



# IT IS TIME TO SWITCH TO ATTACK-BASED METRICS FOR FISMA COMPLIANCE

Presented at Security 2008, Reagan Center, Washington, DC  
November 21, 2008

Alan Paller, Director of Research, SANS Institute, [apaller@sans.org](mailto:apaller@sans.org)

**Why did your agency let the Chinese steal that information?**



# FISMA compliance as it plays out in the US Government today:

*Security person: "You need to make sure your project meets all NIST security requirements."*

*Project person: "Our system goes live in three weeks; NIST documents are two feet thick; it would take a year and a huge amount of money to meet all those requirements – in fact it would take months and \$100,000 just to study all the NIST special pubs and agree on what they require us to do. Do we have any other options?"*

*Security person: "All you have to do is get a consultant to write a report listing risks and then persuade the designated approving authority (DAA) to sign a document saying he accepts the risks."*


*DAA: "I don't understand all the stuff in this consultant's report. I won't sign it."*

*Security person: "I hear you. But if you don't accept the risk and accredit the system, the Deputy Secretary is going to kill the CIO and you and me. Clay Johnson in the White House is pressuring him to get all our systems accredited by July 1."*

*DAA: "OK, Where do I sign?"*



# Why doesn't the agency just implement NIST guidance?

- The guidance is not definitive
  - It is often internally inconsistent or open to interpretation
  - It cannot be audited reliably
  - In other words, agencies cannot rely on NIST for answers to the three most important questions:
- 

