

# Current and Future Issues in Security

Rick Therrien  
TAG-SS Co-chair (Incumbent)

Cybersecurity Operations  
Internal Revenue Service

July 10, 2008



# Infrastructure Security Goals

- Research emerging trends and requirements from the federal government
  - NIST
  - Industry
  - IRS Lessons Learned
- Assess applicability to IRS
- Integrate new trends into IRS infrastructure
  - IRS
  - Contractors
  - State, federal and local agencies (working with Safeguards)

# Integration Efforts

- Work with multiple stakeholders to ensure successful integration of new requirements
  - Participate in Treasury committees
  - Partner with National Institute of Standards & Technology
  - Participate in Federation of Tax Administrators (FTA) Tactical Advisory Group (TAG)
  - Co-Chair TAG Security Subcommittee (TAG SS)

# Brings Stakeholders Into Security Integration

2005



2008



To This...

From This....

# Technology Workstreams Affecting IRS

- Internal Secure Data Transfer
- Federal Desktop Core Configuration
- Security Content Automation Protocol
- The National Vulnerability Database
- Advances in Network Admission Control

# Internal Secure Data Transfer

- Yes, the IRS is working it internally as well... but differently than externally
- FTP and TFTP are open protocols
- Authentication credentials and data are passed in the clear with FTP
- Transmission of data often goes untracked
- Use in IRS identified in GAO audits
- Secure protocols are mature
- Product market exists with FIPS-140-2 certified crypto

# Internal Secure Data Transfer (Cont)

- Solution: Deploy secure protocols with comprehensive, repeatable tracking information
- Secure Shell (SSH) will substitute for FTP, TFTP, and other insecure protocols for IRS sensitive data transfers while also protecting authentication credentials
- Enterprise File Transfer Utility (EFTU), internally developed, will handle file tracking mechanisms (bulk batch mode data transfers)
  - Supports Wintel, Unix, IBM, and Unisys mainframes

# Internal Secure Data Transfer (Cont)

- Quick SSH Wiki:
  - Network protocol that allows data to be exchanged over a secure channel between two computers
  - Encryption provides confidentiality and integrity of data.
  - Uses public-key cryptography to authenticate the remote computer and allow the remote computer to authenticate the user, if necessary
  - Is typically used to log into a remote machine and execute commands, but it also supports tunneling, forwarding arbitrary TCP ports and X11 connections; *it can transfer files using the associated SFTP or SCP* protocols
  - Listens on the standard TCP port 22

# Internal Secure Data Transfer (Cont)

- SSH has many uses:
  - Remote administration of the SSH server computer via terminal (character-mode) console
  - Secure alternative to FTP
  - In combination with rsync to backup, copy and mirror files efficiently and securely
  - In combination with SCP, as a secure alternative for rcp file transfers

# Internal Secure Data Transfer (Cont)

- Port forwarding or tunneling,
  - a (non-secure) TCP/IP connection of an external application is redirected to the SSH program
  - SSH forwards the transmission it to the other SSH party
  - Forwarded connection is encrypted and protected on the path between the SSH client and server only.
  - Good for securing X11, rdesktop, Windows Terminal Services and VNC connections or even forwarding Windows file shares.
- Securely mounting a directory on the server as a file system on the local computer as a full-fledged VPN

# Federal Desktop Core Configuration

- What's FDCC?
- An OMB-mandated security configuration
- Currently exists for Microsoft Windows Vista and XP
- FDCC was originally called for in a 22 March 2007 memorandum from OMB to all Federal agencies and department heads and a corresponding memorandum from OMB to all Federal agency and department Chief Information Officers (CIO).

