RETHINKING FISMA AND FEDERAL INFORMATION SECURITY POLICY

ROBERT SILVERS*

In this Note, the author offers a broad-based critique of the statutory scheme that governs how the federal government must safeguard data on its information systems. Examining two illustrative case studies from major federal agencies, the author identifies serious structural flaws in the design and implementation of the relevant legislation. Through the lens of bureaucratic and organizational theory, he explains why the legislation is not well-suited to achieving comprehensive information security—and why the federal government's track record in this area has been so poor. Finally, the author proposes five concrete reforms Congress should enact to address these shortcomings.

* Copyright © 2006 by Robert Silvers. Law Clerk to the Honorable Kim McLane Wardlaw, United States Court of Appeals for the Ninth Circuit. J.D., 2006, New York University School of Law; B.A., 2002, University of Pennsylvania. Thanks to the staff of the *New York University Law Review*, especially Liz Sepper, Mario Mendolaro, Antoine McNamara, and Stephanie Brannen, for their thoughtful assistance. I am also grateful to the Honorable Robert A. Katzmann, whose enlightening seminar inspired me to pursue this topic. This Note is dedicated to my parents, David and Patty Silvers, for their love and guidance.

Reprinted with Permission of New York University School of Law

INTRODUCTION

A hacker commandeers programming codes for the computer systems that control the Internet.[1] Over the coming months, security breaches are detected in systems at a Pentagon missile testing facility in New Mexico, at a government jet propulsion laboratory in California, and at several NASA research centers. Even as government agents begin to monitor this activity, the hacker runs virtual circles around them, planting "Trojan Horse" viruses on government and university computer systems across the country. Fears mount over unauthorized access to F-18 fighter jet blueprints. The culprit? A sixteen-year-old living with his parents in eastern Sweden.[2]

The advancement and proliferation of information technology (IT) has been hugely beneficial for the federal government. IT is leveraged to maximize productivity and efficiency while enabling the government to offer products and services that were previously infeasible. Yet as the above incident demonstrates, the unprecedented accessibility and storage capacity that make computer systems so attractive for governmental functions create collateral problems of their own. A single malfunctioning chip can destroy information that was previously vulnerable only to flood or fire. The Internet's widespread availability gives anyone with a home computer the potential to access sensitive government databases. Hackers can modify government records without leaving a hint that anything has been changed. And the vast storage capacity of IT systems means that once hackers gain entry, they can compromise an enormous amount of data.

Such security breaches can be devastating to the government and citizens alike. Federal data is often sensitive and unauthorized access can be incredibly harmful. Tax filings contain private financial information about both individuals and organizations. Patent applications contain firms' most closely guarded trade secrets. Social Security numbers can aid the perpetrators of identity theft. Engineering plans and blueprints can assist terrorists in planning future attacks.

Even seemingly mundane data can be vital. The deletion of address rolls can interrupt the delivery of Social Security checks and other government payments. Modification of cargo manifests can allow importers to avoid paying customs duties or to circumvent customs inspections altogether. It is therefore essential that the federal

[1] John Markoff & Lowell Bergman, *Internet Attack Is Called Broad and Long Lasting*, N.Y. TIMES, May 10, 2005, at A1.

[2] *Id.*

Reprinted with Permission of New York University School of Law

government address the problem of information security decisively and comprehensively.

Nevertheless, efforts to secure federal data have been marked by delay, inefficiency, and ineffectiveness. The vast majority of federal agencies are delinquent in meeting their statutory information security obligations.[3] Agencies are unsure of the scope of their responsibilities and are too slow in satisfying those of which they are sure. The potential consequences of such failures are enormous, limited only by the imagination of a hacker or the serendipity of an accidental keystroke.

The threat is not hypothetical. There have been several publicized instances of compromised federal IT systems leading to detrimental results. In fiscal year 2004 alone there were over two thousand reported information security incidents throughout the federal government.[4] In addition to the episode noted above,[5] another hacker accessed at least ninety-seven U.S. government computers from his home in the United Kingdom, allegedly deleting a single file, rendering inoperable over three hundred computers at an American Naval Weapons Station. The U.S. Attorney prosecuting the case described the attack as "the biggest computer hack of all time."[6] Simply put, the federal government must do a better job of ensuring that agencies secure their data from unauthorized access, deletion, or modification.

In this Note, I argue that the current federal legislative scheme for achieving information security—the Federal Information Security Management Act of 2002 (FISMA)[7]—suffers from serious structural defects that account for its poor performance. Through an examina-

---

3 *See infra* note 25 and accompanying text.

4 OFFICE OF MGMT. & BUDGET, EXECUTIVE OFFICE OF THE PRESIDENT, FEDERAL INFORMATION SECURITY MANAGEMENT ACT (FISMA): 2004 REPORT TO CONGRESS 10 (2005) [hereinafter OMB 2004 FISMA REPORT]. The OMB report notes 2,058 reported incidents, but also mentions that agency reporting is "sporadic" and "[l]ess than full." *Id.* There is therefore reason to believe that the actual number of such incidents may be substantially higher.

5 *See supra* note 1–2 and accompanying text.

6 Catriona Davies, *US Army Computers 'Shut Down by Hacker,'* DAILY TELEGRAPH (LONDON), July 28, 2005, at 11 (internal quotation marks omitted). For an account of another breach of federal information security, see Press Release, U.S. Dep't of Justice, Indictment of Robert Lyttle (July 16, 2004), *available at* http://www.usdoj.gov/usao/can/press/html/2004_07_16_lyttle.html (announcing indictment for unlawful access to NASA and Pentagon computer systems and defacing of agency websites). Recent attacks on private-sector data banks have also garnered significant attention. In one highly publicized incident, hackers gained access to over 40 million credit card numbers from a payment processing facility based in Arizona. Eric Dash & Tom Zeller, Jr., *MasterCard Says 40 Million Files Are Put at Risk*, N.Y. TIMES, June 18, 2005, at A1.

7 44 U.S.C. §§ 3541–49 (Supp. II 2004).

Reprinted with Permission of New York University School of Law

tion of two case studies,[8] I demonstrate that agencies lack the proper incentives to adequately perform the task that Congress has mandated. Oversight is weak. Mechanisms available for enforcing agency accountability are misguided and seldom invoked. Agencies unsure of their responsibilities have no point of reference to consult. Because the goal of information security is generally distinct from the substantive policies agencies typically pursue, neither the public[9] nor Congress[10] is moved to apply much pressure. And even when agencies strive to comply fully with their obligations, FISMA's ambiguous drafting can lead to confusion and inefficient results. Only by amending the legislative scheme can Congress begin curing these deficiencies.

This Note will proceed in four parts. Part I briefly surveys the contours of FISMA, Congress's most recent effort at tackling the information security problem. Part II explores two case studies of agency efforts to implement FISMA and explains how those efforts have fallen short. Then, through the lens of organizational and bureaucratic theory, Part III considers *why* agencies have struggled so badly in this area. Finally, Part IV proposes five ways Congress should amend FISMA to address and ameliorate its shortcomings.

I
FISMA: THE CURRENT LEGISLATIVE SCHEME

FISMA marks the culmination of two decades during which Congress addressed these information security problems piecemeal through a scattered mosaic of legislation.[11] The bulk of the Act is comprised of parts that had previously been spread across the Government Information Security Reform Act, the Computer Security Act of 1987, the Clinger-Cohen Act, and the Paperwork Reduction Act of 1980.[12] FISMA takes steps to harmonize overlapping responsibilities, curtail obsolete requirements, and update out-

---

[8] *See infra* Part II.A–B.

[9] *See infra* Part III.C.

[10] *See infra* Part III.D.

[11] H.R. REP. NO. 107-787, pt.1, at 54 (2002), *as reprinted in* 2002 U.S.C.C.A.N. 1880, 1889.

[12] *Id.* The House Report states that FISMA consolidates the Government Information Security Reform Act, Pub. L. No. 106-398, sec. 1061–65, §§ 3531–36, 114 Stat. 1654A, 266–75 (2000), the Information Technology Management Reform (Clinger-Cohen) Act of 1996, Pub. L. No. 104-106, §§ 5001–02, 110 Stat. 679, 679–80, the Computer Security Act, Pub. L. No. 100-235, 101 Stat. 1724 (1988), and the Paperwork Reduction Act of 1980, Pub. L. No. 96-511, 94 Stat. 2812. *Id.*

Reprinted with Permission of New York University School of Law

dated provisions, while also introducing several important new requirements.[13]

FISMA mandates that every federal agency take affirmative steps to assess the susceptibility of its systems to abuse; to consider the magnitude of harm that would result from various breaches; and to implement technological safeguards against such breaches that respond proportionately to the risk of harm.[14] Specifically, FISMA requires that "[e]ach agency shall develop, document, and implement an agencywide information security program . . . to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source . . . ."[15]

Broadly speaking, then, FISMA demands that agencies organically develop information security strategies to safeguard their IT systems from unauthorized access and modification. Once those strategies are in place, FISMA further requires that agencies "periodically test[ ] and evaluat[e] information security controls and techniques to ensure that they are effectively implemented . . . ."[16] Responsibility for developing and testing these safeguards ultimately rests with "[t]he head of each agency,"[17] but is delegated down a chain of command beginning with the agency's Chief Information Officer (CIO) and eventually terminating with "a senior agency information security officer who shall . . . carry out the Chief Information Officer's responsibilities . . . ."[18]

Congress also devised a system of oversight meant to ensure agency compliance with FISMA, vesting the Office of Management and Budget (OMB) with supervisory authority over all agency information security programs.[19] OMB must approve each agency's plan for FISMA implementation;[20] must receive regular updates on agency

---

13 *Id.*

14 44 U.S.C. § 3543(a)(2) (Supp. II 2004) (calling for agencies "to identify and provide information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of" federal data). It is important to note that FISMA does not apply to classified information, which must be safeguarded pursuant to special instructions contained in Exec. Order No. 13,292, 68 Fed. Reg. 15,315 (Mar. 25, 2003) (amending Exec. Order No. 12,958, 60 Fed. Reg. 19,825 (Apr. 17, 1995)). Nevertheless, a significant quantity of sensitive unclassified data is spread across the various federal agencies, and its unauthorized disclosure, deletion, or modification can cause serious harm.

