Fordham Law Review

Volume 79 | Issue 1 Article 12

November 2011

The Federal Information Security Management Act of 2002: A Potemkin Village

Daniel M. White

THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT OF 2002: A POTEMKIN VILLAGE

*Daniel M. White**

Due to the daunting possibilities of cyberwarfare, and the ease with which cyberattacks may be conducted, the United Nations has warned that the next world war could be initiated through worldwide cyberattacks between countries. In response to the growing threat of cyberwarfare and the increasing importance of information security, Congress passed the Federal Information Security Management Act of 2002 (FISMA). FISMA recognizes the importance of information security to the national economic and security interests of the United States. However, this Note argues that FISMA has failed to significantly bolster information security, primarily because FISMA treats information security as a technological problem and not an economic problem. This Note analyzes existing proposals to incentivize heightened software quality assurance, and proposes a new solution designed to strengthen federal information security in light of the failings of FISMA and the trappings of Congress's 2001 amendment to the Computer Fraud and Abuse Act.

TABLE OF CONTENTS

* J.D. Candidate, 2011, Fordham University School of Law. I would like to thank Professor Eric Jensen for his guidance and insight. In addition, I would like to thank my parents and sister for their continuous encouragement and support throughout this process. Last but not least, I would like to thank my wife, Janna, for her constant love and unwavering support.

INTRODUCTION

In early 2007, Estonia was widely considered one of the most technologically integrated countries in the world.[1] Free public Wi-Fi flourished and Estonian citizens could conduct banking, file taxes, vote in parliamentary elections, and pay for goods through cellular phones and e-technology.[2] In April of 2007, Estonia relocated a Soviet World War II memorial.[3] What followed was a crippling retaliatory denial-of-service attack on Estonian infrastructure.[4] In a matter of hours, the attack blocked government communication, a number of online banking portals, and

1. *See* DAVID RICE, GEEKONOMICS: THE REAL COST OF INSECURE SOFTWARE, at xiii (2008) (describing Estonia as "'the most wired nation in Europe' because of its pervasive use of computer networks for a wide array of private and public activities"); *see also* Jon P. Jurich, *Cyberwar and Customary International Law: The Potential of a "Bottom-Up" Approach to an International Law of Information Operations*, 9 CHI. J. INT'L L. 275, 275 (2008).

2. Scott J. Shackelford, *From Nuclear War to Net War: Analogizing Cyber Attacks in International Law*, 27 BERKELEY J. INT'L L. 192, 193–94 (2009).

3. *See* RICE, *supra* note 1, at xii.

4. *See* Jurich, *supra* note 1, at 275.

newspaper circulation.[5] Estonia instantaneously spiraled into a state of anarchy. Within a few days of the attack, riots and civil insurrection caused over 150 injuries and one death.[6] As one commentator observed:

> Never before had an entire country been targeted on almost every digital front all at once, and never before had a government itself fought back in such a prolonged and well-publicized campaign. Indeed, the attacks were so widespread and the results so grave that [Estonian Minister of Defense Jaak] Aaviksoo considered invoking Article 5 of the North Atlantic Treaty Organization ("NATO"), which states that an assault on one allied country obligates the alliance to attack the aggressor.[7]

Fortunately, Estonia was able to regain control of its domestic infrastructure and restore order. [8]

While Russia was initially believed to be responsible for the attacks, the ensuing investigation led to much confusion over who was responsible, and no formal conclusion was ever reached.[9] Although the Estonia incident is a quintessential example of the disorder and destruction a cyberattack can cause, it is only one of many recent instances of cyberwarfare. Other documented attacks include the interruption of air traffic control systems, the corruption of a nuclear power plant control system in Ohio, the co-option of gas pipelines, and the degradation of utility companies and power grids.[10]

Cyberattacks are not limited to those on critical infrastructure. Attacks can be used to gather classified intelligence and, as a Pentagon review noted in 2004, to exploit weaknesses in the Navy's broadcast system used to communicate nuclear launch codes to Trident submarines.[11] This report noted that potential attackers could gain access to the communications network and falsify launch orders, potentially leading to an errant nuclear weapons launch.[12]

There are a number of reasons why cyberattacks are widespread. First, a successful cyberattack need only exploit one weakness in a computer network, while a successful cyberdefense requires defending against all vulnerabilities.[13] Additionally, most cyberattacks—such as the denial-of-service attack waged against Estonia—can be conducted using nearly any

---

5. *See* Shackelford, *supra* note 2, at 193–94.
6. *Id.*
7. *Id.* at 194.
8. *Id.* at 206.
9. *See* Gadi Evron, *Battling Botnets and Online Mobs: Estonia's Defense Efforts During the Internet War*, GEO. J. INT'L AFF., Winter/Spring 2008, at 121, 123.
10. Jason Fritz, Hacking Nuclear Command and Control 5 (2009) (unpublished research paper) (on file with the International Commission on Nuclear Non-Proliferation and Disarmament), *available at* http://www.icnnd.org/research/Jason_Fritz_Hacking_NC2.pdf.
11. *Id.* at 16.
12. *Id.* More recently, Iraqi insurgents have been using widely available software, purchased for twenty-six dollars, to intercept live video feeds from unmanned Predator Drones in Iraq. *See* Siobhan Gorman et al., *Insurgents Hack U.S. Drones*, WALL. ST. J., Dec. 17, 2009, at A1.
13. *See* Fritz, *supra* note 10, at 6.

computer with an Internet connection.[14] Attacks can be easily masked and present none of the logistical difficulties associated with traditional physical attacks.[15] In short, cyberwarfare can be used in place of nearly any traditional form of attack or espionage, and it is often more advantageous. Due to the daunting possibilities of cyberwarfare, and the ease with which cyberattacks may be conducted, the United Nations has warned that the next world war could be initiated through worldwide cyberattacks among countries.[16]

In response to the growing threat of cyberwarfare, and the increasing importance of information security, Congress passed the Federal Information Security Management Act of 2002 (FISMA).[17] FISMA "recognized the importance of information security to the economic and national security interests of the United States."[18] Specifically, FISMA requires each federal agency to adopt and manage an agency-wide program to ensure information and computer network security.[19] Unfortunately, many critics view FISMA as unsuccessful, with one commentator referring to it as a "paperwork drill" that "puts into place and measures paper-based processes, rather than technical processes, for implementing information security."[20] More importantly, FISMA fails to address the root cause of network exploitation: inadequate software quality assurance.[21]

The world has become largely dependent on software, which "helps deliver oil to our cities, electricity to our homes, water to our crops, products to our markets, money to our banks, and information to our minds."[22] However, software is becoming increasingly less reliable.[23] This heightened dependence comes at a time when software and network exploitation are on the rise, and the Internet is rapidly becoming the new battlefield of the twenty-first century. What has become clear is that adequate software quality assurance is of paramount concern and is critical to national security. Unfortunately, Congress has compounded the problem of inadequate software quality assurance. In 2001, Congress amended the Computer Fraud and Abuse Act[24] to prevent the possibility of bringing an action against software manufacturers for negligently manufactured

14. *Id.* at 1.

15. *Id.* at 3.

16. Associated Foreign Press, *Threat of Next World War May Be in Cyberspace: UN*, BREITBART.COM (Oct. 6, 2009, 11:47 AM), http://www.breitbart.com/article.php?id=CNG.d8b45ac8e22de08986da7ef67ae96151.431&show_article=1.

17. Pub. L. No. 107-347, 116 Stat. 2899 (codified at 44 U.S.C. §§ 3541–3549 (2006)).

18. Nat'l. Inst. of Standards & Tech., *Detailed Overview*, http://csrc.nist.gov/groups/SMA/fisma/overview.html (last visited Sept. 23, 2010).

19. *Id.*

20. *INPUT Says FISMA Fails to Improve Overall Security*, INPUT (March 16, 2006), http://www.input.com/corp/press/detail.cfm?news=1168.

21. *See* RICE, *supra* note 1, at 82–83.

22. *See id.* at 6.

23. *Id*. at xv.

