QUEST SOFTWARE®

Smart Systems Management

# Feeling Cyber "Insecure"?

# Showing Progress Towards the Consensus Audit Guidelines

# Overview

- Paul Garver, Vice President, Quest Public Sector

# Cyberattacks Are Real

*"In 2008, the Office of the Inspector General (OIG) says, hackers took over FAA Servers in Alaska, discovered the password of an administrator in Oklahoma and got access to 40,000 FAA user names and passwords."*

CIO Magazine
July 1, 2009

*"In April 2009, government officials confirmed that since 2007, hackers have been slipping into computer systems behind the Joint Strike Fighter weapons project. They gained access through defense contractors on the project."*

CIO Magazine
July 1, 2009

*"In February 2009, an FAA web site was hacked, exposing data on 48,000 current and former employees, according to a recent study by the OIG."*

CIO Magazine
July 1, 2009

# The Reality

*"You can be FISMA compliant and still not be secure."*

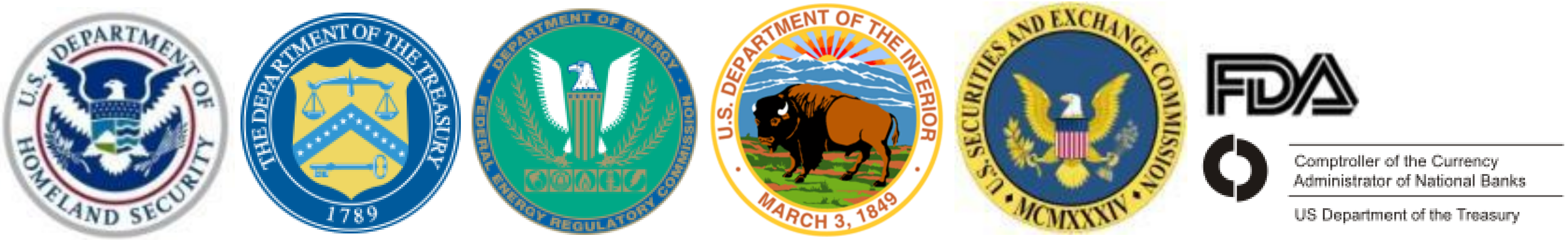
*“Next month the Office of Management and Budget will announce new performance metrics for FISMA, so that agencies can move from static, compliance-based security to risk management based on real-time monitoring and analysis.”*

- **FCW March 2, 2010**

*Interview with Howard Schmidt, White House Cybersecurity Coordinator*

# It’s Our Job to Act

- At least 34 federal regulations apply to organizations that touch critical IT infrastructure in the U.S.
- This is a collection of rules that no one person, agency or department oversees and includes mandates from:


U.S. DEPARTMENT OF HOMELAND SECURITY
THE DEPARTMENT OF THE TREASURY 1789
DEPARTMENT OF ENERGY FEDERAL ENERGY REGULATORY COMMISSION
U.S. DEPARTMENT OF THE INTERIOR MARCH 3, 1849
U.S. SECURITIES AND EXCHANGE COMMISSION MCMXXXIV
FDA
Comptroller of the Currency
Administrator of National Banks
US Department of the Treasury

- Fragmentation like this means uniformly measured and monitored security standards across industries don’t exist.

> *“The current approach of trying to do everything, everywhere, results in accomplishing little, anywhere.”*
>
> **- Daniel Mintz, CTO, Consulting Firm CSC,**
> **former CIO, US Dept. of Transportation**

*Source: Government Accountability Office*

# Quest Value: Four Pillars of Transformation

- Active Directory and Identity Management
  - State Department AD provisioning
  - IDM at NASA, IRS, DHS/ICE
- Unified Communications
  - Exchange management at ICE, USSS, CBP
  - ADEX modernization US Army, USAF worldwide
  - IM audit and security across the intel community
- Application & Database Performance Management
  - End user performance at TSA, US VISIT, BPD
  - Oracle and Java diagnostics at FBI, TSA, US VISIT
- Virtualization Management
  - DHS CBP iLab, FLETC, USCG
  - Desktop virtualization at Centcom

# The State of Security

- Dennis Heretick, Independent Contractor
  - Former Chief Information Security Officer, Department of Justice