15 44 U.S.C. § 3544(b).

16 *Id.* § 3544(a)(2)(D).

17 *Id.* § 3544(a).

18 *Id.* § 3544(a)(3)(A)(i).

19 *Id.* § 3543(a).

20 *Id.* § 3544(b).

Reprinted with Permission of New York University School of Law

compliance; and must submit annual reports to Congress detailing each agency's progress and shortcomings in achieving information security.[21]

Lastly, FISMA fosters accountability by empowering OMB to enforce compliance through a list of suggested sanctions.[22] These sanctions include the power to reduce the agency's requested budget for IT and to appoint to an agency an executive agent who will "contract with private sector sources for the performance of information resources management . . . ."[23]

On paper, then, FISMA appears to be a reasonable tool to kick-start agency efforts in the daunting task of securing federal information systems. The necessary components for implementing an administrative program seem to be there: defined policy goals, specific instructions for implementation, oversight by OMB, and reports to a vigilant Congress. Nevertheless, FISMA's implementation, as the next Part will demonstrate, has been "uneven"[24] at best, and fully dysfunctional at worst.

II
THE AGENCIES' DISMAL RECORD

Since 2002, federal agencies have spent upwards of $4.2 billion to safeguard their information systems.[25] Nevertheless, compliance with FISMA has been largely disappointing. Agencies have been remarkably slow in taking steps to certify the security of their systems and have been subject to criticism from OMB,[26] courts,[27] and their own inspectors general (IGs).[28] Indeed, FISMA's first three years have been plagued by confusion, missed targets, and shocking deficits of accountability.

---

21 *Id.* § 3543(a)(8)(B)–(C).

22 FISMA incorporates by reference the array of punitive measures available to OMB pursuant to 40 U.S.C. § 11303(b)(5) (Supp. II 2004). *See* 44 U.S.C. § 3543(a)(4) (granting Director authority to use measures available under 40 U.S.C. § 11303 to oversee agency information security policies and practices).

23 40 U.S.C. § 11303(b)(5)(B)(iv).

24 OMB 2004 FISMA REPORT, *supra* note 4, at 13.

25 *Id.* at 1.

26 *E.g.*, *id.* at 10 (noting that "OMB is concerned with the accuracy, timeliness and completeness of [security] incident reporting [by various federal agencies]").

27 *See infra* Part II.A.

28 *See* OMB 2004 FISMA REPORT, *supra* note 4, at iv ("While progress has been made, agency IGs continue to identify deficiencies in security policy, procedure and practice.").

Reprinted with Permission of New York University School of Law

A. A Sluggish Response

Federal agencies have failed to approach the problem of information security with the sense of urgency it deserves. Despite localized success in particular agencies or bureaus, most have been persistently unable to fulfill their obligations, and "none of the 24 major agencies has fully implemented agencywide information security programs as required by FISMA."[29] In fiscal year 2004, twenty-three percent of federal information systems lacked the risk assessments and security testing required by FISMA.[30] One-quarter of systems lacked contingency plans to ensure continuity of government operations in case of a security breach. And of the systems covered by such plans, only fifty-seven percent had ever been tested to determine if the plans would actually be effective.[31]

The figures are even more striking within certain agencies, some of which are charged with performing many of the federal government's most sensitive and grave responsibilities. At the Department of Homeland Security, for example, seventy-nine percent of agency systems lacked a tested contingency plan.[32] Homeland Security officials likewise are without a complete inventory of their own information systems.[33] It is difficult to imagine how this crucial agency will meet its FISMA responsibilities when it has been incapable of even cataloguing the very systems it must ultimately secure.

OMB asked twenty-four inspectors general to evaluate the effectiveness of their agencies' FISMA implementation.[34] Seven described themselves as "poor," nine as "satisfactory," and only six as "good."[35] Two inspectors general—from the Departments of Agriculture and Veterans Affairs—failed to submit their findings altogether.[36] One-quarter of the surveyed agencies acknowledged serious systemic defi-

---

[29] *No Computer System Left Behind: A Review of the 2005 Federal Computer Security Scorecards Before the H. Comm. on Government Reform*, 109th Cong. 32 (2006) (statement of Gregory C. Wilshusen, Director, Information Security Issues, United States Government Accountability Office).

[30] OMB 2004 FISMA REPORT, *supra* note 4, at ii.

[31] *Id.*

[32] *The Need to Strengthen Information Security at the Department of Homeland Security: Hearing Before the Subcomm. on Management, Integration and Oversight of the H. Select Comm. on Homeland Security*, 109th Cong. 4 (2005) (statement of Gregory C. Wilshusen, Director, Information Security Issues, United States Government Accountability Office).

[33] *Id.* at 5. The Department of Homeland Security is not the only agency that has failed to inventory its IT systems. According to OMB, nine of twenty-four agencies surveyed were deficient in this area. OMB 2004 FISMA REPORT, *supra* note 4, at 16.

[34] OMB 2004 FISMA REPORT, *supra* note 4, at 9.

[35] *Id.*

[36] *Id.*

Reprinted with Permission of New York University School of Law

ciencies in their FISMA plans of action.[37] It should come as no surprise, then, that the House Government Reform Committee last year rated government-wide FISMA compliance a "D+,"[38] or that OMB has acknowledged that "much work remains" to be done.[39] An agency-by-agency assessment is beyond the scope of this Note; however, through the examination of the following case study on agency (non)compliance with FISMA, I hope to provide a window of analysis into the government's failure to protect its data.

Only one federal case has evaluated an agency's compliance with FISMA.[40] In *Cobell v. Norton*,[41] the plaintiffs were beneficiaries of Individual Indian Money Trusts (IIMT) managed and administered by the Department of the Interior (DOI), serving as trustee.[42] Alleging that DOI had breached its fiduciary duty by failing to protect sensitive trust data from unauthorized external access,[43] plaintiffs sought and won an injunction requiring DOI to disconnect all IIMT computers from the Internet.[44] Their concern was that so long as their data was inadequately safeguarded, outside parties could gain access to sensitive and personal financial and banking records.[45]

The court's findings reveal an agency unwilling or unable to take the necessary steps to secure information systems from intrusion. Judge Lamberth was "alarmed and disturbed" by DOI's failures and the resulting vulnerability of plaintiffs' sensitive data.[46] For example,

---

[37] *Id.* at 6.

[38] HOUSE COMM. ON GOV'T REFORM,109TH CONG., COMPUTER SECURITY REPORT CARD 1 (2006), *available at* http://reform.house.gov/UploadedFiles/Federal%20Computer%20Security%20Report%20Card%20-%202005.pdf.

[39] OMB 2004 FISMA REPORT, *supra* note 4, at iv.

[40] I performed a search on LexisNexis of all federal court cases using the term "FISMA." Two cases appeared: *Cobell v. Norton*, 394 F. Supp. 2d 164 (D.D.C. 2005), discussed *infra*, and *Connecticut ex rel. Blumenthal v. Crotty*, 180 F. Supp. 2d 392 (N.D.N.Y. 2001), a case that addresses the Fishers Island Special Management Area, another FISMA altogether. *Id.* at 395.

[41] 394 F. Supp. 2d 164.

[42] *Id.* at 165.

[43] *Id.* at 275.

[44] *Id.* at 276–77.

[45] *Id.* at 273. It should be noted that FISMA does not explicitly confer a private cause of action; instead, the suit in *Cobell* was for breach of fiduciary duty. The court in *Cobell* considered noncompliance with FISMA as evidence of a failure of the Department of the Interior (DOI) to secure IIMT data in breach of its fiduciary duty to the Native American plaintiffs. *See id.* at 170 ("The [FISMA] requirements reviewed herein are not at issue on the present motion, but they provide the only available baseline standard for government IT security against which to measure Interior's accomplishments in that arena."). Nevertheless, the court's lengthy and detailed account of DOI's efforts provides important and rare insight into how agencies are approaching the information security problem. *See infra* notes 47–49 and accompanying text.

[46] *Cobell*, 394 F. Supp. 2d at 165 (internal quotation marks omitted).

Reprinted with Permission of New York University School of Law

the court found that "*no effort* was made by [Bureau of Land Management] administrators to restrict, block, or deny access from the source" of repeated test attacks on their systems.[47] Similarly, a private contractor hired to assess IT security in DOI's Office of Surface Mining found that its "Intrusion Detection System had not been monitored or reviewed by anyone for approximately forty-five days and that an additional system was connected to the Internet for twenty-six days with no Intrusion Detection System implemented at all."[48]

Perhaps most disturbing was the court's finding that even among those systems that DOI had certified as FISMA-compliant, substantial security weaknesses remained. In granting the injunction, Judge Lamberth noted with disapproval "numerous vulnerabilities that called into question Interior's IT security-related certifications to the Court."[49] This strongly suggests that the self-reporting on which FISMA depends may be an unreliable means of ensuring compliance. DOI reported to OMB in 2004 that eighty-three percent of its systems were protected by "Effective Security and Privacy Controls."[50] Yet *Cobell* casts serious doubt on this assertion. And while hard data is scarce, it seems likely that if the only federal agency to be reviewed in court has failed to meet its obligations, others might have as well.