24. Pub. L. No. 99-474, 100 Stat. 1213 (2001) (codified as amended at 18 U.S.C. § 1030(g) (2006)).

software.[25] Such a liability shield creates fundamental disincentives for software manufacturers to ensure adequate software quality assurance, and has imposed substantial negative externalities on the U.S. federal government that have decreased information security and, in turn, weakened national and economic security.[26]

Various proposals have been made and intense debate has ensued over how best to incentivize software manufacturers to ensure adequate software quality assurance. These proposals are generally rooted in tort theories, and include holding software manufacturers strictly liable for security flaws under products liability theory,[27] as well as a new cause of action for the negligent enablement of cybercrimes.[28] Additionally, incentive systems rooted in contract law have also been proposed.[29]

This Note will analyze existing proposals to incentivize heightened software quality assurance and propose a new solution designed to strengthen federal information security in light of the failings of FISMA and the trappings of the 2001 amendment to the Computer Fraud and Abuse Act. Part I of this Note examines the history, purpose, and enforcement of FISMA. Part I also analyzes common criticisms of FISMA, including the view that FISMA has failed to significantly bolster information security, primarily because FISMA treats information security as a technological problem and not as an economic problem. Existing proposals designed to incentivize heightened software quality assurance are analyzed in Part II.

Part III of this Note argues that the most plausible method to incentivize heightened federal information security is to impose liability on software manufacturers for the breach of an express warranty. This warranty is premised on a newly developed security assurance certification. A federal mandate will direct agencies only to purchase commercial software designated with such a certification. Finally, Part III addresses the advantages and disadvantages of such a mandate.

I. THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT OF 2002 (FISMA)

To better understand the role FISMA plays in information and network security, Part I.A discusses the history, purpose, and current enforcement of FISMA. Part I.B examines contemporary criticisms of FISMA, and Part I.C highlights current efforts to revise FISMA in light of such criticism.

---

25. 18 U.S.C. § 1030(g). The revision states, "No action may be brought . . . for the negligent design or manufacture of computer hardware, computer software, or firmware." *Id.*

26. *See* RICE, *supra* note 1, at 43–44.

27. *See* Kevin R. Pinkney, *Putting Blame Where Blame is Due: Software Manufacturer and Customer Liability for Security-Related Software Failure*, 13 ALB. L.J. SCI. & TECH. 43, 46–48 (2002) (proposing that software manufacturers should be subjected to strict products liability); *see also* RICE, *supra* note 1, at 221–32.

28. *See generally* Michael L. Rustad & Thomas H. Koenig, *The Tort of Negligent Enablement of Cybercrime*, 20 BERKELEY TECH. L.J. 1553 (2005). For additional commentary on Rustad & Koenig's proposal, see RICE, *supra* note 1, at 232–36; *infra* Part II.B.

29. *See infra* Part II.C.

A. The History, Purposes, and Enforcement of FISMA

Information security has a long and intriguing history. One well-known example is that of Histaiaeus, a tyrant under the Persian king Darius.[30] Histaiaeus tattooed the shaved head of his slave with a message urging the ruler of Miletus to revolt against King Darius.[31] Histaiaeus waited for the slave's hair to grow back before he sent the slave to the ruler of Miletus.[32] While primitive, the arrangement allowed the slave to travel inconspicuously to the intended recipient and ensure the message's safe delivery. Countless examples abound throughout history of wars won and lost due to superior—or inferior—information security.[33]

The rapid growth of computing technology and the Internet has presented new challenges to safeguarding information and critical infrastructure.[34] Cyberattacks and exploitations have further fueled the need for superior information security.[35] Beginning in the 1980s, Congress addressed electronic information security through a number of legislative schemes designed to deal with the management and disposition of records, the management of information resources, and a number of other relevant concerns.[36] These efforts manifested themselves in the Paperwork Reduction Act of 1980,[37] the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984,[38] and the Computer Security Act of 1987,[39] among others.[40]

FISMA was designed to consolidate the latter statutes[41] and was signed into law as Title III of the E-Government Act of 2002.[42] FISMA's stated

30. *See* SIMON SINGH, THE CODE BOOK: THE SCIENCE OF SECRECY FROM ANCIENT EGYPT TO QUANTUM CRYPTOGRAPHY 5 (1999).

31. *Id.*

32. *Id.*

33. *See generally id.* (discussing the influence of information security—specifically, cryptography—from Ancient Egypt through World Wars I and II).

34. *See* Shackelford, *supra* note 2, at 193–94. As noted, the attack on Estonia is the quintessential example of the new challenges the Internet poses to information security. Never before has a country's infrastructure been so compromised exclusively because of its connectivity to the Internet. *Id.*; *see also supra* notes 1–7 and accompanying text. For a brief overview of the challenges the Internet poses to safeguarding information and critical infrastructure, see Fritz, *supra* note 10, at 5.

35. *See supra* notes 1–12 and accompanying text.

36. *See, e.g.*, H.R. REP. NO. 107-787, pt. 1, at 54–55 (2002), *reprinted in* 2002 U.S.C.C.A.N. 1880, 1889 (including the authorized use or disclosure of information with regard to the protection of personal privacy, and the disclosure of information to the Congress or the Comptroller General of the United States).

37. Pub. L. No. 96-511, 94 Stat. 2812 (codified at 44 U.S.C. § 3501 (2006)).

38. Pub. L. No. 98-473, 98 Stat. 2190 (codified at 18 U.S.C. § 1030 (2006)).

39. Pub. L. No. 100-235, 101 Stat. 1724 (codified at 5 U.S.C. § 272 (2006)).

40. *See, e.g.*, The Government Information Security Reform Act, Pub. L. No. 106-398, 114 Stat. 1654 (2000) (codified at 40 U.S.C. § 11103(a) (2006)); The Information Technology Management Reform (Clinger-Cohen) Act of 1996, Pub. L. No. 104-106, §§ 5001–02, 110 Stat. 679, 679–80 (codified at 40 U.S.C. § 1401 (2006)).

41. *See* H.R. REP. NO. 107-787, pt.1, at 54, *reprinted in* 2002 U.S.C.C.A.N. 1880–89 ("FISMA eliminates obsolete mandates, updates outmoded provisions, harmonizes overlapping requirements, and strengthens key requirements. The result is a clearer and stronger law. . . .").

42. 44 U.S.C. §§ 3541–3549 (2006).

purpose is to provide effective information security management and oversight for the federal government.[43] In doing so, FISMA recognizes the importance of information security to the United States' national and economic security.[44]

To accomplish its stated purposes, FISMA requires each federal agency to adopt, manage, and document an agencywide program to ensure information security.[45] Federal agencies are directed to utilize a risk-based approach to information security, which consists of each respective agency adopting security measures as required by the classification given to the relative worth of agency information.[46] This approach is designed to reduce security risks to an acceptable level in a cost-effective manner and ensure that information security is maintained throughout the life cycle of the organizational information system.[47]

Once a proper security level has been determined, agencies are instructed to implement and maintain information security policies and procedures

---

43. *See id.* § 3541. The Federal Information Security Management Act of 2002 (FISMA) has six purported purposes, to:

> (1) [P]rovide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets;
> (2) [R]ecognize the highly networked nature of the current Federal computing environment and provide effective governmentwide management and oversight of the related information security risks, including coordination of information security efforts throughout the civilian, national security, and law enforcement communities;
> (3) [P]rovide for development and maintenance of minimum controls required to protect Federal information and information systems;
> (4) [P]rovide a mechanism for improved oversight of Federal agency information security programs;
> (5) [A]cknowledge 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; and
> (6) [R]ecognize that the selection of specific technical hardware and software information security solutions should be left to individual agencies from among commercially developed products.

Id.

44. *See* H.R. REP. NO. 107-787, pt.1, at 55–60, *reprinted in* 2002 U.S.C.C.A.N. 1880, 1889–94; *see also* NAT'L. INST. OF STANDARDS & TECH., FIPS PUBLICATION 200: MINIMUM SECURITY REQUIREMENTS FOR FEDERAL INFORMATION AND INFORMATION SYSTEMS iv (2006) [hereinafter FIPS REPORT], *available at* http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf; Nat'l. Inst. of Standards & Tech, NIST.GOV, http://csrc.nist.gov/groups/SMA/fisma/overview.html (last visited Sept. 23, 2010).

