

# **20 Critical Controls For Cyber Defense: Consensus Audit Guidelines**

John M. Gilligan

IAC Information and Security Meeting

June 10, 2009

# Topics

- Background
- Philosophy and Approach for the “20 Critical Controls”
- Control Examples and List of Controls
- Next Steps
- Final thoughts

# Cyber Security Today—A New “Ball Game”

- Our way of life and economic prosperity depend on a reliable cyberspace
- Intellectual property is being downloaded at an alarming rate
- Cyberspace is now a key warfare domain
- Attacks are increasing at an exponential rate

**Cyber Security is a National Security Crisis!**

# Government Security Environment

- We are in a cyber “war” and are losing badly!
- The IT industry has produced an inherently unsecure environment—total is security not achievable
- CIO mandates exceed time and resources available
- Cyber security is an enormously complex challenge—there are very few true experts

**It is time to focus on ways to make real improvements in security**

## FISMA Was Well Intended; What is Not Working??

- Original intent was good:
  - Ensure effective controls
  - Improve oversight of security programs
  - Provide for independent evaluation
- Implementation took us off course
  - Agencies unable to assess risks
  - (Lots of) NIST general “guidance” became mandatory
  - No auditable basis for independent evaluation
  - Grading became overly focused on paperwork

**Bottom Line: High cost and debates about security improvements!**

# Analogy of Current FISMA Implementation

- An ambulance shows up at a hospital emergency room with a bleeding patient
- Hospital gives inoculations for flu, tetanus, shingles, and vaccination updates
- Hospital tests for communicable diseases, high blood pressure, sends blood sample for cholesterol check, gives eye exam and checks hearing
- At some point, doctors address the cause of the bleeding

**OMB Policy Regarding FISMA Results in a Checklist Approach**

**Meanwhile, the patient is  
bleeding to death!!**

**We Need Triage--Not Comprehensive Medical  
Care**

# How Should We Assess Effective Security?

"Pentagon Shuts Down Systems After *Cyber-Attack*"

*GAO Reports?*

Malicious scans of DoD  
increase 300%!

*Congressional FISMA  
Grades?*

*Percentage of  
Systems Certified?*

*Number of Systems with  
Contingency Plans?*

*AGENCY AUDITOR  
REPORTS?*

*Laptop with Personal  
Information Stolen...*

**We need to objectively measure the effectiveness of security controls!**

# An “Aha” Moment!

- Scene: 2002 briefing by NSA regarding latest penetration assessment of DoD systems
- Objective: Embarrass DoD CIOs for failure to provide adequate security.
- Subplot: If CIOs patch/fix current avenues of penetration, NSA would likely find others
- Realization: Let’s use NSA’s offensive capabilities to guide security investments

**Let “Offense Inform Defense”!**

## “20 Critical Controls”: The Philosophy

- Assess cyber attacks to inform cyber defense – focus on high risk technical areas first
- Ensure that security investments are focused to counter highest threats — pick a subset
- Maximize use of automation to enforce security controls — negate human errors
- Define metrics for critical controls
- Use consensus process to collect best ideas

**Focus investments by letting cyber offense inform defense!**

# Approach for developing 20 Critical Controls

- Engage the best security experts:
  - NSA “Offensive Guys”
  - NSA “Defensive Guys”
  - DoD Cyber Crime Center (DC3)
  - US-CERT (plus 3 agencies that were hit hard)
  - Top Commercial Pen Testers
  - Top Commercial Forensics Teams
  - JTF-GNO
  - AFOSI
  - Army Research Laboratory
  - DoE National Laboratories
  - FBI and IC-JTF
- Prioritize controls to match successful attacks—mitigate critical risks
- Identify automation/verification methods and measures
- Engage CIOs, CISOs, Auditors, and Oversight organizations
- Coordinate with Congress regarding FISMA updates

## Example--Critical Control #1

### *Inventory of Authorized and Unauthorized Devices*

- **Attacker Exploit:** Scan for new, unprotected systems
- **Control:**
  - QW: Automated asset inventory discovery tool
  - Vis/Attrib: On line asset inventory of devices with net address, machine name, purpose, owner
  - Config/Hygiene: Develop inventory of information assets (incl. critical information and map to hardware devices)
- **Automated Support:** Employ products available for asset inventories, inventory changes, network scanning against known configurations
- **Evaluation:** Connect fully patched and hardened machine to measure response from tools and staff