Beyond system-specific failures, the court described a bureaucratic culture marked by indifference, confusion, and lack of accountability. In one exemplary passage, the court noted the "stunning lack of management and oversight of IITD [Individual Indian Trust Data] in the context of the departmental IT security program."[51] While DOI technicians were aware of the scope of the problem, they made no effort to fix it. As the court wrote:

> [A]lthough the importance of segregating IITD has been emphasized by this Court and others for more than four years, Interior's IT security planners have discussed segregation "only in concept. . . . [One DOI senior official noted he was] just not aware that we've actually put it down into a formalized, written plan."[52]

Of course, if the threat of litigation is not enough to force DOI into compliance with its FISMA obligations, it is reasonable to doubt compliance in other, less scrutinized areas as well. Indeed, it is fair to expect that this brand of administrative paralysis holds even more

---

47 *Id.* at 167 (emphasis added) (internal quotation marks omitted).

48 *Id.* (internal quotation marks omitted).

49 *Id.*

50 OMB 2004 FISMA REPORT, *supra* note 4, at 23.

51 394 F. Supp. 2d at 261.

52 *Id.* (quoting trial testimony of W. Hord Tipton, Chief Information Officer, DOI).

Reprinted with Permission of New York University School of Law

strongly when no third party has a substantial direct interest in the government's information security.

B. An Inefficient Response

Even when agencies and their employees fully strive to comply with their information security obligations, portions of FISMA are drafted so ambiguously that it is difficult to know exactly what constitutes those obligations. FISMA's treatment of information systems operated by private contractors presents one such ambiguity. FISMA applies not only to information systems managed by federal agencies, but also to those "systems used or operated . . . by a contractor of an agency or other organization on behalf of an agency."[53] In other words, the legislation requires agencies in certain situations to ensure the security of federal data maintained on third-party systems. Yet the scope of this obligation (i.e., when third-party systems are used or operated "on behalf of an agency") can be ambiguous.[54] In some instances, FISMA's applicability is clear. For example, a third party who creates and maintains an information system for handling federal data would certainly fall within the framework of FISMA.

But in situations where data originating from a federal agency is merely stored on a preexisting third-party system as part of a standard business arrangement, it is unclear as a matter of statutory interpretation whether Congress meant FISMA to apply.[55] Unfortunately, FISMA creates no mechanism for agencies to clarify such ambiguities. The result can be months (or longer) of inaction as bureaucrats and lawyers at various levels of an agency struggle to interpret a technical statutory scheme with which they may have little familiarity.

---

[53] 44 U.S.C. § 3544(a)(1)(A)(ii) (Supp. II 2004); *see also id.* § 3544(b) ("Each agency shall develop, document, and implement an agencywide information security program . . . to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, *contractor*, or other source . . . .") (emphasis added).

[54] The confusion derives from a scattered and complex legislative history and can be traced back to the congressional reports accompanying the Computer Security Act of 1987 (CSA). *See* H.R. REP. No. 100-153, pt.1, at 23 (1987), *as reprinted in* 1987 U.S.C.C.A.N. 3120, 3138 (discussing in vague terms meaning of "on behalf of" as it appears in CSA, FISMA's predecessor). A full analysis of this legislative history is unnecessary for the purposes of this Note. What is significant is that in the situation described herein, the relevant federal actors were unsure of FISMA's applicability to the third-party systems in question.

[55] The congressional report accompanying FISMA sheds no light on the question—it is written largely in broad terms, with platitudes about the importance of information security. The legislative history in fact shows virtually no congressional focus on the "nitty-gritty" of how the statute is to be implemented. *See generally* H.R. REP. No. 107-787, pt.1, at 76–88 (2002). This paucity of detail supports my ultimate conclusion that FISMA as currently drafted does not provide adequate guidance for agencies and that more centralized authority is required. *See infra* notes 98–103 and accompanying text.

Reprinted with Permission of New York University School of Law

The government-wide "SmartPay" program illustrates how such ambiguity can lead to inefficiency.[56] In 1998, the General Services Administration (GSA) awarded contracts to five U.S. banks, one of which was Citibank, to provide federal government agencies with Visa and MasterCard purchase cards.[57] Under this program, federal agencies select one of these five banks to provide for streamlined procurement services. Agency employees then use the cards to purchase goods or services required for work purposes, including office supplies, computer terminals, and travel and fleet services.[58]

In addition to providing for standard credit and billing services, the GSA contract with Citibank allows participating agencies to access the Citibank Custom Reporting System (CCRS). CCRS is a proprietary database designed by Citibank to allow a client to "analyze transaction data and help prevent fraud, waste, and abuse in its purchase card program."[59] The Department of State (State) uses CCRS to, inter alia, track purchasing patterns, analyze individual employees' spending behavior, and detect fraud.[60]

State's use of CCRS raises important information security questions—most immediately whether FISMA requires that protective measures be taken to secure CCRS and the various data systems on which it operates. The answer is manifestly unclear. Worse, there is no obvious place to look for an answer once a close reading of FISMA and its legislative history has borne no fruit. The result may well be an agency sincerely interested in complying with its security obligations but unable to reach a conclusion as to what exactly those obligations are.

The confusion over FISMA's applicability in the contractor context is underscored by a recent Government Accountability Office (GAO) report on data mining and privacy that discusses the Citibank-State relationship.[61] The report notes that because "State uses an

---

[56] For a wealth of information on the SmartPay program, see United States General Services Administration, GSA SmartPay, http://www.gsa.gov/smartpay (last visited Aug. 25, 2006).

[57] The other four banks are Bank of America, Bank One (now J.P. Morgan Chase), Mellon Bank, and U.S. Bank. *Id.*

[58] *Id.*

[59] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-05-866, DATA MINING: AGENCIES HAVE TAKEN KEY STEPS TO PROTECT PRIVACY IN SELECTED EFFORTS, BUT SIGNIFICANT COMPLIANCE ISSUES REMAIN 44 (2005), *available at* http://www.gao.gov/new.items/d05866.pdf [hereinafter DATA MINING].

[60] *Id.* At all times, the purchasing data is under Citibank control on Citibank servers. State played no role in the development of CCRS. It merely opted to use Citibank and CCRS once they had been preapproved by GSA on behalf of the agency community. *See id.* at 44–49.

[61] *Id.* at 23, 44–49, 71–74.

Reprinted with Permission of New York University School of Law

information system operated by Citibank . . . , FISMA requires that State ensure that Citibank's system complies with FISMA provisions."[62] This seemingly unambiguous statement is considerably muddied, however, by the rest of the report. First, GAO also argues that as "the contracting agency for the governmentwide purchase card program, GSA is responsible for ensuring that information and information systems used in the program—including those provided by contractors—follow FISMA guidance."[63] Thus, it is at best unclear whether FISMA responsibilities (to the extent they exist at all with respect to CCRS) fall to State or GSA, neither, or both.[64] The two statements, made on the very same page, arguably contradict each other.

Second, in its list of final recommendations, GAO makes no suggestion that State take further steps to apply FISMA's safeguards to CCRS,[65] even though State had not "specifically evaluate[d] Citibank's compliance with federal security requirements."[66] Indeed, in its official comments to the report, State noted its appreciation that GAO had "not made any recommendations about the Department's compliance with [FISMA] vis-à-vis the Citibank purchase card. *It is not clear that FISMA necessarily applies to the Citibank system.*"[67]

State's comments, combined with the main report's ambiguous treatment of FISMA's applicability, suggest that FISMA's scope in the contractor context is very much an open question. Neither GSA[68] nor State has subjected CCRS to FISMA's procedures. GAO, the investigatory arm of Congress, seems to think FISMA applies to CCRS but has declined to suggest firmly that anyone has responsibility to implement it. And OMB, the overseer of FISMA implementation, has so far remained silent on the issue, at least in public reports. Thus, four federal entities appear to remain quite unsure of what FISMA actually requires.

In gauging its FISMA responsibilities with regard to CCRS, State is thus likely to face a classic Hobson's choice. If it decides to "play it safe" and determine that FISMA does apply to CCRS, it will face a costly and potentially contentious effort to intrude on proprietary sys-

---

62 *Id.* at 23.

63 *Id.*

64 For more on the prospect of inefficient redundant tasking, see *infra* note 72 and accompanying text.

65 DATA MINING, *supra* note 59, at 30 (offering only one recommendation—unrelated to FISMA's application to CCRS— to Secretary of State).

66 *Id.* at 23.

67 *Id.* at 72 (emphasis added).

68 *Id.* at 23 ("GSA has not evaluated vendors' systems for compliance with the specific provisions of FISMA.").

Reprinted with Permission of New York University School of Law

tems operated not just for State, but for thousands of private Citibank clients as well.[69] But if State fails to take protective action, it might well be rebuked by OMB or Congress and face punitive action. One possible result will be a period of administrative paralysis. The consequences of either course of action are so dramatic that there may be an understandable hesitancy to select one or the other.[70]

Assessing the costs of such indecision depends on whether FISMA is actually meant to apply to CCRS. If it is, longer delays in implementation mean ever-longer exposure to the very security threats FISMA was meant to neutralize back in 2002. If FISMA was never meant to apply to CCRS or similar systems, then State employees may spend valuable time and resources trying to determine as much.