45. *See* 44 U.S.C. § 3544(b) ("Each agency shall develop, document, and implement an agencywide information security program . . . .").

46. *See id.* § 3543. The National Institute of Standards and Technology (NIST) requires agencies to categorize their information systems as "low-impact, moderate-impact, or high-impact for the security objectives of confidentiality, integrity, and availability. The potential impact values assigned to the respective security objectives are the highest values . . . from among the security categories that have been determined for each type of information resident on those information systems." *FIPS Report*, *supra* note 44, at 1.

47. *See* 44 U.S.C. § 3544(b)(2)(B)–(C).

consistent with the National Institute of Standards and Technology's (NIST) technological requirements.[48] This includes "periodically testing and evaluating information security controls and techniques to ensure that they are effectively implemented."[49] FISMA entrusts the head of each agency with the ultimate responsibility of testing and ensuring agency compliance with FISMA.[50] However, the head of each agency may delegate this responsibility to a Chief Information Officer (CIO).[51]

To adequately govern agency heads and ensure compliance, FISMA empowers the Office of Management and Budget (OMB) with management authority over federal agencies' information security systems.[52] This authority includes the ability to approve or disapprove of any federal agency's information security system.[53] Ultimately, OMB is required to report to a number of oversight authorities, including science and technology committees and appropriations committees before both the House of Representatives and the Senate.[54] Reports consist of annual evaluations,[55] an "assessment of the development, promulgation, and adoption of, and compliance with, standards developed [under] the National Institute of Standards and Technology Act,"[56] as well as deficiencies in agency practices,[57] and remedial plans designed to remedy such deficiencies.[58] Finally, Congress has empowered OMB to ensure compliance with FISMA through sanctions imposed for non-compliance.[59] This includes the ability to recommend reducing agency budgets or appropriations for information resources.[60]

Consequently, FISMA requires the establishment of, and compliance with, adequate information security standards. The result is an

48. *See id.* § 3544(a)(1)(B)(i). NIST is instructed to "develop standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets . . . ." 15 U.S.C. § 278g-3(a)(3) (2006). It is important to note that these standards do not apply to select, highly classified systems run by agencies such as the Central Intelligence Agency or Department of Defense. *See id.*

49. 44 U.S.C. § 3544(a)(2)(D). The frequency of this testing is based on the designated categorization of the information system. For example, information systems deemed "high-impact" are tested more frequently than information systems deemed "low-impact." *See id.* § 3544(b)(5).

50. *Id.* § 3544(a).

51. *Id.* § 3544(a)(3).

52. *Id.* § 3543(a).

53. *Id.* § 3543(a)(5).

54. *Id.* § 3544(c) (specifically, the Office of Management & Budget (OMB) is required to report to the "Committees on Government Reform and Science of the House of Representatives, the Committees on Governmental Affairs and Commerce, Science, and Transportation of the Senate, the appropriate authorization and appropriations committees of Congress, and the Comptroller General . . . .").

55. *See id.* § 3543(a)(8)(A). An Inspector General or an external auditor performs the evaluation. *See id.* § 3545(b). The evaluation is designed to test "the effectiveness of information security policies, procedures, and practices of a representative subset of the agency's information systems." *Id.* § 3545(a)(2)(A).

56. *Id.* § 3543(a)(8)(B).

57. *Id.* §3543(a)(8)(C).

58. *Id.* §3543(a)(8)(D).

59. *See id.* §3543(a)(4).

60. 40 U.S.C. § 11303(b)(5)(B).

encompassing, multi-layered framework for ensuring federal information security. However, FISMA has been subject to substantial criticism on a variety of grounds. Part I.B examines these contemporary criticisms of FISMA.

B. Contemporary Criticisms of FISMA

Contemporary criticisms of FISMA all share the same conclusion: FISMA fails to bolster actual information security. This conclusion was supported by a Department of Homeland Security report, which found that cyberattacks within federal agencies increased over 250% between 2007 and 2009.[61] This section analyzes three of the more established theories that attempt to explain why FISMA fails to bolster actual information security. Part I.B.1 explains the charge that FISMA is difficult to implement. Part I.B.2 highlights the criticism that FISMA is over-reliant on reporting requirements that misrepresent actual security. Part I.B.3 analyzes the accusation that FISMA treats information security as a technological problem instead of an economic problem.

1. Federal Agencies Have Difficulty Implementing FISMA

In early 2007, an external hard drive containing Social Security numbers, unencrypted names, birthdates, and healthcare files of 198,000 veterans was stolen from the U.S. Department of Veterans Affairs.[62] Some of the veterans whose personal information had been stolen sued, seeking declaratory and injunctive relief premised on alleged violations of FISMA,[63] among others.[64] While the U.S. Court of Appeals for the

---

61. *See* Gregg Carlstrom, *Net Attacks Triple in 2 Years*, FED. TIMES (Aug. 3, 2009), http://www.federaltimes.com/article/20090803/IT01/908030305/1035/IT01. It is important to note that this is a conservative estimate, since it is believed that federal agencies only report fifty to sixty percent of cyberattacks, and the overall figure excludes the Department of Defense, which "receives millions of scans and probes each year." *Id.* This is supported by testimony before the U.S. Senate. *See Information Security: Progress Reported, but Weaknesses at Federal Agencies Persist: Hearing Before the S. Subcomm. on Fed. Fin. Mgmt., Gov't Info., Fed. Servs., & Int'l Sec., Comm. on Homeland Sec. & Governmental Affairs*, 110th Cong. 15–16 (2008) [hereinafter *Weaknesses Hearing*](statement of Gregory C. Wilshusen, Director, Information Security Issues at the Government Accounting Office) ("[F]ive IGs [Inspector Generals] noted that the agency was not following procedures for internal incident reporting, two noted that their agency was not following reporting procedures to [the United States Computer Emergency Readiness Team], and one noted that the agency was not following reporting procedures to law enforcement. Several IGs also noted specific weaknesses in incident procedures such as components not reporting incidents reliably or consistently, components not keeping records of incidents, and incomplete or inaccurate incident reports.").

62. *See* Fanin v. U.S. Dep't of Veterans Affairs, 572 F.3d 868, 870–71 (11th Cir. 2009). Judge Carnes's description of the event is particularly humorous:

> Someone pulled off the trick of making an object disappear from a safe in a darkened office building over a cold and rainy weekend. Unfortunately, the magician never completed the trick by making it reappear . . . . Where it is now is anybody's guess. In the meantime, no one is applauding the trick, least of all the veterans. Some of them have sued the VA.

Id. at 870.

63. *Id.* at 871.

Eleventh Circuit reversed the district court's decision to grant summary judgment to the defendants, and ultimately remanded the case, the decision contains an insightful glimpse into a federal agency's failed compliance with FISMA.[65] The court noted that, after the security breach had occurred, "[t]he Office of the Inspector General concluded that the VA's [Veterans Affair's] security plan did not comply with the agency's own rules for securing data, and it improperly allowed the IT [Information Technology] Specialist access to databases" beyond his security clearance.[66] Furthermore, the court found that it had "no reason to think that all of the alleged violations have been remedied."[67] Thus, the theft of valuable information from the VA confirmed what a number of critics had already believed: federal agencies struggle to properly implement FISMA.[68] Several theories have been promulgated to explain this struggle.[69]

One theory holds that FISMA presents an unfunded mandate that requires agencies to perform additional work within the constraints of a pre-existing budget.[70] As one author explains, "[f]or bureaus that already

64. *Id.* The complaint also alleged violations of the Privacy Act, the E-Government Act of 2002, the VA Claims Confidentiality Statute, the Trade Secrets Act, and the Veterans Benefits, Health Care, and Information Technology Act of 2006. *Id.*

65. *Id.* at 871, 876–78.