# Federal Desktop Core Configuration (Cont)

- Vista FDCC:
  - Based on DoD customization of the Microsoft Security Guides for both Windows Vista and Internet Explorer 7.0
  - Microsoft's Vista Security Guide was produced through a collaborative effort with DISA, NSA, and NIST.
  - Reflects the consensus on recommended settings from DISA, NSA, and NIST for the Windows Vista platform.
- Windows XP FDCC:
  - Based on Air Force customization of the Specialized Security-Limited Functionality (SSLF) recommendations in NIST SP 800-68 and DoD customization of the recommendations
- Image is available to COTS software developers
- One locked-down COE for all Federal Agencies

# Federal Desktop Core Configuration (Cont)

- Computers that are owned or operated by a contractor on behalf of or for the IRS or are integrated into a Federal system are subject to FDCC
- Password policy applies to both local and domain accounts
- Domain configurations that manifest themselves in local FDCC settings
  - E.g., password length managed at the domain level manifests itself at each desktop and laptop
  - Therefore, password length, whether managed via domain or locally, is subject to FDCC
- All wireless interfaces should be disabled
- Internet Explorer 7.0 is a built-in component of the Windows XP and Vista operating systems. For this reason, it needs to be installed and configured according to FDCC settings for all Windows XP and Vista computers.
- Privilege escalation is prohibited e.g., “Power User”
- 12-Character minimum password length