Either outcome is inefficient in two ways. First, as mentioned in the previous paragraph, agencies may divert scarce resources toward determining whether a given information system falls within FISMA's scope. Any statutory scheme will have ambiguities, and courts are generally well-positioned to settle them. FISMA, however, gives rise to no explicit cause of action. Indeed, only one federal case has even

---

[69] Additionally, if FISMA applied to CCRS, there would seem to be no limiting principle to explain why it should not also apply to the systems of every single private entity with which the Department of State does business. For example, would FISMA apply as well to information systems belonging to utilities that provide electricity to State offices? Or to caterers that service State events?

[70] Agencies are often faced with this type of situation, in which all available options lead to unsatisfactory results and administrative paralysis ensues. In one illustrative example, wage regulations for construction jobs in Pennsylvania were in dispute and it was unclear what regulations governed and how they were to be interpreted. Local school boards, which had to complete construction jobs over the summer before the school year commenced, were thus faced with a

> Hobson's choice of sorts. They could utilize prevailing wage rates that had been issued in the past in clear derivation of the statute, but doing so would risk [enormous liability for violations of the governing statutes]. In the alternative, they could wait for the outcome of the [dispute] but this alternative would risk delaying the opening of the school in the fall or the prospect of not doing the necessary construction at all. The administrative process of issuing prevailing wage rates by the Department of Labor and Industry came to a halt, thereby paralyzing the construction [process].

Jarad Handelman, *Labor & Employment:* Dilucente Corp. v. Pennsylvania Prevailing Wage Appeals Board*: The Commonwealth Court Champions the Rights of Pennsylvania Workers*, *Annual Survey of Pennsylvania Administrative Law*, *Survey of Selected Court Decisions*, 7 WIDENER J. PUB. L. 643, 647–48 n.32 (1998); *see also* Kenneth M. Murchison, *Recent Changes in Procedures of the Department of Environmental Quality*, 57 LA. L. REV. 855, 877–78 (1997) (observing dilemma faced by Louisiana Department of Environmental Quality and describing "a Hobson's choice: either use the limited agency resources to focus administratively on the problems that outsiders regard as most important, or lose the presumption of administrative regularity . . . in defending a judicial action for a declaratory judgment").

Reprinted with Permission of New York University School of Law

made reference to FISMA.[71] Thus, FISMA is problematic in that ambiguous statutory provisions can conceivably maintain their ambiguity indefinitely. Given the absence of a judicial clarification mechanism, the lack of clear executive authority to handle agency questions only exacerbates the problem of administrative paralysis, delay, and wasted hours.

The second source of inefficiency arises from a separate, though related, ambiguity: Assuming, arguendo, that FISMA applies to CCRS, it is an open question whether the burden of compliance should fall to State as the end user or to GSA as the federal entity that negotiated the SmartPay agreements on behalf of the agency community. Unfortunately, Congress apparently never contemplated contractual arrangements where individual agencies utilize IT services made available to the broader agency community as a whole, so the legislative history is unhelpful.

Needless to say, requiring each individual agency to perform such security evaluations would be tremendously wasteful and burdensome to all parties involved. For one, agencies would perform gratuitously duplicative work. If twelve agencies used Citibank under the SmartPay program, twelve separate IT teams would be responsible for evaluating the security fitness of the same IT system. While there may, as a theoretical matter, be some benefit to redundant tasking for important government work, overlapping responsibilities of this sort are inefficient and arbitrarily determined.[72]

---

[71] Cobell v. Norton, 394 F. Supp. 2d 164 (D.D.C. 2005). As previously explained, FISMA was not directly at issue in *Cobell*. Rather, the district court looked to DOI's FISMA record as a baseline to evaluate compliance with its fiduciary duty to protect information systems on behalf of various trust recipients. *See supra* notes 43–45 and accompanying text.

[72] There are some situations in which an objective may be so important that it is prudent to engage in duplicative action to ensure that the objective is achieved in case one actor fails in its mission. For example, the U.S. government employs redundancy to "manage hazardous technologies" such as nuclear weapons systems and the air traffic control network. Scott D. Sagan, *The Problem of Redundancy Problem: Why More Nuclear Security Forces May Produce Less Nuclear Security*, 24 RISK ANALYSIS 935, 936–37 (2004); *see also* Martin Landau, *Redundancy, Rationality, and the Problem of Duplication and Overlap*, 29 PUB. ADMIN. REV. 346–58 (1969). However, the present case is considerably different from those just mentioned. First, redundancy programs are largely designed to compensate for mechanical failures in complex technological systems. There is no such risk here. The task FISMA mandates—formulating a plan for complete information security—is initiated not by software or circuitry, but by agency employees following a legislative plan. Second, to the extent duplicative tasking is beneficial, optimum levels of redundancy should be established ex ante and then implemented accordingly. If FISMA requires each participating agency to secure CCRS, levels of redundancy will grow in proportion to the number of agencies that choose to select Citibank for their purchasing programs. This haphazard and somewhat random framework seems out of line with governmental best practices.

Reprinted with Permission of New York University School of Law

As a matter of policy, it makes great sense that FISMA's requirements should fall to GSA. First, it is vastly more efficient to administer a single security program for CCRS, as opposed to having each participating agency expend resources pursuing an identical course. Second, if each agency utilizing CCRS administers FISMA's requirements, Citibank would potentially be subject to various and even conflicting requests from different agencies to bring its systems into compliance. This could lead to diminished quality of service or strained relations with the various agencies. Far easier for streamlined operation of CCRS would be to have GSA, as the signatory to the master contracts, administer the various FISMA requirements on behalf of the agency community. However, the text and legislative history of FISMA do not necessarily compel such a result.

III
EXPLAINING THE FAILURES

In Part II, I demonstrated how agencies have struggled to implement FISMA and to secure crucial data that drive U.S. government operations. In this Part, I attempt to explain *why* implementation has taken such a slow and ineffectual path. Some of my observations are based on institutional realities that inhere in all bureaucratic systems. Others focus on what I perceive to be deficiencies and omissions specific to the legislative scheme created by Congress. By identifying FISMA's problems and their root causes, I hope to lay a foundation for targeted proposals to reform federal information security policy.

Agency employees have little reason to care about FISMA and its sound implementation. Of course, FISMA carries the force of law, which should theoretically compel federal agencies to carry out its prescriptions diligently. Yet it is well recognized that bureaucrats are human beings with human shortcomings and that their behavior is often shaped by considerations of self-interest.[73] When it comes to carrying out FISMA's dictates, agency employees have precious little incentive to pursue an energetic and thorough course. Inertia holds powerful sway for those who would sooner cling to the familiar status

[73] *See generally* William H. Riker, *Political Science and Rational Choice*, *in* PERSPECTIVES IN POLITICAL ECONOMY (James E. Alt & Kenneth A. Shepsle eds., 1990) (discussing rational choice theory and considering private motivations of public employees); Edella Schlager & William Blomquist, *A Comparison of Three Emerging Theories of the Public Policy Process*, 49 POL. RES. Q. 651 (1996) (same); Diane Vaughan, *Rational Choice, Situated Action, and the Social Control of Organizations*, 32 LAW & SOC'Y REV. 23 (1998) (same). *But see* John D. DiIulio, Jr., *Principled Agents: The Cultural Bases of Behavior in a Federal Government Bureaucracy*, 4 J. PUB. ADMIN. RES. & THEORY 277, 282, 318 (1994) (positing that many bureaucrats are driven primarily by motivation to serve public interest).

Reprinted with Permission of New York University School of Law

quo than the unknown and time-consuming tasks that FISMA demands.

A. An Unfunded Mandate

FISMA does not directly bring new funding to the agencies. So, while agencies must perform more work—often with the assistance of costly private contractors—they must effectively do so within the constraints of their preexisting budgets. For bureaus that already consider themselves strapped for cash, these new tasks may foster reluctance towards implementation, and perhaps even resentment aimed at those ordering the new work to be performed.[74] Indeed, the *Cobell* court described how DOI Inspector General Earl Devaney viewed FISMA as "sort of an unfunded mandate that IGs do this work without the resources to accompany it."[75] The result, according to the court, was action "more limited in scope" than what FISMA demands.[76]

B. Unglamorous Work

Compounding the difficulty that arises from funding constraints is the reality that most agency employees likely view FISMA work as "unsexy." Workers are more motivated and productive when they feel their work has a worthwhile purpose.[77] Yet information security is a functionalist objective with no direct connection to substantive policy goals, so one might easily imagine that some agency employees lack a sense that FISMA work is urgent or even particularly important. Securing databases from intrusion *is* important work, but it is unlikely to make for bold headlines in the day's news cycle.[78] Accord-

---

[74] It is well-established that funding levels play a major role in shaping agency behavior and in determining how quickly and effectively programs are implemented. *See* Janet Kelly, *Unfunded Mandates: The View from the States*, 54 PUB. ADMIN. REV. 405, 405–08 (1994) (discussing state agencies and observing problems of compliance resulting from insufficient funding). *See generally* COPING WITH MANDATES: WHAT ARE THE ALTERNATIVES? (Michael Fix & Daphne A. Kenyon eds., 1990) (same).

[75] *Cobell*, 394 F. Supp. 2d at 185 (internal quotation marks omitted).

[76] *Id.*

[77] *See generally* L.L. CUMMINGS & DONALD P. SCHWAB, PERFORMANCE IN ORGANIZATIONS: DETERMINANTS AND APPRAISALS 90–101 (1973) (describing importance of employee motivation in organizational productivity).