66. *Id.* at 871.

67. *Id.* at 876. Nearly a year after the data theft, Robert T. Howard, the Assistant Secretary for Information and Technology, spoke before a Senate subcommittee. Howard stated that the day the hard drive was stolen was "a wake up call . . . . As a result of that incident we began to improve our security posture and create the environment needed to better protect the . . . sensitive information entrusted to us." *Agencies in Peril: Are We Doing Enough to Protect Federal IT and Secure Sensitive Information?: Hearing Before the S. Subcomm. on Fed. Fin. Mgmt., Gov't, Info., Fed. Servs., and Int'l Sec.*, 110th Cong. 1 (2008) [hereinafter *Agencies in Peril*] (statement of Robert T. Howard, Assistant Secretary for Information & Technology, Department of Veteran Affairs). Howard proceeded to identify five areas of FISMA compliance the Department of Veteran Affairs is working to improve. *Id.* at 4–6. Unfortunately, according to the 2008 OMB report to Congress, when asked whether the agency applies common security configurations established by NIST to application information systems, the Department of Veteran Affairs responded only "[s]ometimes (51–70% of the time)." OFFICE OF MGMT. & BUDGET, FISCAL YEAR 2008 REPORT TO CONGRESS ON IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT OF 2002 app. A-104 (2008) [hereinafter 2008 OMB REPORT].

68. *See* Robert Silvers, Note, *Rethinking FISMA and Federal Information Security Policy*, 81 N.Y.U. L. REV. 1844, 1849–63 (2006). Silvers' discussion of *Cobell v. Norton*, 394 F. Supp. 2d 164 (D.D.C. 2005), is particularly enlightening. *See* Silvers, *supra*, at 1851–53. In *Cobell*, Individual Indian Money Trust beneficiaries sought an injunction to disconnect the Bureau of Indian Affairs (BIA) information technology networks from the Internet. The plaintiffs alleged that the BIA lacked adequate information security, and therefore was in breach of its fiduciary obligations to the plaintiffs. *Cobell*, 394 F. Supp. 2d at 165–68. Ultimately, the court's opinion exposed a federal agency whose FISMA compliance had "lagged behind the expansion of the department's Internet presence." *Id.* at 223. For a further example of an agency's struggle to implement FISMA, see *Agencies in Peril*, *supra* note 67, at 4 (statement of Robert T. Howard, Assistant Secretary for Information & Technology, Department of Veteran Affairs) ("While we have made progress, there is still much to be done. With respect to FISMA, there are five problematic areas."), and see generally 2008 OMB REPORT, *supra* note 67 (demonstrating numerous areas of non-compliance despite agencies having had over six years to enact FISMA-compliant policies).

69. *See infra* notes 70–83 and accompanying text.

70. *See* Silvers , *supra* note 68, at 1859.

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."[71]

Another theory holds that FISMA is too vague to ensure adequate information security.[72] For example, federal agencies are required to ensure that private contractors comply with various provisions of FISMA.[73] However, the actual scope of this requirement is vague, and leaves Inspector Generals guessing whether Congress intended FISMA oversight of private contractors in a number of situations.[74] Vagueness is also said to plague OMB's guidance regarding FISMA compliance[75] and the language and clarity of actual NIST technological standards.[76] These ambiguities are compounded because FISMA provides no formal mechanism for resolving uncertainty.[77] This can lead to "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."[78]

Finally, many believe that agencies struggle to implement FISMA because FISMA fails to instill proper accountability within agencies.[79]

---

71. *Id.* To support this view, Silvers cites the testimony of Earl E. Devaney, Inspector General of the Department of Interior, who stated before a Senate Congressional Committee that he viewed FISMA as "sort of an unfunded mandate that IGs [implement FISMA] without the resources to accompany it." *Id.*

72. *See* CTR. FOR STRATEGIC & INT'L STUDIES, SECURING CYBERSPACE FOR THE 44TH PRESIDENCY 69 (2008) [hereinafter CSIS], *available at* http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf; *infra* notes 74–78 and accompanying text. Perhaps the most telling pieces of evidence that FISMA is overly vague is the success of consulting firms that now specialize in FISMA compliance. As one FISMA consulting firm boldly asserts, "Information Security and Privacy regulations are purposely vague to ensure they cover a wide range of organizations over a long period of time without having to be amended by Congress." NETIQ, NETIQ FISMA COMPLIANCE & RISK MANAGEMENT SOLUTIONS 2 (2005), *available at* http://download.netiq.com/CMS/SOLUTIONSHEET/FISMA_broch_final_.pdf.

73. 44 U.S.C. § 3544(a)(1)(A)(ii) (2006).

74. *See* Silvers, *supra* note 68, at 1853 ("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.").

75. *See Protecting Personal Information: Is the Federal Government Doing Enough?: Hearing Before the S. Comm. on Homeland Sec. & Governmental Affairs*, 110th Cong. 5 (2008) [hereinafter *Personal Information Hearing*] (statement of Ari Schwartz, Vice President of the Center for Democracy & Technology). Schwartz testified that with respect to a specific NIST requirement, the wide variation in compliance was attributed to vague guidance from OMB. *Id.*

76. *See Weaknesses Hearing*, *supra* note 61, at 14–15 (statement of Gregory C. Wilshusen Director, Information Security Issues, Government Accounting Office) ("Twenty-three of the major federal agencies reported that they had an agencywide security configuration policy. Although the IGs agreed that their agency had such a policy, several IGs did not agree to the extent to which their agencies . . . applied the common security configurations as established by NIST.").

77. *See* Silvers, *supra* note 68, at 1853.

78. *Id.*

79. *See infra* notes 80–82 and accompanying text.

FISMA empowers the OMB to ensure compliance with FISMA through the threat of a number of sanctions, including the ability to recommend reducing agency budgets or appropriations for information resources.[80] However, as one critic argues, IT sanctions are counterproductive[81] and "so many agencies are delinquent in their FISMA obligations that a 'safety in numbers' mentality may begin to take hold . . . the current environment—in which nearly every major federal agency has work left to do—would make mass punishment . . . disastrous."[82] This belief is further supported by agencies' inability to meet all of FISMA's obligations after six years of working to ensure FISMA compliance.[83]

2. FISMA Is a "Paperwork Exercise"

As explained in the previous section, the composition of FISMA impedes federal agencies from implementing compliant policies. However, even assuming one hundred percent compliance with FISMA, many commentators believe that FISMA would still fail to bolster actual information security.[84] While FISMA requires federal agencies to ensure that their information security systems are compliant with NIST technological standards,[85] a substantial portion of FISMA compliance revolves around reporting requirements.[86] Critics believe there are two fundamental flaws with these reporting requirements that ultimately work to undermine actual information security.[87]

The first flaw critics point to with respect to FISMA reporting requirements are the metrics being measured and reported.[88] This argument theorizes that the metrics used as a basis for FISMA reporting do not actually measure operational security.[89] The key measurements FISMA requires, such as certification and accreditation, plan of action and milestones (POA&M), and percentage of personnel trained, cover the "[p]eople, [p]rocess and [t]echnology aspects of security" but fail to

80. *See supra* notes 59–60 and accompanying text.

81. *See supra* note 70 and accompanying text.

82. *See* Silvers, *supra* note 68, at 1862 (internal citation omitted).

83. *See generally* 2008 OMB REPORT, *supra* note 67 (demonstrating numerous areas of non-compliance despite agencies having had over six years to enact FISMA-compliant policies).

84. *See infra* notes 87–103 and accompanying text.

85. *See* 44 U.S.C. § 3544(a)(1)(B)(i) (2002).

86. *See id.* § 3544(c); *supra* notes 54–60 and accompanying text.

