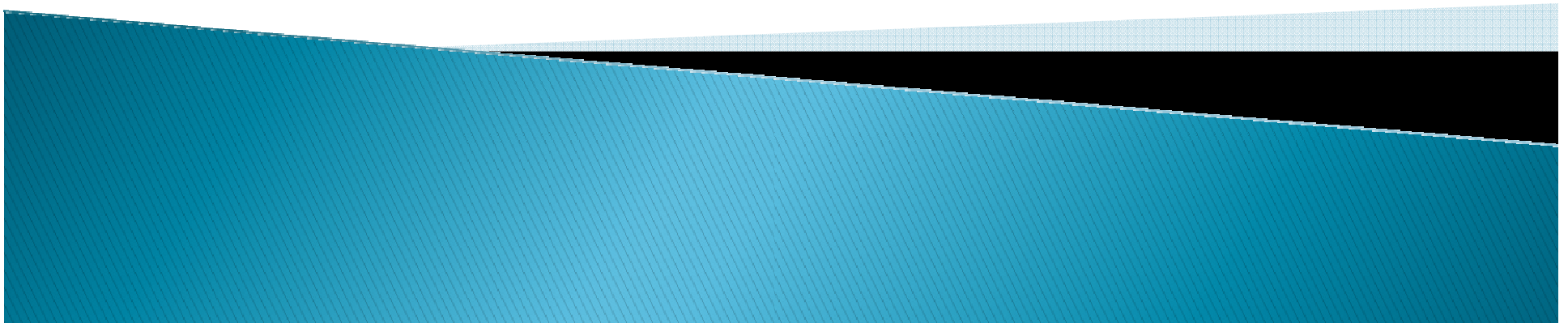
# FDCC Challenge Settings & Implementation

FDCC Implementers Workshop

David L. Dixon

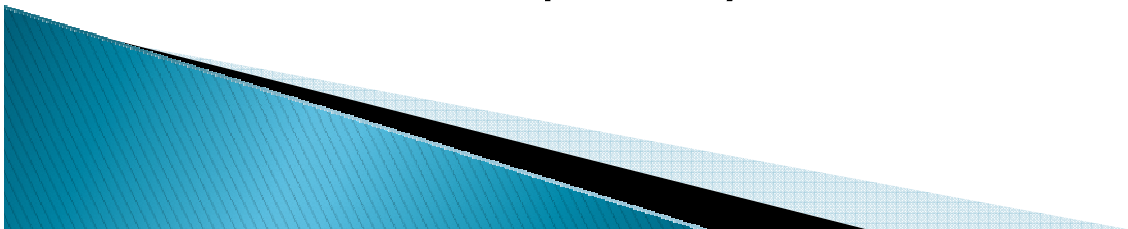
Sr. Consultant, Microsoft Federal Services

FDCC Team



# Agenda

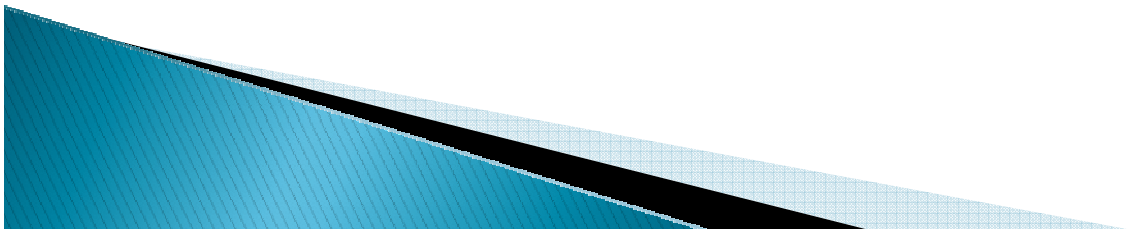
- ▶ **FDCC Challenges**
  - FIPS Setting
  - Mobile Users
  - ActiveX Controls
  - Firewall
  - Miscellaneous
    - File system ACLs
    - Certificate errors (IE)
    - Unsigned Drivers
    - Imaging Build “Gotchas”
- ▶ **Implementing FDCC Settings**
  - Group Policy Objects (GPOs)
  - Local Group Policy