  - Use pass-phrases instead of passwords
  - E.g., Mary had @ 1!ttle Lamb

# Federal Desktop Core Configuration (Cont)

- But we're special...
- OMB policy recognizes that agencies may determine that settings in the FDCC are not practical
- OMB instructed agencies to provide documentation to NIST of any deviations from the FDCC and the rationale for doing so
- Report FDCC compliance through your organization's CIO hierarchy.
- Agency or department CIO must report compliance for that organization.
- Compliance is expressed in a roll-up numbers of compliant versus non-compliant computers
- For non-compliant computers, CIOs must provide a representative sample of SCAP-based (XCCDF version 1.1.4) assessment reports.
- This information should be sent by March 31, 2008
- NIST will perform trend analysis on all Federal data and present findings to OMB
- Takeaway: No Deviations!

# Security Content Automation Protocol

- What's SCAP?
- NIST recently established a suite of interoperable and automatable security standards known as the Security Content Automation Protocol (SCAP).
- Uses XML-based standards, SCAP is simultaneously machine and human readable

# SCAP Goals

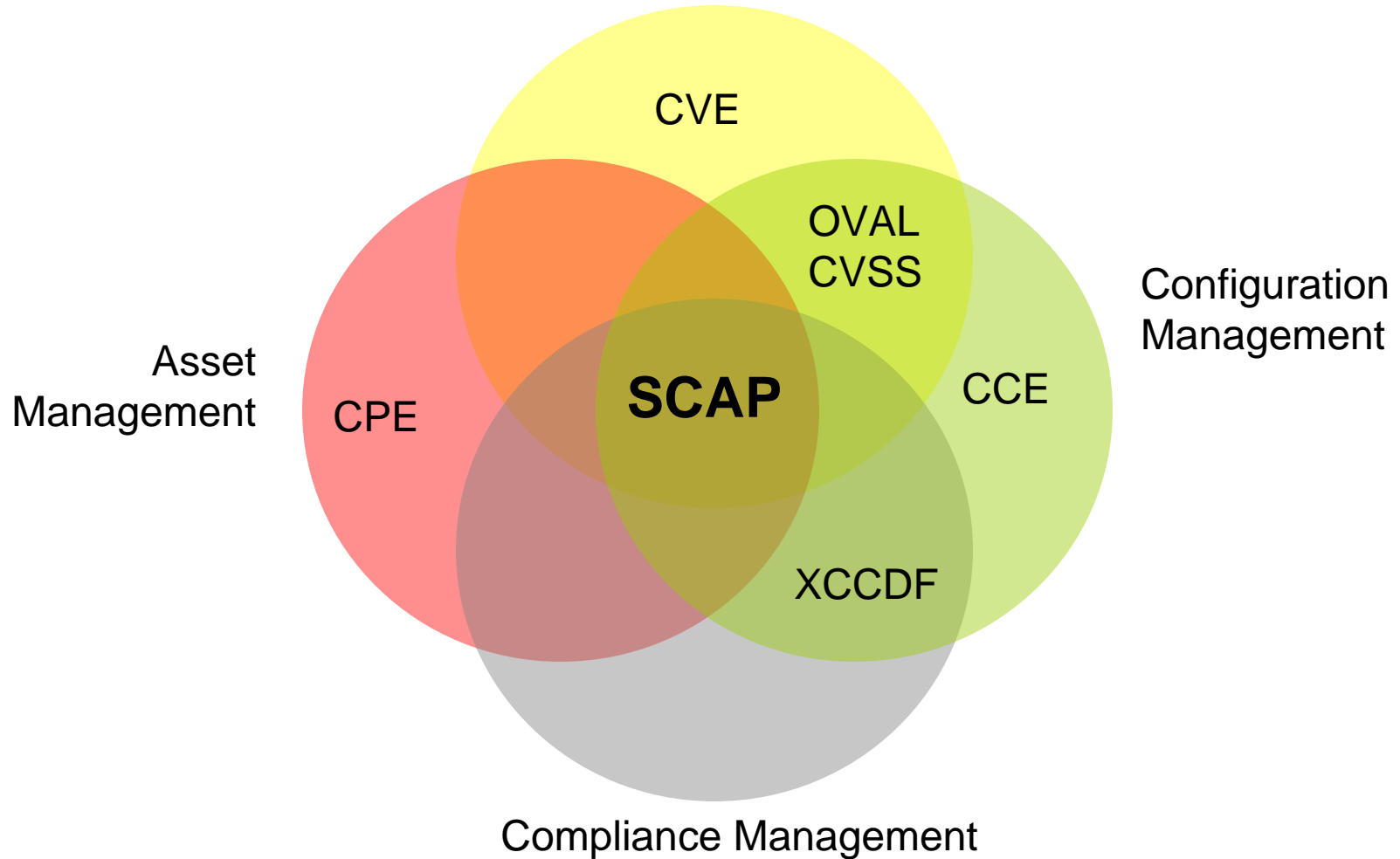
- Enable standardized and automated vulnerability management, measurement, and policy compliance evaluation (e.g., FISMA and DoD 8500.2/8510 compliance)
- Enumeration of vulnerabilities, misconfigurations, platforms, and impact
- Enable the creation of machine readable security configuration checklists
- IRMs in the process of aligning to SCAP