87. *See* Wm. Arthur Conklin, *Why FISMA Falls Short: The Need for Security Metrics*, 41 WIRELESS INTERNET S. PROVIDER PROC. 1, 1–8 (2008), http://www.tech.uh.edu/cae-dc/documents/WISP%202007%20FISMA%20metrics%20paper%20final.pdf; *see also Agencies in Peril*, *supra* note 67, at 2–6 (statement of Tim Bennett, President of Cyber Security Industry Alliance) (identifying general flaws in FISMA reporting); Angela Gunn, *Fed Having Fits over FISMA and Cybersecurity*, BETANEWS (Dec. 12, 2008), http://www.betanews.com/article/Feds-having-fits-over-FISMA-and cybersecurity/1229078893.

88. *See* Conklin, *supra* note 87, at 8–9; *see also Agencies in Peril*, *supra* note 67, at 3 (statement of Tim Bennett, President of Cyber Security Industry Alliance).

89. *See* Conklin, *supra* note 87, at 8–9.

"directly assess aspects of operational security."[90] These critics claim the metrics do not evaluate the underlying effectiveness of a federal agency's security system, or any specific aspect of a system's operational security.[91] Moreover, FISMA reporting requirements do not evaluate relative threat levels, or potential vulnerabilities associated with a system.[92]

Testimony before the Senate Subcommittee on Federal Financial Management, Government Information, Federal Services, and International Security aided the belief that FISMA focuses too heavily on compliance at the expense of actual security.[93] Tim Bennett, President of the Cyber Security Industry Alliance, lamented how FISMA grades reflect how well agencies comply with FISMA-mandated processes, but not how well these processes have actually increased federal information security.[94] He concluded that federal agencies are relying on misleading data to bolster their information security.[95]

To compound this problem, critics have identified a second flaw in FISMA reporting requirements: FISMA provides little incentive to address any metric outside of those required by FISMA reporting requirements.[96] Critics argue that these reporting requirements

> create[] lots of paperwork . . . . By focusing on security reports and the auditing thereof rather than on actual security measures . . . FISMA made it easy for federal [Chief Information Security Officers] to quantify their work in a way the bureaucracy at large could understand. Rather than trying to demonstrate that their systems prevented X number of attacks or deflected Y number of intrusions . . . departments could demonstrate that

90. *Id.* at 8. Conklin provides a useful description of each key FISMA metric and what the metric is used to measure; accordingly:

> Certification and Accreditation measures efforts at defining the appropriate security measures on a system by system basis. The . . . POA&M [Plan of Action and Milestones] metric measures the compliance with an established methodology for correction of discrepancies. The measurement of percentage of personnel trained is an attempt to determine the commitment towards training and awareness.

Id.

91. *Id.*

92. *Id.*

93. *See Agencies in Peril*, *supra* note 67, at 3 (statement of Tim Bennett, President of Cyber Security Industry Alliance).

94. *Id.* at 2; *see also* Jaikumar Vijayan, *Critics Question Value of Federal IT Security Report Card*, IDG NEWS SERV. (May 25, 2008), http://news.idg.no/cw/art.cfm?id=08F0A29C-17A4-0F78-3113197D5C06A6C5 ("The current FISMA reports 'say absolutely nothing about government security,' said Alan Paller, director of research at the SANS Institute, a Bethesda, Maryland based IT training and certification organization. 'This is just a measure of compliance with report generation.' . . . Ironically, he added, some agencies that are making an effort to comply with the true intent of the 396-page FISMA requirements document are getting poor grades on the annual report card, while others that have treated the process as a mere paperwork exercise are getting good grades.").

95. *See* Conklin, *supra* note 87, at 8–9.

96. *See* Gunn, *supra* note 87; *see also Agencies in Peril*, *supra* note 67, at 3 (statement of Tim Bennett, President of Cyber Security Industry Alliance).

> they'd reached their proper level of FISMA compliance . . . and thereby justify their various budgets.[97]

According to critics, FISMA relies too heavily on an agency's compliance with FISMA's reporting requirements as a means of objectively measuring the agency's level of information security.[98] This in turn motivates Chief Information Security Officers to comply only with reporting requirements and ignore underlying information security threats.[99] Tim Bennett provided support to this argument when he explained in his Congressional testimony that some Chief Information Security Officers' performances are measured on their respective abilities to comply with FISMA reporting requirements, and not whether they have "adequately assessed risk in their respective agency or prevented breaches of sensitive information."[100]

Thus, the two flaws identified by critics[101] support the general criticism that the information security assurances FISMA attempts to guarantee through oversight and reporting[102] are undermined by the nature of the compliance, oversight, and reporting processes.[103] To many, this explains why cyberattacks within federal agencies increased over 250% between 2007 and 2009.[104]

---

97. *See* Gunn, *supra* note 87.

98. *See id.*

99. *See Agencies in Peril*, *supra* note 67, at 3 (statement of Tim Bennett, President of Cyber Security Industry Alliance); *see also* Vijayan, *supra* note 94 ("[Director Paller noted] 'First, Congress creates waste by writing FISMA in a way that demands useless reporting, and then it highlights the useless scores in a way that in some cases provides incentives for federal agencies to deliver misleading results.'").

100. *See Agencies in Peril*, *supra* note 67, at 3.

101. *See supra* notes 88–100 and accompanying text.

102. 44 U.S.C. § 3544(c) (2002); *see supra* notes 54–60 and accompanying text.

103. *See supra* notes 88–100 and accompanying text. Interestingly, many commentators feel that FISMA was not designed nor intended to promote actual operational information security, but rather merely to promote awareness within the federal government about the risks cyberattacks pose. *See* Conklin, *supra* note 87, at 8 ("FISMA was intended to introduce information security practices to the Federal government sector and agencies, not to provide a complete and comprehensive solution."). Tim Bennett does not explicitly endorse this view, but recognizes the importance FISMA plays in raising federal information security awareness. *See Agencies in Peril*, *supra* note 67, at 2 (statement of Tim Bennett, President of Cyber Security Industry Alliance) ("FISMA has been fairly successful in getting agencies in general to pay closer attention to their information security obligations. Before FISMA, information security was not a top priority at federal agencies. FISMA has been successful in raising awareness of information security . . . .").

104. *See* Carlstrom, *supra* note 61; *see also* Conklin, *supra* note 87, at 9 ("The recent spate of recurring data disclosures and highly publicized information security failures in Federal agencies highlight the limitations of the current FISMA based approach. . . . The fact that . . . some agencies have not had an information security failure may [be] due as much to luck or lack of knowledge as it is to proper information security management.").

3. FISMA Treats Information Security as a Technological Problem and Not an Economic Problem

According to the National Vulnerability Database (NVD), there are approximately 40,000 known software vulnerabilities[105] that can be exploited to gain remote access to a computer or network.[106] The NVD currently adds, on average, eleven new vulnerabilities each day.[107] Some commentators feel that the most significant failing of FISMA—as opposed to the compliance or reporting issues addressed in the previous sections—lies in its complete failure to address negligent software development.[108] The results, according to critics, are "advanced, dynamic, robust, and effective information security solutions"[109] marred with known software vulnerabilities FISMA cannot even begin to solve.[110] To better understand the criticism being levied, this section first discusses the nature of the software industry, and then examines the specific criticism that FISMA and NIST treat information security as a technological problem, when information security should instead be approached as an economic problem.[111]

a. Software Manufacturers, Liability Shields, and Externalities

It is important to note that the U.S. federal government is the single largest purchaser of information security products.[112] These products, manufactured by civilian software companies, are the same products designed to safeguard federal agencies from external intrusions and exploitations.[113] Thus, software quality assurance becomes exceedingly

105. NATIONAL VULNERABILITY DATABASE, http://nvd.nist.gov/ (last visited Sept. 23, 2010). The National Vulnerability Database (NVD) describes itself as "a product of the NIST Computer Security Division and is sponsored by the Department of Homeland Security's National Cyber Security Division. It supports the U.S. government multi-agency . . . Information Security Automation Program. It is the U.S. government content repository for the Security Content Automation Protocol (SCAP)." *Id.* Its mission is to enable "automation of vulnerability management, security measurement, and compliance (e.g. FISMA)." *Id.*

106. *See Weaknesses Hearing*, *supra* note 61, at 7 (statement of Gregory C. Wilshusen Director, Information Security Issues at the Government Accounting Office).