# Risk Assessment Factors

- Vulnerability or Threats Minus Countermeasures
  - Threat Exploitability (EX) minus countermeasures (CT)
- Likelihood
  - Threat source capability, motivation, gain
  - History and/or predicted success
  - Capability to detect or attribute to source
- Mission Impact Level
  - Mission operations, assets, people, other organizations, national interests

# Threat Categories and Sources

- Threat Categories
  - Hacking and intrusion
  - Malware
  - Insider misuse and abuse
  - Social attacks and deceit
  - Errors and omissions
  - Physical attacks
  - Natural disasters, accidents
- Threat Sources
  - Internal
  - External
  - Partner

# Risk Control

- Analyze Mission Risk Control Requirements
  - Review implemented and planned controls
  - Use policy based requirements checklist for security testing
- Prioritize, Plan and Implement Risk Controls
  - Effectiveness of recommend options
  - Legislation and regulation
  - Operational impact
  - Safety and reliability

# Secure Federal File Sharing Act – HR 4098

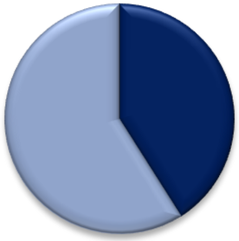
- Within 90 days of enactment, OMB, in consultation with Federal CIO Council will issue guidance to:
  - Prohibit open network peer-to-peer file sharing unless they are:
    - Necessary for business operations
    - Instrumental to directly support agency's mission
    - Necessary for use between, among or within Federal, State or Local government
- Within 180 days of enactment, agencies will:
  - Establish personal use policies
  - Require agency contractors to comply
  - Update security and ethics policies
  - Ensure proper security controls are in place
- One year after enactment OMB will report on agency justification and provide an inventory of peer-to-peer use

# The State of Security

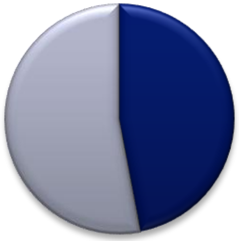
- John Milburn, Vice President, Windows Business Unit

# Survey Says:

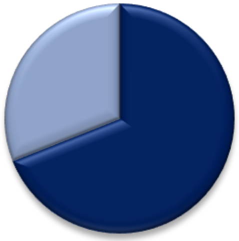
Online survey of government IT executives highlights top five security priorities:



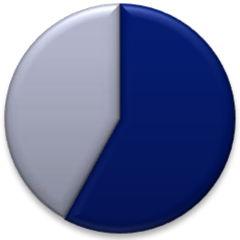
**Mobile devices (encryption, physical security)**
(59%)



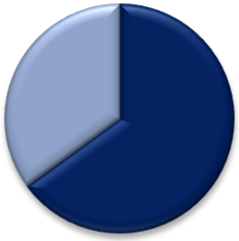
**Physical plant intrusion detection, access control via identity management**
(53%)



**Virtualized environments and cloud computing**
(31%)



**Protection from cyberattacks on critical infrastructure**
(42%)



**Network architecture**
(35%)

> *"Identity management tools were ranked in the top 5 among security investments to be made this year by 37% of survey respondents."*
>
> **- Online Survey of Government IT Executives,**
> **1105 Government Information Group, June 2009**

QUEST SOFTWARE®
Smart Systems Management

*Source: 1105 Government Information Group, June 2009*

# Quest Can Help You:

✓ 1. **Lock down the infrastructure**
Safeguard user identities, protect important information and preserve other mission-critical applications

✓ 2. **Ensure resiliency**
Achieve swift and comprehensive recovery in the event there is a security breach – minor or catastrophic

✓ 3. **Be 100% reliable**
Rely on our proven track record of ensuring security and protection, both inside and outside of your organization

✓ 4. **Deliver comprehensive reports**
Understand and report on conditions and activities in the IT environment, both in real time (with notification) and from a historic perspective (including long-term analysis)

✓ 5. **Demonstrate clear correlation to the cybersecurity initiative**
Solve cybersecurity concerns but also prove – at all levels of the organization – that improvements move the needle on diminishing cybersecurity threats

✓ 6. **Focus on high-risk relevancy platforms**
Address the systems, applications and platforms identified as high-risk by government regulations