[78] Other authors have observed that when a problem does not receive substantial attention in the media, progress in tackling that problem becomes much more difficult to achieve. *See, e.g.*, Robert B. Charles, *Back to the Future: The Collapse of National Drug Control Policy and a Blueprint for Revitalizing the Nation's Counternarcotics Efforts*, 33 HARV. J. ON LEGIS. 339, 357–58 (1996) ("[T]he difficulties of reducing drug use have been exacerbated by the fact that the drug issue has fallen into relative obscurity since the late 1980s. Objective indicators . . . reveal lower interest than at any other time in recent history."); *see also* Lee A. Kimball, *Institutions for the Earth: Sources of Effective Interna-*

Reprinted with Permission of New York University School of Law

ingly, bureaucrats will likely view FISMA tasks as work they *have* to do, but do not necessarily *want* to do. Under such conditions, inertia can easily overpower the impetus to make costly changes. By this logic, it is reasonable to believe that agency employees will seek to minimize the amount of FISMA work they must do.[79] When FISMA is ambiguous about what agencies must do in a given situation—or whether they should do anything at all—there is every incentive for agencies to adopt the narrower and less demanding interpretation.

C. *A Disinterested Public*

Another possible reason for FISMA's disappointingly slow implementation is institutional and specific to the nature of the task: The public as a whole is unlikely to be particularly concerned with agency compliance. As mentioned before, information security is not a substantive public policy goal in the traditional sense of, say, providing healthcare or keeping rivers clean. Rather, it stems from a functionalist aspiration to make government work better from the inside. Taxpayers may have a general interest in streamlined, functional government, but that concern is abstract and unlikely to trigger particularly deep engagement. Very few citizens have any particular, personal stake in FISMA compliance. Interest groups might apply political pressure for agencies to comply with FISMA if they feel their welfare is at stake,[80] but there is no reason in most cases to expect such external pressure.[81] It may be that a security breach of enormous

tional Environmental Protection, 90 AM. J. INT'L L. 701, 701 (1996) (book review) (noting that "forums that create embarrassing public exposure for a government, such as . . . media attention, can bring about policy change" and renewed attention to problems).

[79] One school of administrative theory posits that when agency employees are given substantial discretion in how to perform their duties, they may seek to minimize the amount of work they must do. *See* WILLIAM A. NISKANEN, BUREAUCRACY AND REPRESENTATIVE GOVERNMENT 36–42 (1973) (stating that some bureaucrats make decisions based on personal welfare, including desire to minimize workloads); Steven L. Schooner, *Fear of Oversight: The Fundamental Failure of Businesslike Government*, 50 AM. U. L. REV. 627, 674–75 n.152 (2001) ("[B]ureaucrats might use discretion to further personal goals such as . . . minimizing their own workload . . . ." (quoting William P. Rogerson, *Economic Incentives and the Defense Procurement Process*, 8 J. ECON. PERSP. 65, 86 (1994)).

[80] *See generally* GLEN O. ROBINSON, AMERICAN BUREAUCRACY: PUBLIC CHOICE AND PUBLIC LAW 87–95 (1991) (explaining that regulations are promulgated in response to influence of powerful interest groups seeking to further their own individual interests, regardless of consequences for aggregate social welfare).

[81] The facts presented by the *Cobell* litigation present an exception to this general proposition. In *Cobell*, 394 F. Supp. 2d 164, the plaintiffs had a personal stake in DOI's security compliance because DOI was using government systems to maintain sensitive private trust data. *See supra* text accompanying notes 41–45. But the vast majority of systems covered by FISMA will be used primarily for governmental functions that do not have specific private-sector "clients" like the *Cobell* plaintiffs.

Reprinted with Permission of New York University School of Law

proportions could trigger widespread citizen outrage and attention to the information security problem.[82] Until this happens, however, public interest is likely to remain relatively low.

The lack of public interest in FISMA compliance can create complacency within Congress as well. One can fairly assume that members of Congress field few constituent inquiries about the pace of FISMA implementation. And they almost certainly do not believe their re-election prospects are in any way tied to whether agency CIOs and IGs successfully detect firewall breaches or susceptibility to "Trojan Horse" viruses.[83] These realities explain why congressional oversight of information security is so lackluster.

Congressional oversight can be crucial to ensuring that agencies comply with their statutory mandates.[84] In their classic article on congressional oversight of the administrative state, Professors Mathew McCubbins and Thomas Schwartz distinguish between "police patrol" oversight, where the legislature continuously monitors administrative activity and "fire alarm" oversight, where the legislature waits for interested parties to sound alarms before springing into action.[85] The authors find the latter paradigm to be much more common.[86] Thus, until interested third parties exert pressure on Congress to step up FISMA oversight, we should not expect substantial legislative involvement in the realm of information security.[87] Yet as this section has

---

[82] If, for example, all IRS data were lost and citizens were required to resubmit their annual tax filings, it is very likely the issue would come out of the shadows.

[83] While citizens are entitled to cast ballots based on any criteria they choose, many issues are considered so peripheral and receive so little popular attention that it seems highly unlikely they will influence voting patterns in congressional elections. *See* Jack M. Beermann, Essay, *Administrative Failure and Local Democracy: The Politics of* DeShaney, 1990 DUKE L.J. 1078, 1105 ("[A]dministrative failures may be so low on the political agenda that they will not even be addressed in the electoral process."). It seems fair to assume that compliance with FISMA is fairly low on the totem poll of public interest. *See* Peter H.A. Lehner, Note, *Judicial Review of Administrative Inaction*, 83 COLUM. L. REV. 627, 639 (1983).

> The impact of nonimplementation is usually diffuse and uncertain, so that those harmed will rarely have the incentive to seek political remedies and will often lack the clout needed to obtain them. Congress is too distant from administrative decisionmaking and too unwieldy an institution to respond effectively to agency nonimplementation. Generally, Congress acts only where a widespread problem is perceived. Furthermore, a congressman seldom has an incentive to make the enormous effort needed to get Congress to redirect an agency's implementation policy.

Id.

[84] *See* Mathew D. McCubbins & Thomas Schwartz, *Congressional Oversight Overlooked: Police Patrols Versus Fire Alarms*, 28 AM. J. POL. SCI. 165, 165–66, 176 (1984).

[85] *Id.*

[86] *Id.*

[87] *See* Lehner, *supra* note 83, at 639 n.82.

Reprinted with Permission of New York University School of Law

demonstrated, the public currently seems uninterested in FISMA implementation. A catastrophic security event might change this attitude, but until then, Congress will be unlikely to provide the impetus for administrative action.

D. A Deficit of Accountability and Oversight

Between public apathy and congressional inattentiveness, agencies receive far less scrutiny of their FISMA progress than they do for work considered core to their missions. This relative lack of oversight means bureaucrats have more leeway to make choices and take action (or decline to act).[88] In short, there is a serious accountability gap. Yet, if agencies and their employees fail to implement FISMA as they should, who will hold them accountable if not the public or Congress? OMB alone is tasked with this supervisory function. Yet agencies may have little to fear from OMB under the current regulatory scheme.

Under FISMA, the Director of OMB possesses a non-exhaustive list of tools for "enforc[ing] accountability."[89] Perhaps the most significant is the authority to downwardly adjust an agency's budget request for IT or, once funds have already been appropriated by Congress, to cause some or even all of these funds to be withheld.[90] No agency director would relish such a punishment.

In fact, the nature of the stick is so draconian and counterproductive to agency effectiveness that it is hard to imagine OMB ever fully imposing it. Leveraging IT has led to dramatic improvements in governmental efficiency and capabilities. Punishing an agency by retarding its ability to take advantage of IT sounds a bit like—to use the old expression—cutting off your nose to spite your face. Furthermore, so many agencies are delinquent in their FISMA obligations[91] that a "safety in numbers" mentality may begin to take hold. Even if OMB would consider withholding IT funding for one or two deviant bureaus, the current environment—in which nearly every major federal agency has work left to do[92]—would make mass punishment both politically inconceivable and functionally disastrous. This effectively neutralizes any threat that OMB would use this sanction.

---

88 *See* Beermann, *supra* note 83, at 1106 ("[U]nelected agents are shielded from direct political scrutiny. Thus, given the difficulty of effective oversight, agency actions may not be brought into line with legislatively stated goals.").

89 *See supra* notes 22–23 and accompanying text.

90 40 U.S.C. § 11303(b)(5)(B)(i)–(iii) (Supp. II 2004).

91 OMB 2004 FISMA REPORT, *supra* note 4, at 23–46 (showing that of twenty-four major agencies surveyed, twenty-two had not yet substantially completed their FISMA obligations).

92 *Id.* at iv.

Reprinted with Permission of New York University School of Law

Alternatively, OMB has the authority to "designat[e] for [an] executive agency an executive agent to contract with private sector sources for the performance of information resources management," such as FISMA compliance.[93] In other words, if an agency is not doing its job properly, OMB can appoint someone who will. Whether this authority will encourage FISMA compliance is unclear. It is possible that some agency CIOs or IGs would resent such an infringement on their portfolios and would accordingly strive to comply with FISMA to avoid this outcome. Yet for many agency heads or overworked and underfunded CIOs, such "punishment" might come as welcome relief from a task that no one was excited about performing in the first place.

Finally, a word is in order about the personnel structure Congress created to ensure FISMA compliance. Generally speaking, as more layers of hierarchy are added to a bureaucracy, accountability and effectiveness diminish.[94] When a job is done well, it is unclear who should receive the credit. And more importantly for this Note, when a job is done poorly it is unclear whom to blame.