107. *See* NATIONAL VULNERABILITY DATABASE, *supra* note 105; *see also* JOHN ROLLINS & ANNA C. HENNING, CONG. RESEARCH SERV., R40427, COMPREHENSIVE NATIONAL CYBERSECURITY INITIATIVE: LEGAL AUTHORITIES AND POLICY CONSIDERATIONS 3 (2009), *available at* http://www.fas.org/sgp/crs/natsec/R40427.pdf (finding that software and network exploitation is increasing).

108. *See* RICE, *supra* note 1, at 285–88.

109. Federal Information Security Management Act of 2002, 44 U.S.C. § 3541(5) (2006).

110. *See* RICE, *supra* note 1, at 286.

111. *See id.* at xvi ("Protecting economic and national security from the effects of insecure software is as much an economic issue as it is a technological issue.").

112. *See* CSIS, *supra* note 72, at 56.

113. 44 U.S.C. § 3541 (stating that one of the purposes of FISMA is to "recognize that the selection of specific technical hardware and software information security solutions should be left to individual agencies from among commercially developed products").

important when framed in terms of information security.[114] Many believe this concern only exists theoretically, highlighting that "[n]inety percent of security threats exploit known flaws in software."[115] This is because software engineering practices are influenced by a first-to-market mentality that emphasizes speed over quality, and encourages programmers to ignore serious errors and instead develop software as quickly as possible.[116]

To succeed in the software industry, as in most industries, a company must differentiate itself from the competition. However, given the fluid nature of the technology industry, and the reliance on cash flow to support operations, software manufacturers face increased pressure to rush their products to market in order to better capitalize on the product's innovation.[117] This leads to cost-cutting measures, such as the elimination of testing processes designed to ensure adequate quality assurance, which is traditionally one of the more expensive phases of development.[118] Thus, the inherent nature of the technology industry is said to provide a disincentive to thoroughly test software for known defects before releasing the product into the open marketplace.[119] This disincentive is supplemented, and some commentators say aided, by the liability shield imparted on the technology industry by Congress and the courts.[120]

---

114. *See* RICE, *supra* note 1, at 43–44 ("The real cost of insecure software is . . . cyber crime, insufficient testing, lost productivity, economic losses . . . and sometimes even death . . . . It is becoming more and more apparent . . . that the real cost of insecure software lies in what we are giving up—national and economic security.").

115. *See id.* at 133. *But see* Pinkney, *supra* note 27, at 66 ("Most telling though, is CERT's finding that over ninety-five percent of intrusions use known vulnerabilities for which counter-measures are available."). Some of the most common software vulnerabilities include password detection, buffer overflow, and denial of service attacks. For a comprehensive explanation of these attacks, see *id.* at 51–59.

116. *See* Jonathan Jacky, *Safety-Critical Computing: Hazards, Practices, Standards, and Regulation (*1994), reprinted in COMPUTERIZATION AND CONTROVERSY: VALUE CONFLICTS & SOCIAL CHOICES 767–92 (Rob Kling ed., 1996), *available at* http://staff.washington.edu/jon/pubs/safety-critical.html.

117. *See* RICE, *supra* note 1, at 44; Pinkney, *supra* note 27, at 72–73 ("Software manufacturers are eager to reduce time to market. Some manufacturers who otherwise might take due care preventing security-related software failure are forced under a no liability rule to lower their standard of care in order to compete with manufacturers not taking due care."). Thus, the software industry model functionally creates a "race to the bottom" in terms of software quality assurance.

118. *See* RICE, *supra* note 1, at 45.

119. *See* Pinkney, *supra* note 27, at 67–68 ("Software is rushed to market and shipped with default configurations that disable security features. Such software is replete with foreseeable vulnerabilities (e.g., buffer overflows, cross-site scripting, or unexpected operator attacks) because it trusts user input without testing to see whether the input is trustworthy. Even after many years and thousands of examples, software manufacturers still offer programs destined for security-related software failure."); Rustad & Koenig, *supra* note 28, at 1556.

120. *See infra* notes 121–27 and accompanying text. Rustad & Koenig explain the recent history of the courts' attitudes towards software manufacturers' use of adhesion contracts, stating:

> Prior to the mid-1990s, U.S. courts were reluctant to enforce adhesion contracts in the form of software agreements. However, the courts' attitudes have since changed in favor of broad enforceability of mass market license agreements; the

Consumers face numerous obstacles when pursuing potential remedies against software manufacturers. Software manufacturers traditionally use adhesion contracts,[121] making any remedy rooted in contract law significantly more difficult to attain.[122] Moreover, these contracts merely "license" the intellectual property of the underlying software, and at no point is the ownership of the software actually sold to the consumer.[123] Additionally, there is currently no defined standard of care for software manufacturers.[124] Without a standard of care, tort remedies are largely foreclosed.[125] In 2001, Congress amended the Computer Fraud and Abuse Act to prevent the possibility of bringing an action against software manufacturers for negligently manufactured software.[126] Without meaningful contract or tort remedies, "despite an epidemic of computer security flaws, no plaintiff has recovered damages for cyber crimes enabled by flawed software under any legal theory."[127]

Critics maintain that, as a consequence of the fundamental disincentives software manufacturers have to ensure adequate quality assurance, substantial negative externalities[128] have been imposed upon consumers,

---

> current trend is to enforce one-sided software agreements so long as the user has an opportunity to review and manifest assent to the terms.

Rustad & Koenig, *supra* note 28, at 1565.

121. *See* RICE, *supra* note 1, at 180–83. Rice describes how software adhesion contracts absolve software manufacturers of responsibility and accountability. *Id.* at 183.

122. See *infra* note 127.

123. *See* Rustad & Koenig, *supra* note 28, at 1562–67. The typical software industry shrinkwrap contract creates a "reverse unilateral contract." *Id.* at 1563. This contract typically disclaims any meaningful warranties, and makes litigation exponentially more difficult through unfavorable choice of law and forum selection clauses. *Id.* at 1564. As Rustad and Koenig explain, "[v]ery few consumers are even aware that they waive their implied warranty of merchantability, surrender their right to file suit in a court of law, and agree to submit to arbitration in a distant forum by the mere act of clicking on an icon labeled 'I agree.'" *Id.* at 1564; *see* RICE, *supra* note 1, at 181.

124. *See* RICE, *supra* note 1, at 184.

125. *Id.* (observing that "a claim for damages against a non-existent standard is impossible"); *see* Pinkney, *supra* note 27, at 46–47 ("A number of legal doctrines have constrained the market as well, at least historically. Several doctrines under the UCC coalesced to prevent effective contracting over liability for software failure. Furthermore, the common law disallowed recovery for the economic losses typical of software failure suits.").

126. 18 U.S.C. § 1030(g) (2006). The revision states, "No action may be brought . . . for the negligent design or manufacture of computer hardware, computer software, or firmware." *Id.* This revision was largely a response to several court decisions that expanded the scope of the existing Computer Fraud and Abuse Act to extend to market transactions, resulting in several software manufacturers being found liable for damages caused by vulnerabilities found in negligently manufactured software. *See* Pinkney, *supra* note 27, at 65; *see also* Shaw v. Toshiba Am. Info. Sys., Inc., 91 F. Supp. 2d 926 (E.D. Tex. 1999) (finding liability for the sale of floppy disk controllers containing faulty code).