# Consensus Audit Guidelines:

## Critical Controls for Effective Cyber Defense

1: Inventory of Authorized and Unauthorized Devices

2: Inventory of Authorized and Unauthorized Software

3: Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers

4: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches

5: Boundary Defense

6: Maintenance, Monitoring, and Analysis of Audit Logs

7: Application Software Security

8: Controlled Use of Administrative Privileges

9: Controlled Access Based on Need to Know

10: Continuous Vulnerability Assessment and Remediation

11: Account Monitoring and Control

12: Malware Defenses

13: Limitation and Control of Network Ports, Protocols, and Services

14: Wireless Device Control

15: Data Loss Prevention

16: Secure Network Engineering

17: Penetration Tests and Red Team Exercises

18: Incident Response Capability

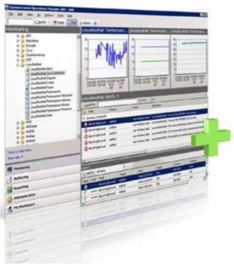
19: Data Recovery Capability

20: Security Skills Assessment and Appropriate Training to Fill Gaps

# Control 2: Inventory of Software

- Extend System Center Configuration Manager to Unix, Linux and Mac systems
  - Capture detailed hardware and software inventory from non-Windows systems
  - Run standard reports to track agency assets
  - Meter applications to determine real usage
  - Combine non-Windows inventory with Windows inventory to view enterprise assets
- Identify and control user and group access to resources across the enterprise
- Collect, store and report on data from Active Directory and Windows

Quest® Management Xtensions CONFIGURATION MANAGER 2007 EDITION

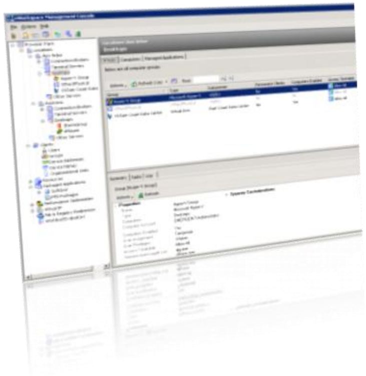


Quest® Reporter

# Control 3: Secure Configurations for Hardware and Software: VDI

Quest® vWorkspace

- Ensure centralized configuration management for local and remote users
- Secure telework gateway
  - Secure: Two-factor authentication, an SSL gateway, and comprehensive delegation of administrator privileges
  - High availability: rapid recovery with one-click reprovisioning
- Automate time-consuming configuration tasks
  - Dynamically create desktop and Start menu shortcuts
  - Connect to shared network folders and printers
  - Execute scripts
  - Configure user registry settings and environment variables
  - Lock down user with standard Explorer shell policies



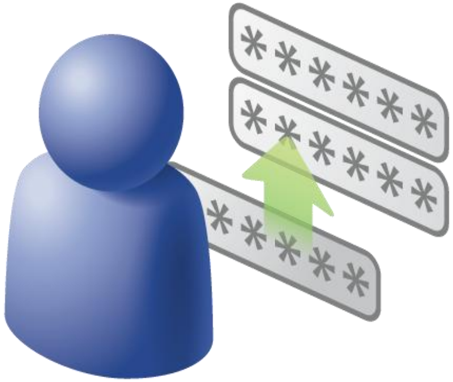
# Control 3: Secure Configurations for Hardware and Software

- Perform automated comparisons of Active Directory and Windows configurations
- Support internal and external operational practices
- Strengthen and enforce security policy across platforms
- Extend “good” policy from Windows to non-Windows systems and applications
- Consolidate logins around more secure identities and practices
- Eliminate redundant and inconsistent passwords and policy

Quest® Reporter

Quest® Password Manager

Quest® Authentication Services



# Control 5: Boundary Defense

- Implement strong authentication
  - One-time password (OTP) authentication
    - Active Directory-based
    - Token-agnostic
    - Zero-impact migrations
    - Multiple form factors
  - Extend Windows TFA to Unix/Linux/Java
    - CAC
    - Gemal to smart cards
    - OTP (Quest Defender, Verisign, RSA)
- Protect critical data and resources
    - Create a DMZ for web-based access
    - Web single sign-on
    - Authentication based on Active Directory

Quest® Defender

Quest® Authentication Services

QUEST SOFTWARE®
Smart Systems Management

# Control 6: Maintenance, Monitoring and Analysis of Audit Logs

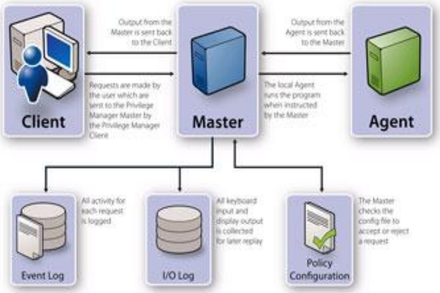
Quest® ChangeAuditor® for Active Directory