FISMA vests degrees of responsibility in at least four individuals within each agency: the agency head herself; the agency IG and CIO; and the agency CIO's specially designated assistant for FISMA.[95] This means that in any given agency at least four senior executives share FISMA oversight responsibility, supervising the employees who will actually execute the testing and programming that FISMA demands. This kind of overlapping and duplicative responsibility breeds the administrative inertia and complacency for which bureaucracies are (in)famous.[96] Indeed, the *Cobell* court was at a loss to explain why or on whose watch DOI had failed so utterly in securing the Indian Trust servers; all that was clear was the failure itself, making ameliorative measures all the more difficult to devise and implement.

This much is clear: Agencies lack the incentive to implement FISMA vigorously in the way that Congress, OMB, and now even the

---

[93] 40 U.S.C. § 11303(b)(5)(B)(iv).

[94] *See* PAUL C. LIGHT, THICKENING GOVERNMENT: FEDERAL HIERARCHY AND THE DIFFUSION OF ACCOUNTABILITY 64 (1995) (arguing that link between thickening government and diffusion of accountability expresses itself in associated costs including information distortion, administrative inertia, and disunity of command).

[95] *See* 44 U.S.C. § 3544(a)(3)(A)(i) (Supp. II 2004) ("The head of each agency shall delegate to the agency Chief Information Officer the authority to . . . designat[e] a senior agency information security officer who shall carry out the Chief Information Officer's responsibilities under this section.").

[96] *See generally* LIGHT, *supra* note 94 (discussing development of and problems associated with growing layers of management in government agencies).

Reprinted with Permission of New York University School of Law

courts, envision. This failure can be attributed to a number of causes. Congress and the public largely fail to apply pressure. OMB has means at its disposal to enforce compliance, but those means are either so draconian or so toothless that agencies likely do not take them seriously. Agency employees themselves view FISMA responsibilities as mundane work—and *unfunded* mundane work at that.

I have now problematized the FISMA scheme, demonstrating what agencies are doing wrong and why. In Part IV I propose a series of reforms to address these shortcomings.

IV
Some Proposed Solutions

To achieve the goal of agencywide information security, it is vital to assess the shortcomings of the current program. Equally important is the more constructive task of formulating innovative solutions to tackle—or at least mitigate—these shortcomings. Accordingly, in this section, I propose five reforms to the FISMA legislative scheme.

Some of the problems outlined in Part III result from statutory ambiguity, which Congress can readily address through clarifying legislation. Other problems, however, stem from FISMA's structural design, resulting in perverse incentives and a lack of accountability. There is no "silver bullet" to eliminate these institutional deficiencies. Nevertheless, structural measures that bolster oversight and shift responsibility to those with proper incentives may help mitigate the administrative sclerosis that has plagued FISMA during its first four years.

A. Coordinate from the Top: A Federal Information Security Czar

Perhaps the most fundamental lesson to emerge from the FISMA experience is the error of casting agencies off on their own in the expectation that they will take the necessary measures to keep their data secure. Oversight is a must, and it is not coming from Congress, the public, or the courts. OMB reviews annual reports—some of them damning—but a laissez-faire attitude seems to prevail.

To ensure agency compliance with FISMA, Congress should amend FISMA to create a position within OMB to oversee all federal information security planning: an Information Security Czar (ISC) with full interpretive authority to direct the scope and manner of agency implementation.

The impact of such a position would be both symbolic and functional. Symbolically, it would signal to agency heads, Chief Information Officers, and Inspectors General that Congress takes this matter

Reprinted with Permission of New York University School of Law

seriously. It will help dispel any illusion, apparently common throughout the agency community, that agencies may implement FISMA if and when they feel they can accommodate it. And it will breathe the fresh air of congressional action into an aging legislative scheme that seems to be losing its sense of urgency.

More importantly, the ISC could serve invaluable functional purposes. First, the ISC would be authorized by statute to exercise oversight over federal agencies by monitoring their compliance with FISMA.[97] If an agency were delinquent in its responsibilities, the ISC could order it to change tactics or to reallocate resources as necessary. Of course, the ISC should exercise this power judiciously, and the actions of the ISC should be subject to review by the Director of OMB. But the key point is that external oversight would come into play throughout the entire process and parties would not have to look to the courts (as they did in *Cobell*) as a first resort to enforce FISMA's various mandates.

Moreover, when an agency is uncertain about the scope of its FISMA obligations, the ISC could provide answers. In the current FISMA scheme, agencies are left largely to their own devices to resolve ambiguities. Recall, for example, the uncertainty facing the State Department and GSA as to whether FISMA applies to Citibank's purchasing card systems.[98] Were Congress to create an ISC, State's employees would have an immediate point of contact to settle the question, thus saving considerable time and resources in trying to answer the question themselves. Additionally, an ISC would presumably have no hidden incentives to avoid more agency work. One might therefore expect more impartial responses than when the agencies police themselves.

The ISC would also serve an important standardization function. If an ambiguity arose in one agency, the ISC could issue direction not only to that agency, but to all others as well. Thus, FISMA would be

---

[97] Scholars surveying other public policy goals have suggested that centralized "czar" positions can be very effective at increasing accountability and improving government performance. One such prominent position is that of the federal "Drug Czar":

> The White House Drug Czar should be the chief voice within the Administration on whether counter-narcotics programs continue to be funded or not, and at what levels, in consultation with OMB and the appropriations committees. In all anti-drug efforts, the Drug Czar—and not individual agency heads—should be viewed by OMB and Congress as the primary decision-maker. To achieve this goal, the President must be unequivocal, vocal and constant in his support of the Drug Czar, and should delegate to him or her the fullest authority possible, within the bounds of the law, on all issues relating to the nation's counter-narcotics efforts.

Charles, *supra* note 78, at 404.

[98] *See supra* Part II.B.

Reprinted with Permission of New York University School of Law

implemented consistently across the agency community. Even without specific queries, the ISC would be ideally situated to survey the various agencies' efforts toward FISMA compliance. The ISC could accordingly issue best practices guidelines to agencies to apprise them of which methods work and which do not.[99]

Lastly, the ISC should have the authority—subject to review by the Director of OMB—to settle FISMA-related disputes between agencies. This authority would enable the ISC to assign responsibilities with an eye towards efficiency when two or more agencies utilize a given information system. Consider again the Citibank SmartPay example. If FISMA were held to apply, it would make far more sense for GSA to bear the burden of compliance than for each agency contracting with Citibank to do so independently.[100] Yet under the current system, there is no guarantee that GSA would undertake this significant task. The ISC, as a centralized authority with no self-interested bureaucratic stake in the issue, would be well positioned to assign responsibility in a sensible, cost-effective manner.

Of course, critics might respond that a new Czar position would simply pile on one more layer of bureacracy and do little to advance FISMA compliance at the agency level. Or worse, the position might even diminish accountability by taking responsibility out of the hands of the individual agencies and placing it elsewhere. Indeed, as noted above, some have argued forcefully that when administrative hierarchies expand, accountability tends to diffuse as it becomes difficult to assign credit or blame.[101]

There may be some merit to this critique, but an ISC would nevertheless serve invaluable standardization and clarification functions. Weighing the costs and benefits of this new position thus becomes a theoretical exercise in approximating the value conferred by these new functions against the resulting diffusion of accountability. It is difficult to assign hard values to such abstract concerns. To mitigate any accountability costs, however, one might pare down the responsibilities of the ISC office so that it focuses less on active, ongoing oversight and more on responsive problem solving. That is, the ISC could concentrate less on monitoring agency progress with FISMA compliance, and more on resolving inter-agency disputes and statutory ambi-

---

[99] For a detailed article discussing the increasing popularity of regulatory governance through best practices, see generally David Zaring, *Best Practices*, 81 N.Y.U. L. REV. 294 (2006).

[100] *See supra* note 72 and accompanying text.

[101] *See* LIGHT, *supra* note 94, at 86–87 (noting that as bureaucracies expand, it becomes difficult to assign blame when things go wrong and credit when things go right; therefore, accountability diminishes and agency performance suffers).

Reprinted with Permission of New York University School of Law

guities as they arise on an ad hoc basis. Such a middle-ground arrangement would help dispel fears about another layer of bureaucratic oversight while also clarifying uncertainties efficiently and expeditiously.

Other critics might argue that creating a new position within OMB does not go far enough; instead, Congress should create an entirely new agency to manage federal information security. Such a dramatic step, however, is unwarranted. OMB is uniquely positioned to manage agencies—indeed, managing agencies and considering their competing demands is OMB's raison d'etre.[102] Given the tasks the ISC would perform (e.g., oversight, standardization, and mediating claims between agencies), it makes great sense to locate this office within the larger management enterprise of OMB.

Moreover, an entirely new agency would come with two distinct costs. The first cost is financial: Creating new agencies requires enormous financial commitments that Congress may not be prepared to stomach. In contrast, merely creating a new office within an existing agency would not require the significant overhead and startup costs that a newly-created organization entails.

The second cost comes from a loss of administrative simplicity and experience. OMB is already tasked with implementing FISMA, in addition to the myriad other oversight functions it performs for the federal administrative state. Internal government management is OMB's forte, and there is no reason to give up this expertise by vesting oversight in a new agency. An ISC within OMB could bring targeted focus to the information security problem without losing the structure and experience that OMB already brings to the table.