127. RICE, *supra* note 1, at 184.

128. Externalities exist when self-interest prohibits the consequences of a particular course of action from being internalized by an actor because the consequences fall on another. *See* DUKEMINIER ET AL., PROPERTY 42 (6th ed. 2006). As David Rice explains, "Self-interest often wins over self-correction no matter how sublime or frivolous self-interest might be. In the story of software, then, the relationship between self-interest, incentives, and market failure is significant." RICE, *supra* note 1, at 42.

including the U.S. federal government.[129] In the context of inadequate software quality assurance, commentators believe that these externalities decrease information security, and in turn, weaken national and economic security.[130]

b. FISMA & NIST's Reluctance to Embrace Liability

Recall that NIST was established for the purpose of "develop[ing] standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets."[131] FISMA mandates agencies to implement and maintain information security policies and procedures consistent with NIST's technological requirements.[132] This section addresses the criticism that FISMA, in conjunction with NIST, attempts to ensure federal information security through reactionary standards designed to minimize the threat posed by insecure software, instead of proactively promulgating a regime that encourages software manufacturers to design safer software at the outset.[133] Consequently, the effectiveness of FISMA is severely undermined because FISMA fails to recognize that economic incentives that encourage manufacturers to minimize software insecurity in the design process can better promote federal information security than any technological requirements FISMA may advance.[134]

One critic highlights that NIST recognizes the importance of ensuring secure software from the development stage.[135] In a report containing a set of standards developed and promulgated by NIST for the U.S. Election Assistance Commission, NIST states, "experience in testing software and systems has shown that testing to high degrees of security and reliability is from a practical perspective not possible. Thus, one needs to build security, [and] reliability, . . . into the system design itself and perform a security fault analysis on the implementation of the design."[136] Despite recognizing that best practice dictates developing secure software and adequately testing the software prior to release,[137] "NIST has remained silent on how to do this as well as what a standard for software might look like."[138]

By failing to properly incentivize software manufacturers to internalize externalities, it is believed that FISMA is severely impaired from bolstering

129. The U.S. government is the single largest purchaser of information security products. *See* CSIS, *supra* note 72, at 56.

130. *See supra* note 114 and accompanying text.

131. 15 U.S.C. § 278g-3(a)(3) (2006).

132. 44 U.S.C. § 3544(a)(1)(B)(i) (2006).

133. *See* RICE, *supra* note 1, at xvii.

134. *See id.*; *see also infra* note 142 and accompanying text.

135. *See* RICE, *supra* note 1, at 285.

136. NAT'L INST. OF STANDARDS & TECH., REQUIRING SOFTWARE INDEPENDENCE IN VVSG 2007: STS RECOMMENDATIONS FOR THE TGDC 10 (2006), *available at* http://vote.nist.gov/DraftWhitePaperOnSIinVVSG2007-20061120.pdf.

137. *See id.*

138. RICE, *supra* note 1, at 286.

information security throughout federal agencies.[139] This is because every new piece of information security software introduced into federal agencies increases the overall entropy of the security framework established by FISMA.[140] One critic explains that as entropy increases, more logistical support is needed to ensure the adequate implementation of NIST standards and overall compliance with FISMA.[141] This creates a cycle of inefficiency where benefits hardly exceed costs.[142]

C. The New FISMA & Recent Developments in Information Security

In light of the numerous criticisms,[143] and a continual increase in security attacks within federal agencies,[144] commentators have proposed suggested changes to FISMA.[145] These proposals include holding software manufacturers strictly liable for security flaws under products liability theory[146] and the creation of a new cause of action for the negligent enablement of cybercrimes.[147] Additionally, incentive systems rooted in contract law have also been proposed.[148] Congress has also held numerous hearings to invite proposals to improve FISMA.[149] Most of the hearings yielded schemes designed to address agency compliance impediments and the underlying metrics FISMA uses to measure information security.[150]

---

139. *See infra* note 142 and accompanying text.

140. *See* RICE, *supra* note 1, at 287 ("In no case has a commercial security technology been introduced into the market that did not substantially increase the entropy of the system as a whole.").

141. *Id.*

142. *Id.* ("The painful irony of this situation is that . . . every security technology we introduce into the market simply slows down the applications and systems we are trying to protect. . . . Performance starts to lag. Firewalls slow down network traffic, anti-virus sucks down processor cycles on our laptops, intrusion detection systems consume network bandwidth with their logging information. In almost every case, the benefits of security technologies are fairly well matched against their costs. Added in sum, the costs start looking rather ridiculous. When we consider we are paying this money simply to further crash test yet more software applications, the costs seem utterly foolish.").

143. *See supra* Part I.B.1–3.

144. *See supra* note 61 and accompanying text.

145. *See infra* notes 146–50 and accompanying text.

146. *See* RICE, *supra* note 1, at 221–32; *see generally* Pinkney, *supra* note 27 (advocating that software manufacturers be subject to strict products liability).

147. *See* Rustad & Koenig, *supra* note 28, at 1553; *see also* RICE, *supra* note 1, at 232–36.

148. *See infra* Part II.C.

149. *See, e.g.*, *Agencies in Peril*, *supra* note 67; *Personal Information Hearing*, *supra* note 75; *Weaknesses Hearing*, *supra* note 61.

150. *See, e.g.*, *Weaknesses Hearing*, *supra* note 61, at 21–22 (statement of Gregory C. Wilshusen, Director, Information Security Issues at the Government Accounting Office) ("In prior reports, GAO [the Government Accountability Office] and IGs have made hundreds of recommendations to agencies for actions necessary to resolve prior significant control deficiencies and information security program shortfalls. For example, we recommended agencies correct specific information security deficiencies related to user identification and authentication, authorization, boundary protections, cryptography, audit and monitoring and physical security. We have also recommended that agencies fully implement comprehensive, agencywide information security programs by correcting weaknesses in risk assessments, information security policies and procedures, security planning, security training, system tests and evaluations, and remedial actions. The effective implementation of these recommendations will strengthen the security posture at these agencies."). Director

However, none of the hearings on FISMA or NIST addressed the issue of incentivizing software manufactures to ensure adequate information security software quality assurance.

After six years and numerous hearings, the Federal Information Security Management Act of 2008 was proposed to Congress.[151] The revised FISMA proposed to incorporate numerous changes, including heightened reporting and independent audits, among others.[152] The bill passed the Senate's Homeland Security and Governmental Affairs Committee, but the 110th Session of Congress ended before the bill could be put to a vote.[153] The bill has currently not been reintroduced into the new session of Congress. Thus, the question still remains how to best incentivize software manufacturers to ensure adequate software quality assurance.

II. COMPETING PROPOSALS OVER HOW BEST TO INCENTIVIZE SOFTWARE MANUFACTURERS

Having discussed FISMA, contemporary criticisms of FISMA, and the current state of the software industry in Part I, the controversy this Note seeks to address in Part II concerns how best to incentivize software manufacturers to ensure adequate software quality assurance within federal agencies. Part II.A analyzes proposals rooted in strict liability. Part II.B examines proposals rooted in general negligence theory, including a newly envisioned cause of action for the negligent enablement of cybercrime. Finally, Part II.C investigates proposals to incentivize software manufacturers that are rooted in contract law.

A. Strict Products Liability

Many commentators believe that strict products liability presents the best vehicle to incentivize the software industry to ensure adequate software quality assurance. This section first explores the arguments offered to support the application of strict liability to the software industry, before examining the disadvantages of a strict liability standard.

1. The Case for Strict Liability

Greenman v. Yuba Power Products, Inc.[154] was one of the first cases to allow a plaintiff to recover damages for an injury sustained from using a power tool on a theory of liability that "relied neither on proof of fault nor

Wilshusen then proceeded to specifically propose clearer requirements for testing and evaluating security controls, enhancing FISMA reporting requirements, and conducting annual independent evaluations in accordance with audit standards or a common approach and framework. *Id.* at 26–31.

151. S. 3474, 110th Cong. (2008).

152. *Summary of S. 3474: Federal Information Security Management Act of 2008*, GOVTRACK.COM, http://www.govtrack.us/congress/bill.xpd?bill=s110-3474&tab=summary (last visited Sept. 23, 2010).