- Collect data on all access-related events across heterogeneous systems
  - Monitor access to critical systems and detect inappropriate or suspicious access-related events
- Store event logs in a secure repository
  - Automate the collection and storage of event logs
- Real-time notification and smart alerts
  - Identify when patterns of changes occur
- Reporting
  - Access predefined reports
  - Generate custom reports quickly and flexibly
  - Use online portal to access reports when needed

# Control 8: Controlled Use of Administrative Privileges

Quest® Privilege Manager *for Unix*

- Control access granularly
  - Based on roles, rules and policies
  - Available for Windows as well as Unix and Linux
- Audit elevated access and activities
  - Who, what, when, where, and how
  - Keystroke logging
- Strengthen elevated authentication
  - One-time passwords (OTP)
  - Extend Windows smart cards to Unix, Linux and Mac
- Monitor for abnormal behavior, specifically during off-peak hours


Client
Output from the Master is sent back to the Client
Requests are made by the user which are sent to the Privilege Manager Master by the Privilege Manager Client
Master
Output from the Agent is sent back to the Master
The local Agent runs the program when instructed by the Master
Agent
Event Log
All activity for each request is logged
I/O Log
All keyboard input and display output is collected for later replay
Policy Configuration
The Master checks the config file to accept or reject a request

# Control 9: Controlled Access

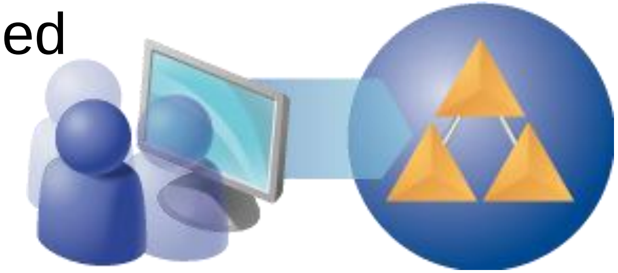
- Extend Active Directory access control to:
  - Unix, Linux and Mac
  - Applications (Java and standards-based)
  - Enterprise SSO based on AD authentication
- Gain granular control of AD-based access
  - Role and rule-based
- Control access to resources
  - Files, folders, shared, etc.
- Control exactly what administrators can do
  - Nothing more, nothing less
  - For existing groups and Windows Group Policy

# Control 11: Dormant Account Monitoring and Control

- Accelerate de-provisioning
  - Terminate enterprise access with a single action
  - Reduce the number of user accounts to de-provision
- Gain visibility into dormant and inactive accounts
- Get alerts when inactive accounts are used
- Find dormant accounts and take action on them
  - Monitor and track configuration and usage of mailboxes
  - Monitor and record failed login attempts and account lockouts

Quest® ActiveRoles® Server

MessageStats™



QUEST SOFTWARE®
Smart Systems Management

# Control 18: Incident Response Capability

InTrust®

- Establish automatic actions to certain events
  - Reverse changes immediately
- Audit changes granularly (who, what, when, where and how as well as before and after values)
- Get real-time alerts when an event occurs

# Critical Controls for Instant Messaging (IM)

Quest® Policy Authority for Unified Communications

- CAG 2: Inventory of authorized software
  - Correlate end-user identities from corporate directory to user handles and phone numbers
  - Establish peer-to-peer (P2P) controls; Block Skype, FastTrack (e.g., Kazaa), BitTorrent, OpenNapster, IRC, Gnutella etc.
- CAG 5: Boundary Defense
  - Repel known and zero-day virus infections
  - Provide content filtering/tagging for IM chats
- CAG 9: Controlled Access and block use of:
  - Enterprise IM servers; financial and public IM platforms
- CAG 15: IM data leak protection
  - Block unwanted protocols; protect sensitive data
  - Enforce regulatory compliance
  - Capture IM and file transfers; PIN-to-PIN and SMS
  - Demonstrate compliance with HR 4098

# QUESTIONS?

- Contributors:
  - Paul Garver, Vice President, Quest Public Sector
  - Dennis Heretick, former CISO, Department of Justice
  - Einar Mykletun, Federal Security & Compliance Architect
  - John Milburn, Vice President & GM, Windows Business Unit
  - Andy Sullivan, IM Security Product Manager
  - Keith Graham, VDI Product Manager