B. Trade in That Stick for a Carrot

One of the problems identified in Part III was that OMB has yet to develop an effective and realistic mechanism for enforcing FISMA

---

[102] *See* Office of Mgmt. and Budget, OMB's Mission, http://www.whitehouse.gov/omb/organization/role.html (last visited June 4, 2006).

> OMB's predominant mission is to assist the President in overseeing the preparation of the federal budget and to supervise its administration in Executive Branch agencies. . . . OMB evaluates the effectiveness of agency programs, policies, and procedures, assesses competing funding demands among agencies, and sets funding priorities. . . . OMB's role is to help improve administrative management, to develop better performance measures and coordinating mechanisms, and to reduce any unnecessary burdens on the public.

Id. For a detailed analysis of the inner workings of OMB, see generally SHELLEY LYNNE TOMKIN, INSIDE OMB: POLITICS AND PROCESS IN THE PRESIDENT'S BUDGET OFFICE (1998).

Reprinted with Permission of New York University School of Law

accountability.[103] Cutting off agency IT funding is a dramatic and largely counterproductive measure. For this reason, agency heads probably do not take this threat very seriously, thereby undermining its effectiveness. Accordingly, OMB should formulate new incentives to induce FISMA compliance.[104]

In particular, OMB should utilize positive inducements rather than punitive ones. One solution would be the positive analog to the punitive measure already available: Agencies with exemplary records of FISMA compliance should qualify for *more* IT funding and personnel. That is, agencies whose FISMA compliance surpasses a given threshold, or who demonstrate marked year-over-year improvement, would be rewarded with more resources, or "bonus funds."[105]

Bureaucracies are always hungry for additional funds: If anything could be expected to motivate an agency's CIO, it is the prospect of greater resources at her disposal. Indeed, it is well established in the political science literature that the prospect of more funding can substantially impact an agency's agenda.[106] This incentive could be implemented immediately and with credibility, whereas there is virtu-

---

[103] *See supra* notes 89–94 and accompanying text.

[104] The relevant statutory text contains a list of measures available to OMB, 40 U.S.C. § 11303(b)(5)(B) (Supp. II 2004), but the list is non-exhaustive and also authorizes the Director of OMB to "take any action that the Director considers appropriate . . . to enforce accountability of the head of an executive agency for information resources management . . . ." *Id.* § 11303(b)(5)(A).

[105] One commentator has suggested a similar budgetary bonus as a spur to increased agency compliance in the context of the Electronic Freedom of Information Act (EFOIA), where agencies have largely failed to comply with their statutory obligations. Martin E. Halstuk, *Speed Bumps on the Information Superhighway: A Study of Federal Agency Compliance with the Electronic Freedom of Information Act of 1996*, 5 COMM. L. & POL'Y 423, 465–66 (2000) ("Congress in the EFOIA could have provided positive incentives to encourage agency compliance. The EFOIA, for example, could have allowed agencies that met deadlines to keep a percentage of the money collected in FOIA fees.").

[106] *See* RANDAL O'TOOLE, REFORMING THE FOREST SERVICE 104 (1988) ("For top managers, larger budgets mean greater prestige. For middle managers, larger budgets mean more people on their staff, and this generally provides them with higher salaries. For lower managers, larger budgets mean greater opportunities for advancement."); Jonathan Bendor et al., *Stacking the Deck: Bureaucratic Missions and Policy Design*, 81 AM. POL. SCI. REV. 873, 882, 886 (1987) (noting two prominent models: one hypothesizing "a bureau chief interested only in increasing his agency's appropriations," and another in which bureau chiefs "are interested in both budgets and missions"); Jane C. Murphy & Margaret J. Potthast, *Domestic Violence, Substance Abuse, and Child Welfare: The Legal System's Response*, 3 J. HEALTH CARE L. & POL'Y 88, 98–99 (1999) (noting that prospect of additional funding plays significant role in shaping agency behavior); David W. Sar, *Helping Hands: Aid for Natural Disaster Homeless vs. Aid for "Ordinary Homeless,"* 7 STAN. L. & POL'Y REV. 129, 139 (1995) (same); Lois A. Weithorn, *Protecting Children from Exposure to Domestic Violence: The Use and Abuse of Child Maltreatment Statutes*, 53 HASTINGS L.J. 1, 54 (2001) (same).

Reprinted with Permission of New York University School of Law

ally no chance that OMB would impose punitive sanctions on the dozens of federal agencies currently in noncompliance.[107]

Of course, implementing a positive inducement scheme would require a congressional commitment to increase the agency IT budget. In a political environment where deficit reduction is a priority and budget cuts are common,[108] it is unclear whether the political will exists for such an expansion. That is ultimately a matter for Congress to decide. However, given the importance of information security, and the failures in the current FISMA regime that have been documented in this Note, it would surely be advisable to consider at least a modest appropriation to assess the workability of a positive inducement program.

C. *Institute Surprise Inspections*

OMB should carefully oversee agencies' efforts even after they certify a given system secure. The *Cobell* litigation is a stark reminder that a task may not be completed despite an agency's assurances to the contrary—an agency declaring a system secure does not necessarily make it so.[109] Accordingly, Congress should authorize OMB to launch surprise inspections of agency IT systems.

Surprise inspections have an established pedigree within the federal administrative state. They have been used successfully in several regulatory contexts as a means of enhancing compliance "by increasing the likelihood that violations will be detected."[110] Agencies often utilize surprise inspections to monitor compliance by nongovernmental actors who are subject to federal regulation: For example, they are prominent in such fields as food safety,[111] workplace safety,[112] custody of government property,[113] and environmental regu-

---

[107] Of course, OMB would still maintain the authority to invoke punitive measures against recalcitrant agencies.

[108] *See* Robert Pear, *Domestic Spending Squeezed Throughout the Government*, N.Y. TIMES, Feb. 7, 2006, at A14 (describing recent budget cuts totaling $39 billion and explaining that more cuts are likely).

[109] *See supra* notes 47–50 and accompanying text (noting that significant security breaches were identified in systems that had been certified FISMA-compliant by DOI).

[110] Andrew Chin, *Spoiling the Surprise: Constraints Facing Random Regulatory Inspections in Japan and the United States*, 20 NW. J. INT'L L. & BUS. 99, 102 (1999).

[111] *See, e.g.*, 7 C.F.R. § 301.78-10(c)(2) (2006) (setting out guidelines for irradiation of quarantined fruits and vegetables and calling for "unannounced inspection visits to the [irradiation] facility by an inspector").

[112] *See, e.g.*, 29 C.F.R. § 1960.31(a) (2005) (authorizing Secretary of Labor to conduct "announced or unannounced inspections" of hazardous workplaces when there is reason to doubt compliance by employer).

[113] *See, e.g.*, 41 C.F.R. § 109-27.5105(a) (2005) (authorizing Department of Energy to conduct "[u]nannounced inspections" of contractors storing precious metals).

Reprinted with Permission of New York University School of Law

lation.[114] However, the government can also use surprise inspections to monitor itself. Several classes of federal employees are subject to random drug or alcohol screening, for example.[115] And the military utilizes surprise drills as a way of testing system readiness.[116]

In the FISMA context, OMB technicians could without warning initiate tests, review procedures, and question relevant agency personnel about their work. The specter of such inspections—even if they were relatively rare—would enhance accountability and create strong incentives for agencies to implement FISMA properly and thoroughly. Moreover, it could cause agencies to reassess their initial evaluations, which might catch errors originally overlooked.

One might imagine two potential obstacles to a regime of surprise inspections in the FISMA context, but neither appears insurmountable. First, agencies might be "tipped off" to an oncoming inspection and make adjustments before inspectors arrive.[117] Yet this problem emerges generally from corruption, where unscrupulous regulators accept bribes in return for advance notice.[118] While a firm with private funds at its disposal may be induced to attempt such a scheme, it is unlikely that an agency, whose spending is subject to comprehensive oversight, would do so. Moreover, private firms are profit-maximizing entities that may be shut down entirely if they fail an inspection, so the cost of failing an inspection can be extraordinarily high; federal agencies are not nearly so vulnerable.

A second objection is that, in practice, agencies often do not have the resources necessary to perform surprise inspections frequently enough to modify the behavior of regulated entities.[119] Thus, critics

---

[114] *See, e.g.*, 40 C.F.R. § 55.8 (2005) (authorizing surprise inspections by Environmental Protection Agency).

[115] *See, e.g.*, 10 C.F.R. pt. 26, app. A, 2.1(a)–(c) (2006) (requiring operators of certain nuclear facilities to test employees randomly for drug use); 49 C.F.R. § 219.609 (2005) (mandating random testing for railroad employees).

[116] *See, e.g.*, Matthew Cox, *Surprise Scud Drill Is Very Real for Soldiers*, GANNETT NEWS SERVICE, Mar. 11, 2003, http://www.gannettonline.com/gns/faceoff2/20030311-18084.shtml (detailing surprise drill which tested soldiers' response time to chemical weapons attack).

[117] *See* Chin, *supra* note 110, at 115–17 (noting that Occupational Safety and Health Act and Mine Safety and Health Act criminal provisions prohibiting advance notice of surprise inspection are integral parts of these statutes). The problem of prior notification has also emerged in the context of the Animal Welfare Act, 7 U.S.C. §§ 2131–59 (2000), which seeks to protect certain animals from various forms of inhumane treatment. *See* Carole Lynn Nowicki, Note, *The Animal Welfare Act: All Bark and No Bite*, 23 SETON HALL LEGIS. J. 443, 468 (1999) ("[R]esearch facilities are often given prior notification before inspections occur.").

[118] *See* Chin, *supra* note 110, at 116.

