

Looking for a New FISMA

Introduction

The Federal Information Security Management Act (FISMA) of 2002 was authored with good intentions, but has endured very poor execution. It's a generally well known fact that FISMA has had many critics over the years that accuse the law of focusing more on documentation than actual implementation of security practices within the Federal space – including the Department of Defense. Within the DoD alone, the law has been responsible for the creation of volumes and volumes of documentation – much of which is obsolete or outdated by the time it is published and approved as part of the certification and accreditation process. In recent testimony to Congress, Vivek Kundra, Federal Chief Information Officer, Administrator for e-Government and Information Technology Office of Management and Budget wrote that, "...over the last six years, the Department of State spent \$133 million amassing a total of 50 shelf feet, or 95 thousand pages, of documentation for about 150 major IT systems." He then referred to these pages as "paper snapshots."

The transition from DITSCAP to DIACAP several years ago for the DoD has alleviated a lot of the over-burdensome documentation requirements, and thankfully, the security posture of enclaves or information systems is no longer inferred from how thick the DITSCAP binder is. In the past, the thicker the DITSCAP binder, the more secure the system was thought to be – that makes *perfect* sense, right? Wrong.

DIACAP solved a lot of this misconception by focusing less on documentation and more on the implementation of security controls. However, there is still a long way to go, and the focus remains on compliance, instead of performance. This article will identify the two fundamental issues with existing compliance processes that comprise the majority of FISMA scoring, and will highlight some ongoing efforts to reshape FISMA in 2010.

Performance vs. Compliance: Securing Well or Scoring Well?

The first question to ask is, *are you more interested in securing your infrastructure and systems or getting a good FISMA score?* These two aren't always mutually exclusive, but they can be more often than not. The number one, fundamental flaw I (and many others) see in FISMA, is that the focus is primarily on whether or not you have a control in place – instead of the effectiveness of that control. I'll give you two examples –

First, DoD policy requires a continuity of operations test to be conducted annually for information systems and enclaves – it's one of the controls in DoDI 8500.2. I've seen instances where, during a certification and accreditation effort, an information system was given a compliant score for this control because the system manager had conducted a continuity test that year, even though that test failed miserably. I've also seen an overwhelming use of so-called table-top continuity tests that give the system managers the ability to state that their system's continuity of operations was tested, but the system managers still have no idea how the system would fare if their system or the critical infrastructure it relies on became unavailable for any reason. This of course jeopardizes the security posture of the organization and more specifically the mission that the information system or enclave supports.

Second, monthly vulnerability scanning of information systems is also a requirement and certainly a best practice given the volume of patches that are released weekly and the volatility in technology today. Again, I have seen, as part of C&A validation teams, that many organizations are happy to proclaim that they are scanning monthly, but when you dig a little deeper, you quickly learn that nobody is reviewing the results of the scans.

In the two examples above, do the system or enclave managers meet the letter of the FISMA Law? Yes. Is the security posture of the organization or its mission positively impacted by these efforts? Absolutely not. The final product with respect to the two controls above is the appearance that all is well, when in fact, it's quite the opposite.

Because of the focus on *do you have it?* instead of *how well does it work?*, it's not very difficult to manipulate the FISMA process for a solid grade of A or B, but doing so provides a false sense of security, and makes organizations within the Federal Government unnecessarily vulnerable. If organizations choose to look a level deeper and perform assessments geared at assessing effectiveness, their FISMA scores will almost certainly suffer. This incentivizes organizations to review their systems and enclaves according to the letter of the law and focus on what they have instead of how well what they have works.

The good news is that FISMA reporting in 2010 is changing. OMB is going to begin looking more closely at spending habits of federal organizations to get a better understanding of the correlation between government spending and the performance impact of security dollars. Again, the shift seems to be moving away from compliance efforts (do you have it – yes or no?) into performance based metrics that describe how well those compliance efforts are working.

In his written testimony to Congress, Kundra outlines several initiatives that are in progress designed to proliferate some of the new goals being attached to proposed amendments to the FISMA law. Some of these programs include:

New Approach

- A new focus on coordination with the Cybersecurity Coordinator leading the way and involving the private sector and the Comprehensive National Cybersecurity Initiative (CNCI)
Shifting to performance-based culture by proliferating White House aspirations of transparency
 - through TechStat, implementing continuous monitoring, managing and analyzing information security costs, and new centralized reporting capabilities such as CyberScope
 - Taking an enterprise approach to managing Cybersecurity by establishing standards such as the Federal Desktop Core Configuration and the Trusted Internet Connections initiative, putting more
 - emphasis on awareness and cybersecurity education and training, leveraging Federal purchasing power through the use of Blanket Purchase Agreements, implementing Federal Identify Management initiatives like HSPD-12
 - Developing more robust research and development plans by enhancing the relationship between the government and the private sector (e.g., The Special Cyber Operations Research and Engineering (SCORE))
-

Hopefully Congress will get FISMA 2.0 right by ensuring the new law focuses more on performance, and less on yes or no compliance. Anything less than metrics based on performance will ensure that organizations continue spending millions of dollars complying instead of actually securing the Federal infrastructure.