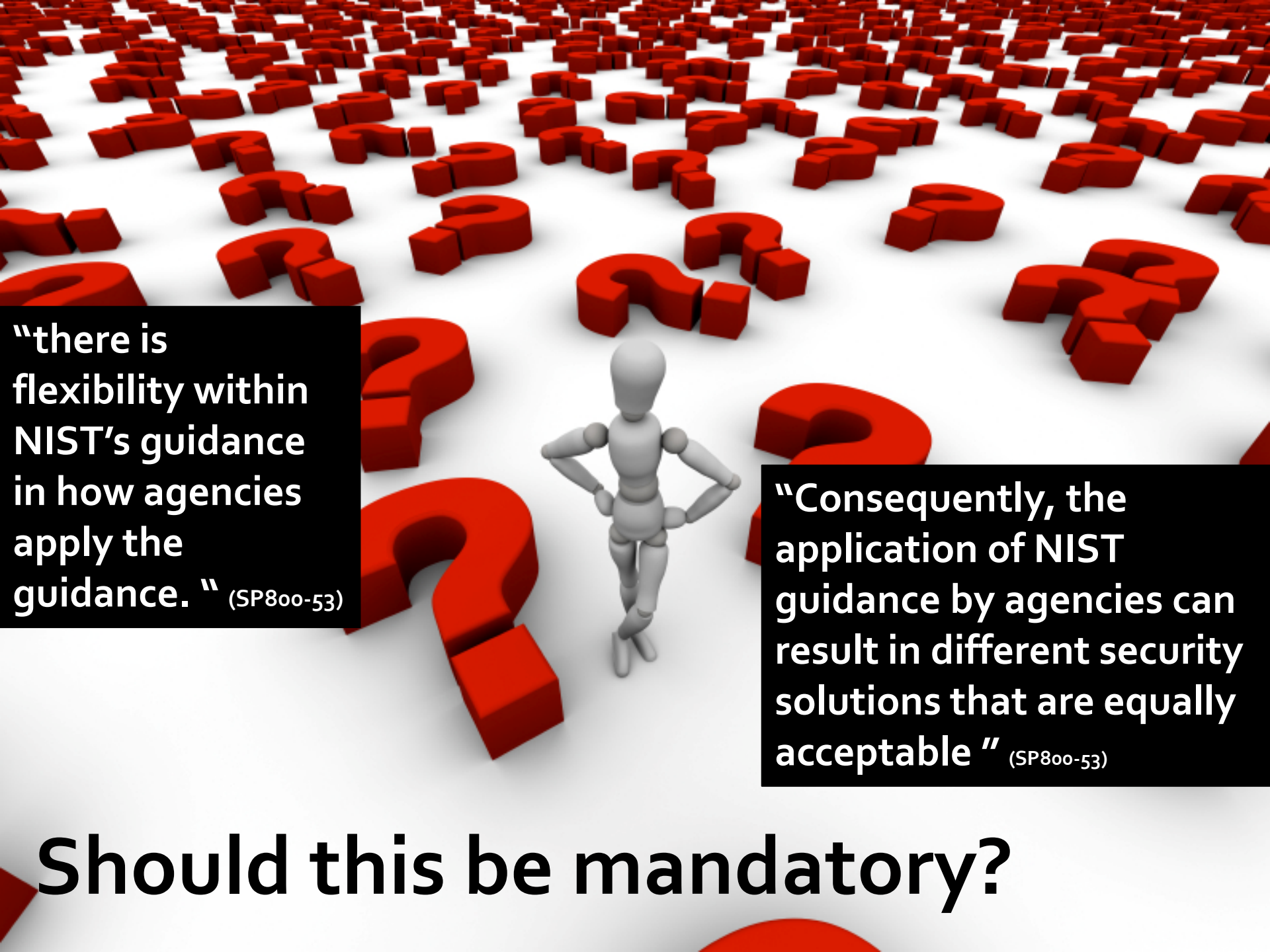


# The three unanswered questions:

1. What do we have to do to secure our systems?
2. How much is enough?
3. Whom can we trust to give us the right answers?



Question: Doesn't NIST guidance answer these questions?



**“there is flexibility within NIST’s guidance in how agencies apply the guidance.” (SP800-53)**

**“Consequently, the application of NIST guidance by agencies can result in different security solutions that are equally acceptable” (SP800-53)**

**Should this be mandatory?**



Addressing all the controls  
results in high costs and  
ineffective threat reduction.



**... also causes wasteful wars between  
inspectors general and CIOs/CISOs**


overlooking the obvious





**You would have to be crazy not  
to manage “the known bads.”**

**And nearly every system  
on the Internet is at risk  
from these same threats  
and same vulnerabilities.**



A CENTRAL THEME OF THE CNCI  
(COMPREHENSIVE NATIONAL  
CYBER INITIATIVE)

**“Defense Must  
Be Informed by  
the Offense”**

# Who understands offense?

- NSA Red Teams
- NSA Blue Teams
- DoD Cyber Crime Center (DC<sub>3</sub>)
- US-CERT (plus 3 agencies that were hit hard)
- Top Commercial Pen Testers
- GAO
- Top Commercial Forensics Teams
- JTF-GNO
- AFOSI
- Army Research Laboratory
- DoE National Laboratories
- FBI and IC-JTF

Would they be willing to combine their knowledge to define the most important defensive investments CIOs must make?

# Consensus Audit Guidelines (CAG)

- Four tasks:
  1. Agree on the controls that would stop or quickly recover from the known attacks
  2. Provide real-world examples of those attacks
  3. Agree on how to measure the effectiveness of those controls
  4. Help contractors now doing C&A and other FISMA reporting to shift to supporting agencies in implementing the key controls and in measuring them.

# An Example: Attack-Based Control

1. Locked down configurations for hardware and software for which such configurations are available.

Why?

How bad guys are getting into well-protected systems?

**Spear Phishing** - Victims being attacked while doing what they should be doing

What's wrong with this hypertext url?