## Example--Critical Control #3

### Secure Configurations for Hardware and Software on Laptops, Workstations and Servers

- **Attacker Exploit:** Automated search for improperly configured systems
- **Control:**
  - QW: Define standard images that are hardened versions
  - QW: Negotiate contracts for secure images
  - Config/Hygiene: Executive metrics with trends for systems meeting configuration guidelines
- **Automated Support:** Employ SCAP compliant tools to monitor/validate HW/SW/Network configurations
- **Evaluation:** Introduce improperly configured system to test response times/actions

# 20 Critical Controls for Effective Cyber Defense (1 of 2)

## *Critical Controls Subject to Automated Collection, Measurement, and Validation:*

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 Security 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

## 20 Critical Controls for Effective Cyber Defense (2 of 2)

**Additional Critical Controls (not directly supported by automated measurement and validation):**

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

# Relevance of 20 Critical Controls to FISMA and NIST Guidelines

- FISMA
  - Security protections commensurate with risk
  - Implementation of minimum controls
  - Product selection by agencies
  - Periodic testing and evaluation of controls
- NIST Guidelines
  - Risk assessment is starting point
  - Selection of controls based on risk
  - 20 Critical Controls are subset of 800-53 controls

**20 Critical Controls allows agencies to comply with FISMA!**

# Relevance of 20 Critical Controls to FISMA 2.0 \*

- *“monitor, detect, analyze, protect, report, and respond against known vulnerabilities, attacks, and exploitations” and “continuously test and evaluate information security controls and techniques to ensure that they are effectively implemented.”*

\*Senate Homeland Security and Government Affairs Committee: (Draft ICE Act of 2009)

# 20 Critical Controls: Initial Pilots

- State Department
  - Performed mapping of attack patterns to 20 Critical Controls
  - Implemented dashboard to track progress of subordinate organizations
- Nuclear Regulatory Commission
  - Currently collecting testing data

# Next Steps

- Distribute revised document—Updated to reflect public comments (~ 80 sets of comments received)
- Assess pilot implementations at State Dept and Nuclear Regulatory Commission
- Continued engagement with CIOs, CISOs, Auditors/IGs
  - Identify additional FY '09 government pilot sites
  - Develop recommendations regarding policy implementation and “scoring” approach
- Workshops on specifications for tools for each control including expanded use of SCAP

# Comments on 20 Critical Controls

- “The federal government needs to focus limited resources on protecting our networks from consistent cyber attacks that threaten our national security and the Consensus Audit Guidelines is a good first step.”—Sen. Tom Carper
- “This is an excellent document. Hopefully it will get broad adoption.”—Amit Yoran, Netwitness
- "Thank you for your work on the Consensus Audit Guidelines as they are a good encapsulation of requirements needed for Federal IT Security."-- Peter McDonald, Symantec
- "Bottom line, a great effort..." —Col Gary McAlum, USAF (Ret)
- "I want to say that the CAG is a great start. I find that the document provides a common baseline of security, and realistic suggestions to validate that the controls are improving security. Hopefully, auditors will actually look at the outputs of the tests; rather than just check off that some control has been put into place."-- Timothy McKenzie, Raytheon
- "We find the document to be an excellent guide for Cyber defense..." -- Tom Kreidler, Lumeta
- "I am impressed with the content of the CAG document. Nice work!"  
-- Clint Kreitner, The Center for Internet Security

# Final Thoughts

- Federal government with industry support can lead global change
- In the near-term we must focus our efforts to make measurable progress
- Automation of security control implementation and enforcement is essential
- A well managed system is a harder target and costs less to operate

**We Need to Stop the Bleeding—Now!**

# Contact Information

John M. Gilligan

[jgilligan@gilligangroupinc.com](mailto:jgilligan@gilligangroupinc.com)

703-503-3232

[www.gilligangroupinc.com](http://www.gilligangroupinc.com)