# SCAP Protocol Suite

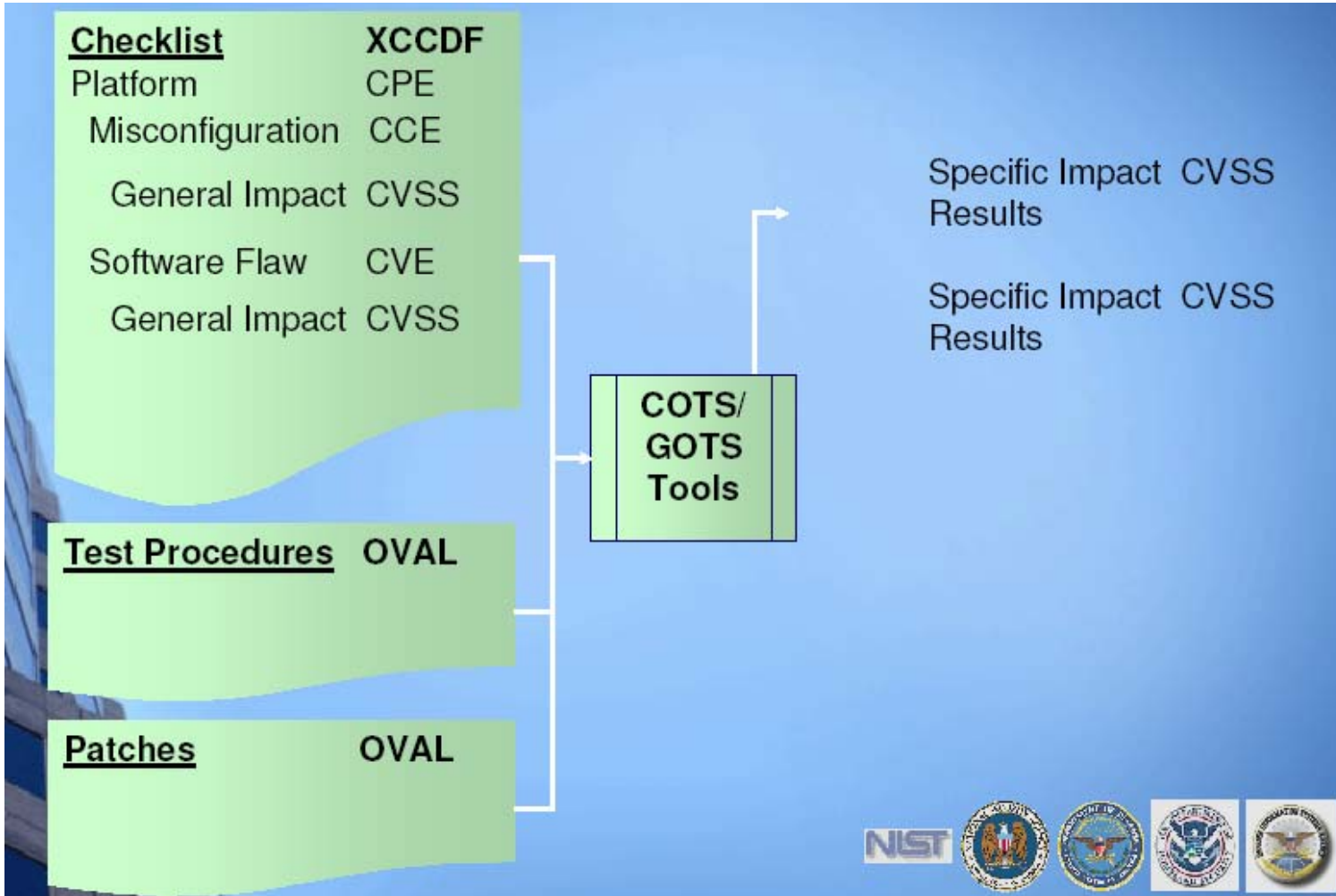
- Extensible Configuration Checklist Description Format (XCCDF):
  - Standard XML for specifying checklists and for reporting results of checklist evaluation.
- Open Vulnerability and Assessment Language (OVAL):
  - Standard XML for test procedures
- Common Vulnerabilities and Exposures (CVE):
  - Standard nomenclature and dictionary of security related software flaws
  - The goal of CVE is to make it easier to share data across separate vulnerability capabilities (tools, repositories, and services)
- Common Configuration Enumeration (CCE):
  - Standard nomenclature and dictionary of software mis-configurations
  - CCE Identifiers can be used to cross-correlate the configuration statements in configuration best-practice documents from the Center for Internet Security (CIS), National Institute of Standards and Technology (NIST), National Security Agency (NSA), and Defense Information Systems Agency (DISA).
- Common Platform Enumeration (CPE):
  - Standard nomenclature and dictionary for product naming
- Common Vulnerability Scoring System (CVSS):
  - Standard for measuring the impact of vulnerabilities

# SCAP Protocol Framework

Software Flaw Management



# How does SCAP work?



Source: SCAP  
Nuts-n Bolts;  
<http://nvd.nist.gov>



# SCAP Value and Benefits

## SCAP Value

Feature	Benefit
Standardizes <i>how</i> computers communicate vulnerability information – the protocol	Enables interoperability for products and services of various manufacture
Standardizes <i>what</i> vulnerability information computers communicate – the content	Enables repeatability across products and services of various manufacture Reduces content-based variance in operational decisions and actions
Based on open standards	Harnesses the collective brain power of the masses for creation and evolution Created and evolved with the broadest perspective
Utilizes configuration and asset management standards	Mobilizes asset inventory and configuration information for use in vulnerability and compliance management
Applicable to Federal Risk Management Framework – Assess, Monitor, Implement	Reduces time, effort, and expense of risk management process
Traceable to security mandates and guidelines	Automates portions of compliance demonstration and reporting
Keyed on NIST SP 800-53 security controls	Automates portions of FISMA compliance demonstration and reporting

