20 Most Important Controls For Continuous Cyber Security Enforcement:
Consensus Audit Guidelines

John M. Gilligan

Information Security and Privacy Advisory Board

April 1, 2009

Topics

- Background
- Philosophy and Approach for the “20 Most Important Security 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

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
  - (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 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?

Congressional FISMA Grades?

Malicious scans of DoD increase 300%!

Number of Systems with Contingency Plans?

Percentage of Systems Certified?

AGENCY AUDITOR REPORTS?

Laptop with Personal Information Stolen…

We need to objectively measure the effectiveness of security controls!

20 Most Important Security Controls: Philosophy

- Leverage cyber offense to inform cyber defense – focus on high payoff areas
- Ensure that security investments are focused to counter highest threats — pick a subset
- Maximize use of automation to enforce security controls — negate human errors
- Use consensus process to collect best ideas

Focus investments by letting cyber offense inform defense!

Approach for developing 20 Most Important Security 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
  - GAO
  - Top Commercial Forensics Teams
  - JTF-GNO
  - AFOSI
  - Army Research Laboratory
  - DoE National Laboratories
  - FBI and IC-JTF
- Prioritize controls to match successful attacks
- Describe automation/verification methods
- Engage CIOs, CISOs, Auditors, and Oversight organizations
- Coordinate with Congress regarding FISMA updates

Example--Critical Control #1
Inventory of authorized and unauthorized hardware

- **Attacker Exploit**: Scan for new, unprotected systems
- **Control**: Accurate, up to date inventory controlled by automated monitoring and configuration management
- **Automated Support**: Employ products available for asset inventories, inventory changes, network scanning against known configurations
- **Evaluation**: Connect fully patched and hardened machine to test response from automated tools

Example--Critical Control #2
Secure Configurations for Hardware and Software
(where such configurations are available)

- **Attacker Exploit**: Automated search for improperly configured* systems
- **Control**: Deploy “locked down” configurations
- **Automated Support**: Employ SCAP and similar tools to monitor/validate configurations
- **Evaluation**: Introduce improperly configured system to test response times/actions

* Incorrectly configured or using manufacturer settings

20 Most Important Security Controls

(Critical Controls Subject to Automated Verification--1 thru 15)

1. Inventory of authorized and unauthorized hardware.
2. Inventory of authorized and unauthorized software.
3. Secure Configurations for Hardware and Software For Which Such Configurations Are Available.
4. Secure Configurations of Network Devices Such as Firewalls And Routers.
5. Boundary Defense
6. Maintenance and Analysis of Complete Security Audit Logs
7. Application Software Security
8. Controlled Use of Administrative Privileges
9. Controlled Access Based On Need to Know
10. Continuous Vulnerability Testing and Remediation
11. Dormant Account Monitoring and Control
12. Anti-Malware Defenses
13. Limitation and Control of Ports, Protocols and Services
14. Wireless Device Control
15. Data Leakage Protection
16. Secure Network Engineering
17. Red Team Exercises
18. Incident Response Capability
19. Disaster Recovery Capability
20. Security Skills Assessment and Training To Fill Gaps

Comments on 20 Most Important 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 area good encapsulation of requirements needed for Federal IT Security.”-- Peter McDonald, Symantec
- "Bottom line, a great effort...“ -- 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

Relevance of 20 Most Important Controls to FISMA 2.0 *

- *"Establish security control testing protocols that ensure that the information infrastructure of the agency, including contractor information systems operating on behalf of the agency, are effectively protected against known vulnerabilities, attacks, and exploitations."*
- *"Establishing a prioritized baseline of information security measures and controls that can be continuously monitored through automated mechanisms."*

*Senate Homeland Security and Government Affairs Committee: (Draft FIIRE Act of 2008)

Next Steps

- Refine CAG document—Updating to reflect public comments (~ 50 sets of comments received)
- Continued engagement with CIOs, CISOs, Auditors/IGs
  - Identify FY ‘09 government pilot sites
  - Develop recommendations regarding policy implementation and “scoring” approach
- Workshops on specifications for tools for each CAG control (Starting late April)

Final Thoughts

- Federal government can lead global change
- In the near-term we must focus our efforts to make measurable progress
- Automation of security controls 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
703-503-3232
www.gilligangroupinc.com

Backup

Cyber Security Commission

- Structure
  - Congressional sponsorship; managed by CSIS
  - Broad government, industry, and academic expertise and close coordination with CNCI
- Observations
  - Leadership must focus on National Security issue
  - Technology and governance lagging needs