<http://www.microsoft.com/security>

# How Spear Phishing Destroys Your Perimeter

- An e-mail arrives in inboxes of US Gov officials, from Karen Evans, saying:
  - “ I just got off the phone with the folks at Microsoft who gave me a heads-up about a major new vulnerability. They won't be making the patch public until next Tuesday, but have offered us early access to the patches. Before you leave work today go to the following Microsoft site and download the new patch

<http://www.microsoft.com/security/USGOV-Alert-windows.msp>



Search Microsoft.com for:



## Trustworthy Computing: Security

- Security Home
- Security Updates
- Recent Incidents
- Partners


### Information For

- Home Users
- IT Professionals (TechNet)
- Developers (MSDN)
- Small Businesses
- Worldwide Security Sites

### Trustworthy Computing

- Overview
- Privacy
- Reliability
- Business Integrity

**YOUR IT STAFF**



**IS ARMED AND READY**

GET SECURITY TOOLS AND TRAINING >

Microsoft

## Windows Security Update Summary for May 2005

Published: May 10, 2005

The security update for May 2005 is an important update for Microsoft Windows. If you have any of the software listed on this page installed on your computer, you should install the related update.



[Skip the details and get the updates now](#)

### Security Bulletin MS05-024

**Maximum severity:** Important ([What is a severity level?](#))  
**Update number:** 894320 ([What is an update number?](#))  
**Supported software affected:**

- Windows 2000 Service Pack 3 (SP3)

**Technical bulletin:** [Vulnerability in Windows 2000 Remote Code Execution \(894320\)](#)

### Check the Version

If you are not sure whether the software you are running is affected, check the version.

- [Get instructions for how to check](#)

### For More Information

Find support information about these security issues in the Microsoft Knowledge Base.

- [KB894320](#)

[↑ Top of page](#)

**Security Alerts**



Get e-mail or alerts about security updates

### Related Links

- [Technical Bulletins](#)
- [Software Life Cycle Support Information](#)
- [Security Bulletin FAQ](#)
- [How to Tell If a Security E-Mail Notice Is Really From Microsoft](#)
- [Protect Your PC](#)

**Why it went to the wrong place: html code was actually:**  
**<a href="http://www.hackersite.com">http://www.microsoft.com/security/USGOV-Alert-windows.msp</a>**

**Would it have fooled anyone in your organization?**

# Then what happens?

- Malicious software causes the victim to make a legal web connection to a server controlled by the attackers.
- That server sends software and commands to control the now slave computer.
- Slave computer searches all other computers (note it is inside the firewall so it has access) and collects huge amounts of data.
- Slave computer compresses the data and sends it to a storage computer from which it is later moved to the attacker's systems.



# What would have stopped that attack?

Locked down configurations : FDCC

Effective security controls are **money savers** and **mission enablers**. Air Force results:

1. Cut patch time from 57 days to 72 hours
2. Reduced costs by tens of millions of dollars
3. Made users happier

# Sample Attack-Based Controls

1. Locked down configurations; rapid patching (plus application procurement standards enforcement)
2. Wireless device control
3. Application security testing/remediation
4. Secure, robust audit logs; monitored regularly
5. Dormant account control
6. Boundary defense (web proxies; no agency.gov access from outside in; data leakage protection, IDS/IPS)





# What does the CAG Provides

1. Description of each control
2. Sample real-world attack(s) that were successful because the control was not effectively implemented
3. Method to validate effective implementation of the control – typically with automation
4. Warnings




# Next Steps

- CAG team meets to agree on the final list and identify ways to maximize automation
  - Period of public comment and revisions
  - CAG team ensures implementation methods are cost effective and auditing methods are reliable
  - The CIO Council reviews CAG and if acceptable, asks OMB to change its guidance to use CAG controls to measure FISMA.
- 



A CHALLENGE: Helping security people develop the skills to implement and test the critical security controls.

Why should they change?



Mike Jacobs (12 months ago): “70% of our staff have soft skills; only 30% have specialized security skills. If we don’t reverse that ratio in the next two years, we’ll be out of business.”



# QUESTIONS

Alan Paller  
apaller@sans.org