# FDCC Challenges

(1 of 7)

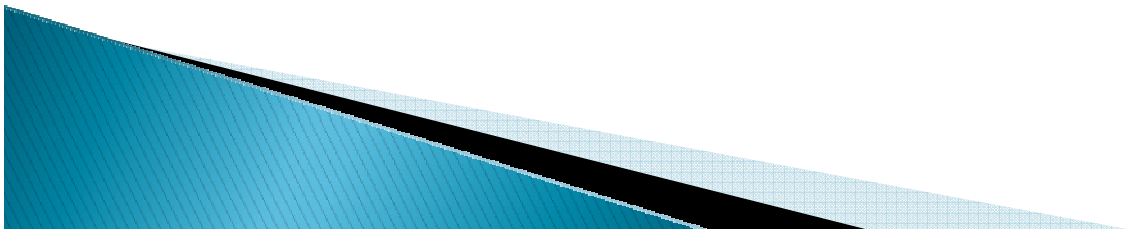
- ▶ FIPS (Federal Information Processing Standard)
  - Setting → *Computer Configuration / Security Settings / Local Policies / Security Options / System cryptography: Use FIPS compliant algorithms for encryption, hashing and signing*
  - Has ramifications for:
    - Accessing SSL web sites
      - SSL 3.0 protocol (uses MD5 algorithm; not supported by FIPS)
    - Terminal services (RDP)
      - By default, RDP not FIPS compliant (56-bit RC4)
      - RDP to XP not possible when FIPS enabled
    - BitLocker Drive Encryption (BDE)
      - Recovery passwords can't be stored anywhere, including AD
      - This is true for other encryption solutions that use recovery passwords, not just BDE
    - Encrypted File System (EFS)
      - Enabling FIPS after EFS will only encrypts with FIPS going forward
    - Others (ADFS, WSUS and ASP.NET and ClickOnce apps and any third party encryption software that is not FIPS compliant)



# FDCC Challenges

2 of 7

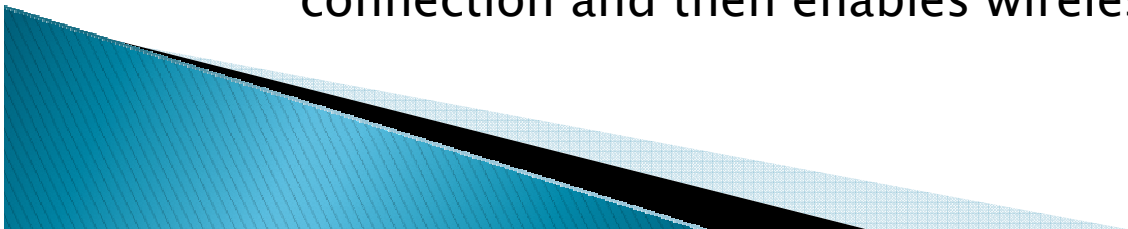
- ▶ FIPS (Federal Information Processing Standard)
- ▶ **What You Can Do**
  - **Accessing SSL web sites**
    - Internal: reconfigure to support FIPS (TLS 1.0)
    - External: report sites to NIST/OMB
  - **Terminal Services (RDP)**
    - Enable FIPS on Terminal Server
    - Upgrade to RDP 5.2 or higher on client
    - W2K3, Vista and W2K8 natively support client or server with FIPS enabled
    - **XP as TS server with FIPS enabled not possible**
  - **BitLocker Drive Encryption (BDE)**
    - Must use randomly generated keys, **not recovery passwords**
      - No FIPS approved way to derive keys from a password
    - Must use USB for key storage
  - **EFS**
    - Decrypt and re-encrypt data to ensure FIPS ciphersuites are used for all data
  - **ADFS** – download hotfix (KB 935449)
  - **WSUS** – need WSUS 3.0
  - **ASP.NET 1.1 to 2.0** (KB 911722)
  - **ClickOnce/VS 2005** – rewrite in VS 2008
  - **Third party encryption software**
    - Only an issue if software has components that use Crypto API
    - Check with vendor to identify/resolve FIPS issues