Objective: “Game Changing” recommendations

Cyber Security Commission Recommendations

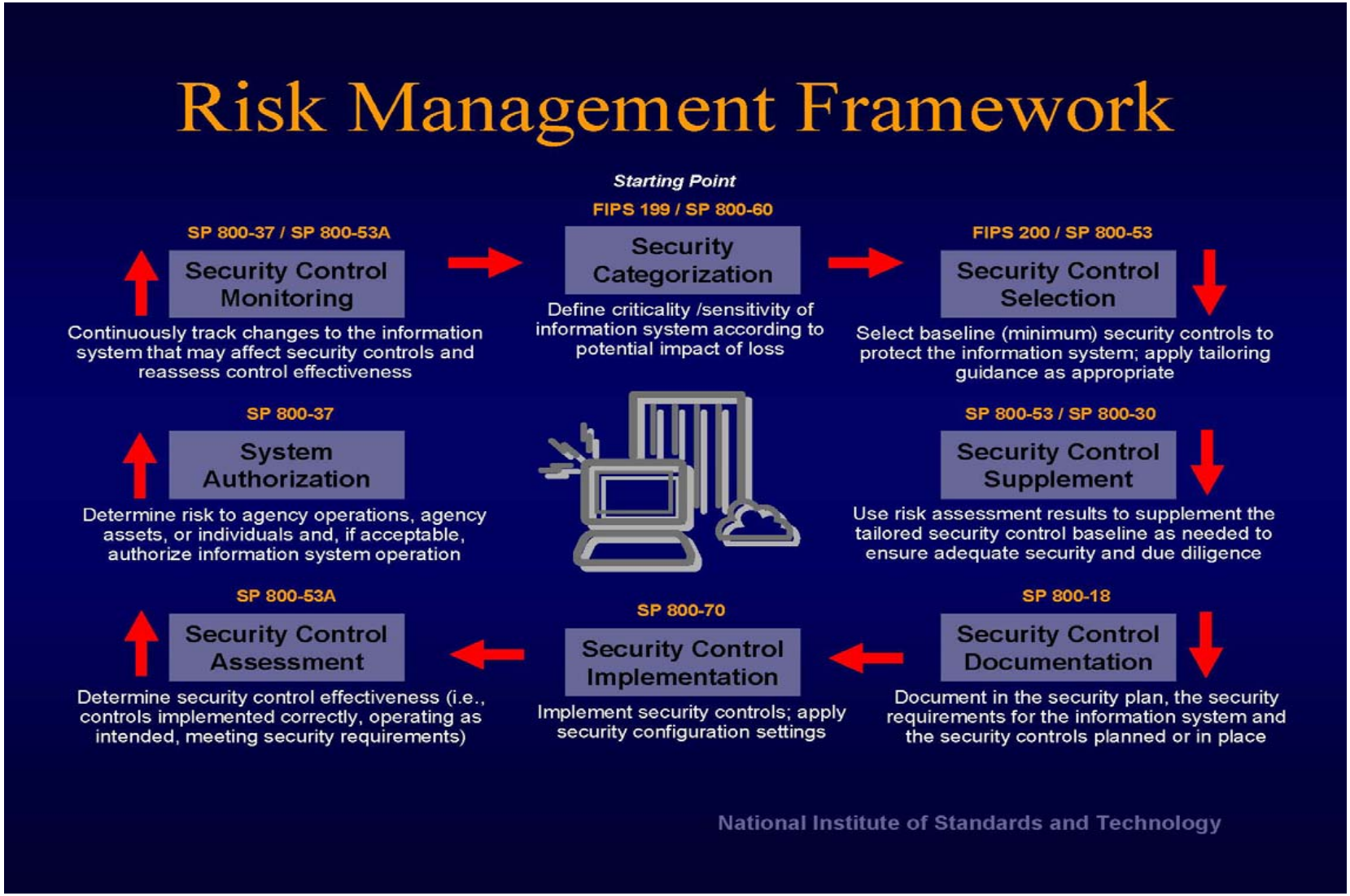
- Develop National Strategy for Cyberspace and publish National Cyberspace Doctrine
- Elevate and consolidate authorities for cyberspace (to White House)
- Enhance partnership with private sector
- Leverage elevated authority to coordinate existing regulatory authorities
- Use federal acquisition authorities to change industry model
- Modernize legal and policy framework

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

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

program



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

NIST Security Guidance

- NIST Risk 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)

A very impressive list of guidance—but is it contributing to improved security?