[119] In particular, the Occupational Safety and Health Administration (OSHA) has been cited as having insufficient resources to carry out surprise inspections effectively. *See, e.g.*, Chin, *supra* note 110, at 110 ("[T]he shortage of enforcement resources available to OSHA

Reprinted with Permission of New York University School of Law

argue that they function more as a paper tiger than as an effective inducement to compliance. Given budgetary constraints, it may be true that surprise inspections within any given agency will only occur relatively infrequently. Nevertheless, such a program would not be impotent. OMB separately evaluated twenty-four agencies in its last FISMA report.[120] If OMB subjected each of these agencies to a surprise inspection at least once per year, it is likely that each CIO would take this prospect seriously. Furthermore, it does not seem overly taxing for OMB to conduct twenty-four inspections over the course of a year; OMB can surely conduct two inspections per month given that each target agency is headquartered in Washington, D.C. (The Occupational Safety and Health Administration, on the other hand, must send teams to workplaces across the nation.)[121]

D. Amend FISMA to Avoid Duplicative Work

One narrow but effective reform would be for Congress to amend FISMA so that when multiple agencies utilize a single information system, OMB determines which of them bears responsibility for FISMA implementation. In the SmartPay program case study above, I noted that fundamental principles of efficiency suggest that GSA, as negotiator of the master contracts with Citibank, should bear the burden of FISMA compliance.[122] Yet under the current legislative scheme, nothing dictates such a result.

If OMB had the power to assign FISMA responsibilities in such situations, it could ensure efficient results. It is clearly preferable to have one government agency (GSA) consult with Citibank rather than several or even dozens. OMB—and especially the new information security czar I have proposed[123]—would be well positioned to delegate work in an efficient and fair-minded manner.

E. Leverage the Private Sector

Lastly, if agencies themselves are not getting the information security job done, Congress should find people who will. We have seen that, for a variety of reasons, proper incentives are not in place

---

is longstanding and widely acknowledged, and has had the practical effect of limiting the frequency of surprise inspections by the agency."). Critics have also complained that the Department of Agriculture has been lax in conducting inspections to enforce the Animal Welfare Act. *See* Nowicki, *supra* note 117, at 468 ("Despite [Department of Agriculture] recommendations of four inspections per facility per year, actual statistics show that the agency averaged less than two inspections per facility per year between 1988 and 1992.").

120 OMB 2004 FISMA REPORT, *supra* note 4, at 1.

121 *See* Chin, *supra* note 110, at 111–12.

122 *See supra* Part II.B.

123 *See supra* Part IV.A.

Reprinted with Permission of New York University School of Law

for agency employees to implement FISMA in a timely and rigorous fashion. Congress should accordingly amend FISMA to require that private-sector contractors conduct the requisite initial security testing and appraisals.

Partnerships between administrative agencies and the private sector are increasingly common.[124] They are a manifestation of the ethos of privatization—the idea that private actors can perform certain kinds of "governmental" work better than the government itself. Indeed, FISMA already contemplates a private role in addressing the government information security problem: One explicit purpose of the Act is to "acknowledge that commercially developed information security products offer advanced, dynamic, robust, and effective information security solutions, reflecting market solutions for the protection of critical information infrastructures important to the national defense and economic security of the nation that are designed, built, and operated by the private sector . . . ."[125] In the realm of information security, it may be that profit-seeking IT firms will bring the correct set of incentives to the table. Where bureaucracies avoid work, enterprising firms seek it out and strive to perform well enough to be hired again. Where bureaucracies are quick to declare a job done, private firms look for more work and more fees.

However, Congress should not commission private contractors to complete all agency FISMA work. The cost would be high and the consequences of continuous private management of government IT systems too uncertain. But if contractors were brought in for prelimi-

---

[124] Professor Freeman has written extensively on this development. Notably, she observes that:

> The scope of activities for which government agencies contract with private providers, whether for profit or not, appears moreover to have expanded. Not only do private providers furnish social services such as health care, and fulfill local government responsibilities such as waste collection and road repair; they also increasingly perform such traditionally public functions as prison management.

Jody Freeman, *The Private Role in Public Governance*, 75 N.Y.U. L. REV. 543, 552 (2000); *see also* Jody Freeman, *Collaborative Governance in the Administrative State*, 45 UCLA L. REV. 1, 33–66 (1997) (describing collaborative governance strategies including negotiated rulemaking and permitting); Jody Freeman, *The Contracting State*, 28 FLA. ST. U. L. REV. 155, 164–69 (2000) (noting various types of government contracting and grants to private sector for wide variety of services); Jody Freeman, *Extending Public Law Norms Through Privatization*, 116 HARV. L. REV. 1285, 1310–14 (2003) (discussing economic and public perspectives on benefits of privatization); Philip J. Harter & George C. Eads, *Policy Instruments, Institutions, and Objectives: An Analytical Framework for Assessing "Alternatives" to Regulation*, 37 ADMIN. L. REV. 221, 223–27 (1985) (describing policy instruments—as well as agency and private institutions—that influence firms' decisions regarding resources devoted to assuring health and safety of their workers).

[125] 44 U.S.C. § 3541(5) (Supp. II 2004).

Reprinted with Permission of New York University School of Law

nary diagnostic work, the outcome might be quite appealing. With a mandate to evaluate all systems within a given agency, a contractor would have every incentive to do the work expeditiously rather than letting it drag on. Additionally, contractors would have an incentive to find and identify vulnerabilities quickly, so that they might secure further contracts to fix those problems.[126]

Even if an agency decided to complete the FISMA work on its own, it would have a contractor-generated "roadmap" for how to proceed. This small boost should not be underestimated; the hardest part of any task is often getting started. Once agencies are aware of the flaws in their systems, they cannot claim ignorance of the problem. Accountability would surely be bolstered if CIOs were specifically presented with a list of necessary tasks. When compared with DOI's dysfunctional and snail-paced internal efforts described by the *Cobell* court, outsourcing becomes a very attractive option indeed.

Some, however, are more cautious about the trend of outsourcing governmental functions. In particular, maintaining oversight and enforcing accountability can become quite difficult—even impossible—when dealing with private contractors. One commentator, for example, has recently noted that "lack of oversight and control becomes an inevitable consequence of privatization, producing imbalance between those in government who should oversee and those in the private sector who are meant to be overseen."[127] Skeptics, then, may argue that farming out information security work to the private sector is dangerous in that those doing the work will ultimately be unaccountable, and might therefore underperform.[128]

Such worries are probably overstated. For one, ultimate responsibility for implementing FISMA would still remain with the indi-

---

[126] My proposal requires all diagnostic work to be completed by private contractors, but does not foreclose the prospect of agencies hiring contractors to do further FISMA-related work.

[127] Paul R. Verkuil, *Public Law Limitations on Privatization of Government Functions*, 84 N.C. L. REV. 397, 399–400 (2006).

[128] Examples of outsourcing gone wrong are not infrequent. *See, e.g.*, *Aviation Security and the Future of the Aviation Industry Before the Subcomm. on Aviation of the H. Comm. on Transportation & Infrastructure*, 107th Cong. 75–76 (2001) (statement of Gerald L. Dillingham, Director, Physical Infrastructure Issues, United States General Accounting Office) (noting failure of airport security guards employed by private airlines to effectively control access to secure areas and to screen passengers prior to September 11th terrorist attacks); Steven L. Schooner, *Contractor Atrocities at Abu Ghraib: Compromised Accountability in a Streamlined, Outsourced Government*, 16 STAN. L. & POL'Y REV. 549, 555–57 (2005) (discussing Abu Ghraib prison torture scandal in Iraq and prominent role of private contractor interrogators); Sidney A. Shapiro, *Outsourcing Government Regulation*, 53 DUKE L.J. 389, 408–09 (2003) (describing failure of accounting industry to set adequate standards for securities regulation and Congress's post-Enron effort to shift responsibility back to administrative state).

Reprinted with Permission of New York University School of Law

vidual agencies and OMB. My recommendation is only that preliminary diagnostic work be outsourced across the board, so the scope of the privatization would not be as extensive as in some of the programs to which critics point. Moreover, the hope of securing further government contracts to fix diagnosed problems would seriously incentivize contractors to bring to light any and all deficiencies.

There are certainly theoretical arguments that caution against the outsourcing of FISMA responsibilities. Yet the performance of the agency community to date has been uninspiring overall. As a result, it may be time to try new solutions to these old problems. Perhaps a trial outsourcing program could be introduced in one or two agencies, with those agencies' CIOs conducting parallel security assessments to confirm that the private contractors are up to the task. It may in fact be the CIOs who learn something from the contractors.

CONCLUSION

Information security is a serious issue that demands serious attention. In spite of its various and deep flaws, FISMA makes an important first step by placing this issue on agency agendas. Yet it is only a first step, and equally important is continual vigilance and oversight to ensure that agencies implement FISMA in a speedy and thorough manner.

One common theme that emerges in this area is the danger of excessive decentralization. Problems seem to occur because agencies are cast adrift with a copy of FISMA and little else to guide or prod them. Achieving government-wide information security requires a holistic government-wide effort, with active participation from agencies, of course, but also from Congress, OMB, and even the private sector. These last three participants are currently absent, and my proposed reforms seek to insert them into the process.

Of course, there is no overnight solution for achieving effective information security. Nevertheless, we must take note of the institutional realities that have hampered agency efforts during FISMA's first three years. By confronting these realities quickly and effectively, Congress can finish the task it started and move us closer to a government in which all federal data is secure.

Reprinted with Permission of New York University School of Law