# FDCC Challenges

3 of 7

- ▶ Mobile User Scenarios
  - Traveling users (includes many execs)
  - Need remote access back to HQ (VPN)
  - Need wireless capabilities while on road
  - FDCC recommends disabling three key services
    - Remote Access Connection Manager (RACM)
    - Wireless Zero Configuration (XP)
    - WLAN AutoConfig (Vista)
    - Limited to 2 cached logons
      - Could be issue for shared laptop users when disconnected
- ▶ **What you can do**
  - Use third-party wireless clients/apps
  - ID subset of mobile users
    - Create OU and apply policy that allows these services
    - Develop solution that “intelligently” detects absence of wired connection and then enables wireless



# FDCC Challenges

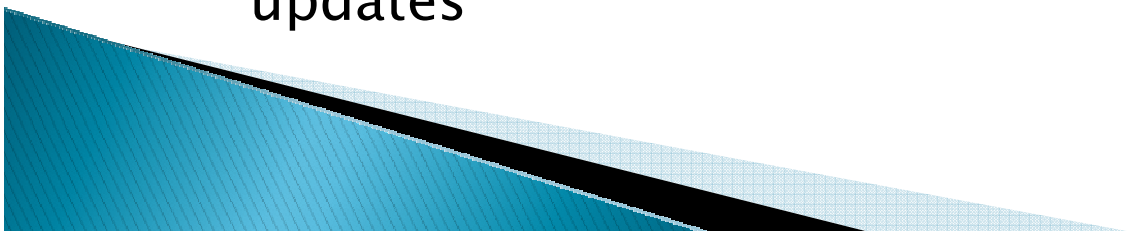
4 of 7

## ▶ ActiveX Controls

- FDCC restricts download of (signed and unsigned) ActiveX controls in Internet and Restricted Sites Zones
- FDCC recommends blocking install of ActiveX controls by IE Processes (XP only)– could impact Windows Update

## ▶ What You Can Do

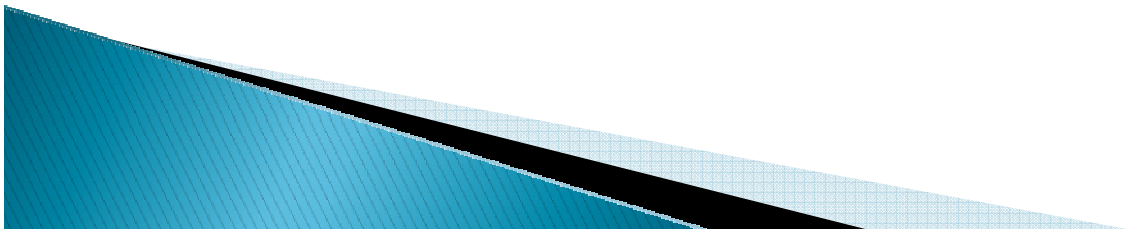
- XP: “Package” ActiveX controls for deployment via Group Policy or standard software distribution mechanisms (.msi)
- Vista: Use ActiveX Installer Service (Axis)
  - Allows users to install ActiveX controls from sites that are approved by Group Policy
- Use WSUS or SUS in lieu of Windows Update to deploy updates



# FDCC Challenges

5 of 7

- ▶ Windows Firewall
  - FDCC mandates blocking of
    - File and print sharing
      - Includes admin shares (i.e. c\$)
    - Central management required
      - Local admins can't add exceptions
  - **What You Can Do**
    - Find alternative to admin shares for administration of desktops
      - Remote desktop and admin exemptions are allowed by FDCC
        - RDP, MMC, WMI, etc and associated ports allowed
    - Allow Admin to configure a role-specific exception for admin shares in policy
      - Use Security Groups and apply Admin permissions to GPO that loosen this for admins across OUs



# FDCC Challenges

6 of 7

## ▶ Miscellaneous

### ◦ File system ACLs:

- Users don't have permissions to run:
- Net.exe – Will impact orgs that use logon scripts
- Regedit and regedt32.exe – reviewing (and modifying registry)
- Mshta.exe – impacts opening .hta files (some help files)