Source: FDCC'  
Secure Content  
Automation Protocol;  
August 2007

# Some FDCC XP Policies in SCAP Form

```
<refine-value idref="password_history_enforcement_var" selector="24_passwords" />
<refine-value idref="maximum_password_age_var" selector="5184000_seconds" />
<refine-value idref="minimum_password_age_var" selector="86400_seconds" />
<refine-value idref="minimum_password_length_var" selector="12_characters" />
<refine-value idref="password_complexity_var" selector="enabled" />
<refine-value idref="PasswordStorageReversibleEncryption_var" selector="disabled" />
<refine-value idref="maximum_application_log_size_var" selector="16777216_bytes" />
<refine-value idref="maximum_security_log_size_var" selector="83886080_bytes" />
<refine-value idref="maximum_system_log_size_var" selector="16777216_bytes" />
<refine-value idref="prevent_guest_application_log_access_var" selector="enabled" />
<refine-value idref="prevent_guest_security_log_access_var" selector="enabled" />
<refine-value idref="prevent_guest_system_log_access_var" selector="enabled" />
<refine-value idref="retention_application_log_var" selector="overwrite_as_needed" />
<refine-value idref="retention_security_log_var" selector="overwrite_as_needed" />
<refine-value idref="retention_system_log_var" selector="overwrite_as_needed" />
```

# SCAP Report Example – Database Vulnerability Report

Vulnerabilities by Risk Level



High Risk

Medium Risk

Low Risk

Informational

## Agent jobs privilege escalation

**Description:** Permissions to escalate privileges through the SQL Agent have not been removed

**Versions:** Microsoft SQL Server 7.0 and 2000

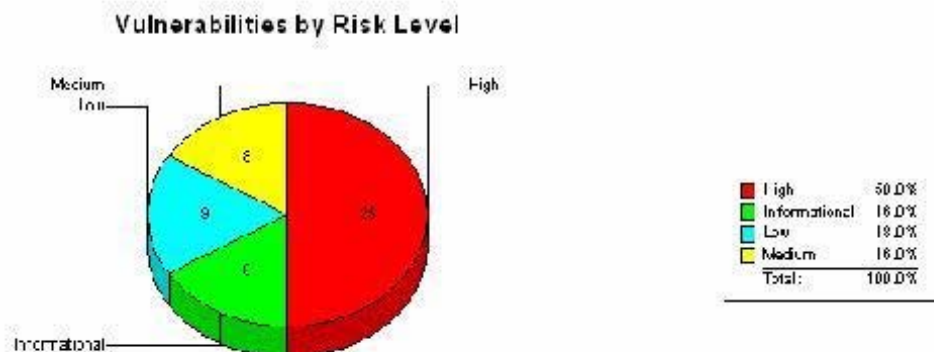
**CVE:** CVE-2002-0721 **CCE:** CCE-NO-MATCH **CPE:** cpe://Microsoft/sql\_server/2000

**References:** <http://www.microsoft.com/technet/security/bulletin/MS02-043.asp>  
<http://online.securityfocus.com/bid/5483>

**Summary:** A security issue exists that allows privilege escalation to be done through the Agent service. By default, the public group is allowed to create jobs that the Agent runs. By crafting a malicious job using extended stored procedures

Source:  
[www.appsecinc.com](http://www.appsecinc.com)

# SCAP Report Example – Database Vulnerability Report



⊗ High Risk    ⚠ Medium Risk    ? Low Risk    ⓘ Informational

## ⊗ Agent jobs privilege escalation

**Description:** Permissions to escalate privileges through the SQL Agent have not been removed

**Versions:** Microsoft SQL Server 7.0 and 2000

**CVE:** CVE-2002-0721    **CCE:** CCE-NO-MATCH    **CPE:** cpe://Microsoft:sql\_server:2000

**References:** <http://www.microsoft.com/technet/security/bulletin/MS02-043.asp>  
<http://online.securityfocus.com/bid/5483>

**Summary:** A security issue exists that allows privilege escalation to be done through the Agent service. By default, the public group is allowed to create jobs that the Agent runs. By crafting a malicious job using extended stored procedures

Source:  
[www.appsecinc.com](http://www.appsecinc.com)

# The National Vulnerability Database

- FDCC, SCAP and its protocols... it doesn't end with Windows
- There are currently 160 checklists; hardening guides covering servers, routers, RDBMS, flavors of UNIX and Linux, etc.
- All are being converted to SCAP versions
- Beta SCAP checklists include Office 2007, Red Hat, Solaris 10, Symantec A/V

# The NVD (cont.)

- The NVD ‘connects the dots’ from NIST policies, to implementation, to compliance with security controls and patches (eventually) for all IT system components automating the process of implementing secure systems and keeping those systems continuously secure
- “NVD is the U.S. government repository of standards based vulnerability management data represented using the [Security Content Automation Protocol](#) (SCAP). This data enables automation of vulnerability management, security measurement, and compliance.”