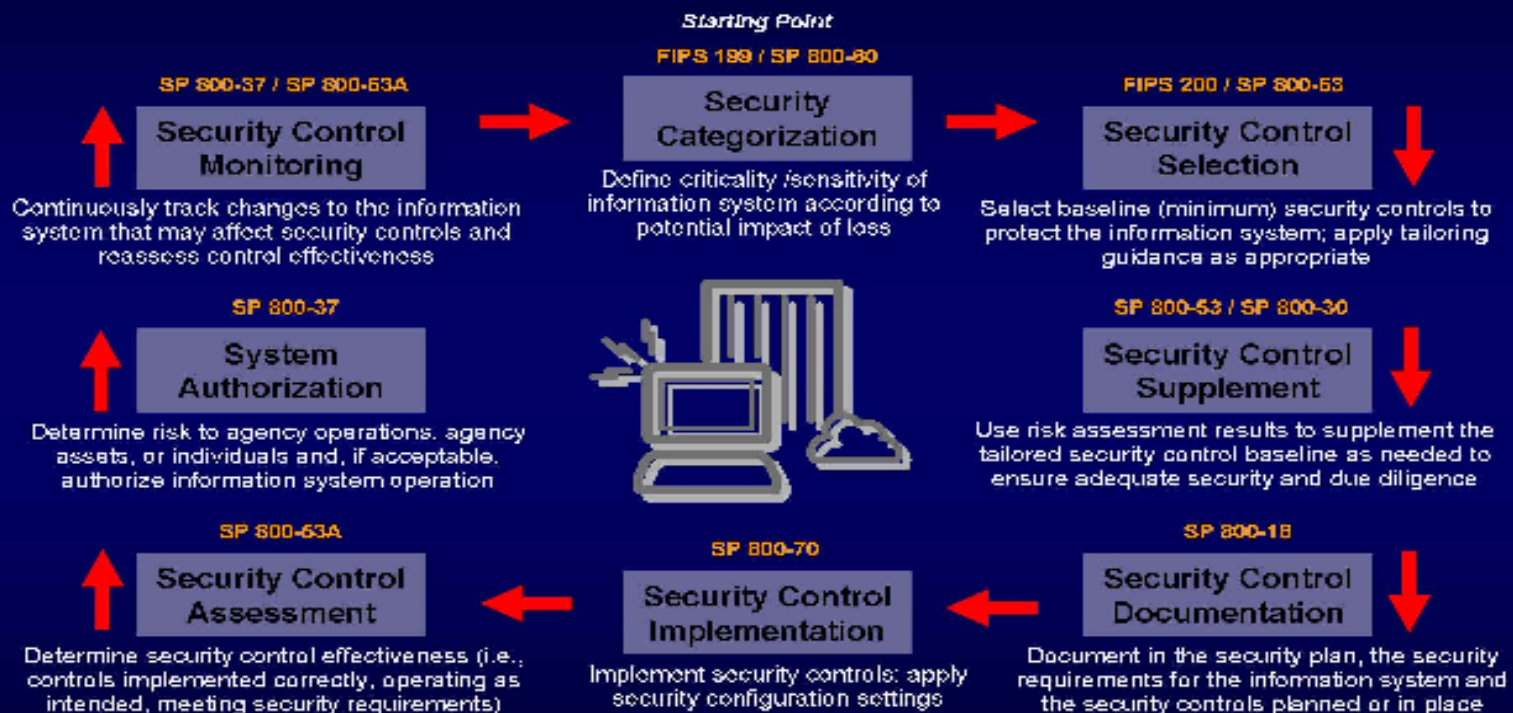
# Backup

# FISMA Original Intent

- Framework to ensure effective information security controls
- Recognize impact of highly networked environment
- Provide for development and maintenance of minimum controls
- Improved oversight of agency information security programs
- Acknowledge potential of COTS capabilities
- Selection of specific technical hardware and software information security solutions left to agencies
- Provide independent evaluation of security program

However: FISMA has evolved to “grading” agencies based largely on secondary artifacts

# Risk Management Framework



National Institute of Standards and Technology

**NIST Guidance: 1200 pages of FIPS Pubs, Special Pubs, Security Bulletins, etc.**

# NIST Security Guidance

- NIST Risk Management Framework consists of over 1200 pages of guidance
- An additional security-related mandatory 15 Federal Information Processing Standard (FIPS) Publications
- Over 100 additional security related special publications
- Over 35 Interagency Reports
- Over 65 Security Bulletins (since 2002)

**Very comprehensive guidance—but are Agencies able to effectively implement it?**