Information Security Controls – All or Nothing?

John Gilligan, the former Air Force Chief Information Officer, illuminates the second fundamental issue with FISMA in his recent testimony to Congress. He also notes that FISMA was a positive step towards securing our federal infrastructure, and that it has some positive elements, however the overall approach is flawed. The primary example he provides is that FISMA does not focus on a small subset of security controls that will affect the greatest impact on information security. Instead, FISMA requires organizations to implement, "...the entire catalog of controls (over 300 separate controls) published by the National Institute of Standards and Technology (NIST)." For DoD, it's somewhere in the neighborhood of 150 controls to align with DoDI 8500.2 (however, the Department is looking at the possibility of abandoning DoDI 8500.2 for NIST SP 800-53).

This approach has caused organizations to perform at sub-par levels in their attempts to get *something* in place to satisfy a control or requirement – even if that something is insufficient or not effective. Again, this is the approach of being able to check a box, and not worry about how well that *something* performs. Also, implementing every control in the catalog is simply not feasible for very large, global Federal organizations with tight budget restrictions or insufficient resources.

To remedy this problem, a consortium of information security experts from government and the private sector came together to develop a new compliance vertical. This new cornerstone of compliance and performance is known as the *Twenty Critical Controls for Effective Cyber Defense: Consensus Audit Guidelines (CAG)*, and was released in late 2009.

The CAG takes the approach of identifying the 20 most critical information security controls that if addressed properly will mitigate risk associated with a large percentage of threats faced by Federal IT. What is great about these top 20 is that 15 of them are automatable. The top 20 controls recommended by the CAG include:

Control	Automatable
→ Inventory of Authorized and Unauthorized Devices	Yes
→ Inventory of Authorized and Unauthorized Software	Yes
→ Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers	Yes
→ Secure Configurations for Network Devices such as Firewalls, Routers, and Switches	Yes
→ Boundary Defense	Yes
→ Maintenance, Monitoring, and Analysis of Audit Logs	Yes
→ Application Software Security	Yes
→ Controlled Use of Administrative Privileges	Yes
→ Controlled Access Based on Need to Know	Yes
→ Continuous Vulnerability Assessment and Remediation	Yes
→ Account Monitoring and Control	Yes
→ Malware Defenses	Yes
→ Limitation and Control of Network Ports, Protocols, and Services	Yes
→ Wireless Device Control	Yes
→ Data Loss Prevention	Yes

→ Secure Network Engineering	No
→ Penetration Testing and Red Team Exercises	No
→ Incident Response Capability	No
→ Data Recovery Capability	No
→ Security Skills Assessment and Appropriate Training to Fill Gaps	No

Source: www.sans.org/critical-security-controls/

For each control, the CAG provides a description about how attackers exploit the lack of the control, How the control can be implemented to include quick win scenarios, mapping to NIST controls, procedures and tools for implementing the control, metrics for measuring compliance and performance of the control, and testing procedures.

For organizations struggling with compliance with FISMA, or for those that already have a good grade in FISMA that may be based on compliance rather than performance, I highly recommend reviewing the CAG. Perform an audit based on the performance measures defined in the CAG to get a good idea of how well your information security controls fare against performance-based criteria – which will hopefully be the future foundation of FISMA 2.0.

Conclusion and Further Reading

If you are unfamiliar with the new efforts to modify FISMA or the CAG, I highly recommend further research, as my description here is merely the tip of the iceberg. Many information security professionals within the Federal space are excited about adjustments to the FISMA metrics and the law itself, but some claim that drafts of the new law are not different enough, and may actually hurt future cybersecurity efforts. I recommend doing the research and forming your own opinion. The best time to affect change is before it's implemented. Either way, be prepared for change in the coming months and years as the Federal Government attempts to get better at managing and affecting information security.

More information and additional reading on these topics can be found here:

Twenty Critical Security Controls for Effective Cyber Defense: Consensus Audit Guidelines (CAG)

<http://www.sans.org/critical-security-controls/>

Testimony to Congress regarding FISMA

<http://www.sans.org/newsletters/newsbites/newsbites.php?vol=12&issue=24#sID200>

Draft Proposed Law has limited release. Look for:

H.R.4900 - Federal Information Security Amendments Act of 2010

About the Author

Chris Merritt | is the president and CEO of Prolific Solutions, LLC (www.prolific-solutions.net) and has been consulting for the DoD for over seven years. He is the author of proVM Auditor (www.provmauditor.com), a vulnerability assessment aggregation and compilation tool, and holds a number of information security certifications, including CISSP and CISA. He earned his Master's degree in information assurance from Norwich University in 2007.