# The NVD (cont.)

- Some NVD statistics
  - 30,778 vulnerabilities tracked
  - 160 checklists
  - 141 US-CERT alerts
  - 2,192 US-CERT Vulnerability notes
- Bottom line: NVD represents the future-state of IRS systems monitoring and compliance
  - IRS needs to align security infrastructure investments and programs with the NVD
  - We're just scratching the surface!

# Advances In Network Admission Control (NAC)

- What is NAC?
- NAC is a suite of technologies previously implemented separately as point-based solutions
  - Anti-virus client
  - Personal Firewall
  - End-point HID
  - 802.1x
  - RADIUS
  - Authentication protocols (EAP, LEAP, PEAP, EAP-FAST)
  - Strong Authentication
    - PKI certificates, symmetric keys, OTPs
- NAC's goal is to provide a highly scalable solution that better integrates these technologies

# Advances in NAC (Cont)

- NAC in a nutshell:
- Without NAC - Network jacks and access points are protected only by little to no physical security
  - You see a jack, you plug in, you get an IP address, you're in!
- Authenticates people and devices to the network itself (Ethernet and TCP/IP)
  - (AD authenticates people and computers to a Windows forest only, not to the underlying LAN infrastructure)
- Challenges users and computers for credentials (strong ones, if you want)
- Inspects devices to see if they have good security protection products and checks to see if devices are patched
- Provides user and device remediation handling
  - Devices are sent to a DMZ for patches, signature updates, etc.
- Allows for segregation of devices and subsequent limitations on application access based on the security posture of the device, and even the user

# Advances in NAC (Cont)

- NAC is not a mature solution despite being built on mature technologies (because the underlying technologies are problematic)
- 802.1x is not scalable
  - Ok for a few LANS, very cumbersome for 100's of LANs
- Looks a lot like WPA-2, because it is
  - Potential for duplicative efforts and overlapping solutions with wired and wireless protection
- RADIUS being moved up to Integral General Purpose authenticator status
  - Not just for remote access anymore

# Advances in NAC (Cont)

- Authentication solutions are stove-piped according to dedicated technologies
  - PKI is easier said than done
  - Symmetric key management infrastructure is cumbersome
  - OTPs and other authenticators typically application-specific, not enterprise
  - And then there's smartcards...
- Active Directory is still a key player; NAC - AD integration leaves something to be desired
- Management tools are device configuration management tools at best
  - Security posture monitoring and compliance “manager of managers” needed
- A/V, HID, Personal Firewall... all stove-pipes

# Advances in NAC (Cont)

- IPv6 with its many new security enhancements, only muddies the waters right now
- What you can accomplish for a laptop, you can't for a printer, network scanner, or other less programmable device
- Solution vendors have very different approaches and very different understandings of the domain
  - Mixed bag of expectations, solutions
- Confederated shops now have to work even more closely together (across and down into):
  - Active Directory
  - Symantec
  - Cisco
- NAC still has growing pains, but finally companies have recognized the need to better integrate these technologies into a highly scalable and effective solution

# Advances in NAC (Cont)

- Despite to bleak picture, NAC has some operational success and is building a strong foundation of deployments
- Scale is now in 1,000's of endpoints per customer/owner
- Time has come for IRS to begin adoption of NAC technologies

# Links and References

- FDCC
- <http://nvd.nist.gov/fdcc/index.cfm>
- SCAP
- <http://nvd.nist.gov/scap.cfm>
- National Vulnerability Database
- <http://nvd.nist.gov/home.cfm>
- National Checklist Program
- <http://checklists.nist.gov>

# Questions ???

Rick Therrien

Senior IT Security Advisor

Internal Revenue Service

202-283-2848

Richard.Therrien@irs.gov