### ◦ What You Can Do

- Net.exe
  - Consider Vbscript as an alternative
  - Group Policy scripts
- Justify exceptions when there is clear impact on supportability and productivity

### ◦ Certificate Errors

- Setting: *Computer Configuration|Administrative Templates|Windows Components|Internet Explorer|Internet Control Panel|Prevent ignoring certificate errors*
- If certs has expired, are revoked, have name mismatches, will not allow access to web site

### ◦ What You Can Do

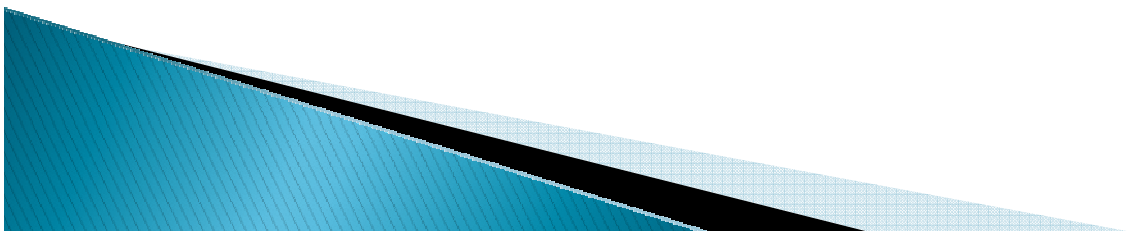
- Resolve certificate issues prior to FDCC deployment

### ◦ Unsigned Drivers (XP)

- FDCC recommends all device drivers be signed
- Many XP drivers are not signed
- Little chance of getting drivers signed now

### ◦ What You Can Do

- Use “warn but allow installation” for admins on XP
  - Will block silent install or updates of drivers
- Report drivers that are common and unsigned that manufacturers need to run through WHQL
- Vista
  - Most device drivers are signed
  - Allows users to install drivers in the Trusted Driver Store
  - Driver signing not limited to vendor; administrators can sign drivers as well

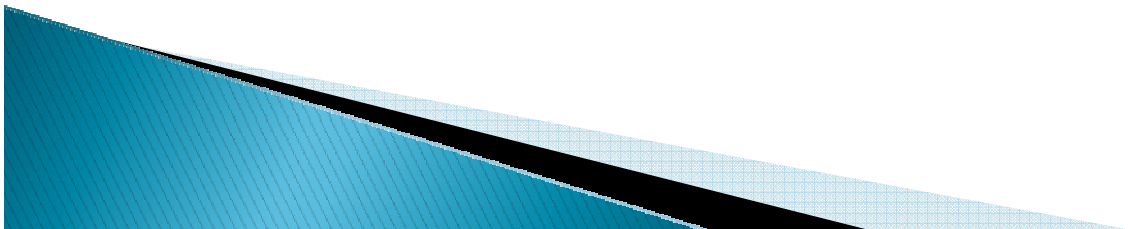




# FDCC Challenges

7 of 7

- ▶ **Miscellaneous** (cont)
  - **Image build “Gotchas”**
    - Certain FDCC settings could impact imaging process:
      - MSS: Enable Automatic Logon disabled
      - Do not process the run once list
      - Interactive Logon: Message text
      - Interactive Logon: Message title
  - **What You Can Do**
    - Delay applying these settings until after imaging process is completed
    - Can be implemented via regedit (or similar command)



# Implementing FDCC

- ▶ Two primary methods
  - Active Directory Group Policy Objects (GPOs)
  - Local Group Policy
- ▶ GPOs
  - Reinforce policy while in domain
  - Easy to deploy and manage centrally
  - FDCC settings contained in 9 GPOs
    - 3 common (Account Policy, IE7 and Additional Settings)
    - 3 for both XP and Vista (Security, Specific Additional and Firewall)
- ▶ Local Policy
  - Enforce FDCC policy for disconnected, mobile users
    - Standalone computers
    - Removed from domain
  - More than just security settings (.inf) file
    - Microsoft has LGPO tool to apply FDCC policy
    - Third party solutions