153. *Id.*

154. 377 P.2d 897 (Cal. 1963).

on warranty."[155] Approximately two years later, the American Law Institute promulgated Section 402A of the Restatement of Torts, which recommended courts impose strict liability on manufacturers for defective products by finding liability even when "the seller has exercised all possible care in the preparation and sale of his product."[156] Numerous rationales for strict liability have developed in courts over time.[157] These rationales generally hold that (1) proving negligence is too burdensome for plaintiffs because manufacturers control the production process,[158] (2) manufacturers are in the best position to absorb and spread the cost of any injury their product causes,[159] (3) strict liability incentivizes manufacturers to produce safer products,[160] and (4) contractual remedies cannot be trusted to adequately protect the consumer.[161]

Commentators believe that many of the barriers strict products liability was designed to overcome are pervasive in the software industry, and this lends support to extending strict products liability to software manufacturers.[162] Several observations support this idea. First, proving negligence is too burdensome for plaintiffs because software is becoming increasingly complex and consumers can no longer be expected to adequately test software products for defects.[163] As one commentator explains:

> When purchasing a computer it is common for the original hardware to come from one supplier, the firmware from a second supplier, and the installed operating system from the third supplier using configuration

155. GOLDBERG ET AL., TORT LAW: RESPONSIBILITIES AND REDRESS 843 (2008).

156. RESTATEMENT (SECOND) OF TORTS § 402A (1965).

157. *See, e.g*, Escola v. Coca Cola Bottling Co., 150 P.2d 436, 467 (Cal. 1944) (Traynor, J., concurring); FRANK J. VANDALL, STRICT PRODUCTS LIABILITY 17–28 (1989); Gregory C. Keating, *The Theory of Enterprise Liability and Common Law Strict Liability*, 54 VAND. L. REV. 1285, 1298 (2001); William L. Prosser, *The Assault Upon the Citadel (Strict Liability to the Consumer)*, 69 YALE L.J. 1099, 1116–24 (1960); Roger J. Traynor, *The Ways and Meanings of Defective Products and Strict Liability*, 32 TENN. L. REV. 363, 365–66 (1965); Pamela T. Westfall, Note, *Hepatitis, AIDS and the Blood Product Exemption from Strict Products Liability in California: A Reassessment*, 37 HASTINGS L.J. 1101, 1106–08 (1986).

158. *See Escola*, 150 P.2d at 443 ("Manufacturing processes, frequently valuable secrets, are ordinarily either inaccessible to or beyond the ken of the general public. The consumer no longer has means or skill enough to investigate for himself the soundness of a product."); VANDALL, *supra* note 157, at 21–22.

159. *Greenman*, 377 P.2d at 901. For additional analysis of this rationale, see Prosser, *supra* note 157, at 1120. Interestingly, this particular rationale was at one point controversial, with one commentator going so far as to call it a step towards socialism. *Id.*

160. *See Escola*, 150 P.2d at 462; *see also* VANDALL, *supra* note 157, at 21; Prosser, *supra* note 157, at 1119 ("It is said . . . that strict liability will provide a healthy and highly desirable incentive for producers to make their products safe."); Traynor, *supra* note 157, at 366.

161. The doctrine of strict products liability was largely a reaction to the "remarkable legal gymnastics" courts were engaging in to impose liability through contract law for injuries sustained by a defective product. Prosser, *supra* note 157, at 1118; *see* VANDALL, *supra* note 157, at 17–19.

162. *See infra* notes 163–83 and accompanying text.

163. *See* RICE, *supra* note 1, at 219; Frances E. Zollers et al., *No More Soft Landings for Software: Liability for Defects in an Industry That Has Come of Age*, 21 SANTA CLARA COMPUTER & HIGH TECH. L.J. 745, 755 (2005).

> (system settings) from yet a fourth supplier. Add extra hardware, e.g., a Network card, from a second hardware supplier that alters firmware settings and uses drivers from yet another party. The drivers alter the way the operating system works and interacts with all other hardware; the new hardware itself interacts directly with the extant hardware. The hardware, firmware, and software were all designed, built, and tested by humans who are fallible. The original specification was created by a human as were the manuals for the end users. Failure at any stage can result in the aspirations of the user not being met. When dashed expectations also lead to injury and death, it is almost impossible for the injured party to pinpoint exactly what went wrong and who is responsible. Strict liability is seemingly appropriate for these very reasons.[164]

While the commentator believes strict liability is appropriate only when software defects lead to physical injury or death, other commentators think strict liability is warranted regardless of physical injury or death.[165] The argument holds that if consumers cannot be expected to adequately inspect common household tools like a lawnmower or chainsaw prior to purchase, consumers should not be expected to adequately inspect software.[166]

Second, consistent with the *Greenman* court's rationale for finding a products manufacturer strictly liable,[167] it has been argued that good public policy demands holding software manufacturers strictly liable for damage caused by faulty software.[168] The lack of tools available to law enforcement to combat transnational cybercrime,[169] China and Russia's increasing efforts to exploit software vulnerabilities for commercial and

---

164. Zollers, *supra* note 163, at 755.

165. *See* RICE, *supra* note 1, at 219; Pinkney, *supra* note 27, at 82.

166. *See* RICE, *supra* note 1, at 219.

167. *Greenman v. Yuba Power Prods., Inc*, 377 P.2d 897, 901 (Cal. 1963). In *Greenman*, Justice Traynor alluded to his own concurrence in *Escola v. Coca Cola Bottling Co.*, 150 P.2d 436, 467 (Cal. 1944), where he stated:

> Even if there is no negligence, however, public policy demands that responsibility be fixed wherever it will most effectively reduce the hazards to life and health inherent in defective products that reach the market. It is evident that the manufacturer can anticipate some hazards and guard against the recurrence of others, as the public cannot . . . . It is to the public interest to discourage the marketing of products having defects that are a menace to the public. . . . Against such a risk there should be general and constant protection and the manufacturer is best situated to afford such protection.

150 P.2d 436, 440–41 (Cal. 1944) (Traynor, J., concurring).

168. *See* RICE, *supra* note 1, at 219–20; Zollers, *supra* note 163, at 782.

169. *See* Tom Espiner, *Interpol: Give Us Tools To Fight Cybercrime*, CNET NEWS (Mar. 21, 2006), http://news.cnet.com/Interpol-Give-us-tools-to-fight-cybercrime/2100-7348_3-6052249.html; *see generally* ROLLINS & HENNING, *supra* note 107 (analyzing the existing U.S. statutory framework and constitutional authority for combating cyberattacks); Mike Keyser, Note, *The Council of Europe Convention on Cybercrime*, 12 FLA. ST. J. TRANSNAT'L L. & POL'Y 287 (2003) (providing a detailed overview of the European Convention on Cybercrime); Jennifer J. Rho, Comment, *Blackbeards of the Twenty-First Century: Holding Cybercriminals Liable Under the Alien Tort Statute*, 7 CHI. J. INT'L L. 695 (2007) (highlighting current deficiencies in curbing international cybercrime and proposing cybercriminals be held liable under the Alien Tort Statute).

political gain,[170] and record highs of general cybercrime rates[171] are all cited as reasons why strict liability should be imposed on software manufacturers.[172] This argument is premised on the belief that software manufacturers are best positioned to prevent larger disorder caused by inadequate software quality assurance.[173]

Third, critics believe that contract law fails to offer consumers meaningful remedies for damage caused by inadequate software quality assurance.[174] As noted in Part I, software manufacturers rely on adhesion contracts and complex licensing agreements to shield themselves from contractual liability.[175] It is contended that this is not altogether different from the legal landscape that initially spurred the adoption of strict products liability in the early 1960s.[176] As one commentator explains, without a strict liability regime that reallocates the risk from the consumer to the manufacturer, software manufacturers will never provide warranties to remedy consumer losses.[177]

Finally, critics maintain that software manufacturers are the "least-cost avoider[s]"[178] and subjecting software manufacturers to strict products liability would incentivize the production of better, safer software.[179] The argument holds that strict liability would incentivize software manufacturers by eradicating "the notion that software may be 'incrementally improved' at the expense of consumers and national

---

170. The People's Republic of China is currently developing an "informationalized" army comprised of computer experts manning terminals, in contrast to soldiers manning tanks. *See* Jurich, *supra* note 1, at 278. Many U.S. officials and experts "of all political persuasions" throughout government and private industry feel China is behind many of the most "egregious" cyberattacks on the United States; one senior Air Force official has estimated that, "as of two years ago, China has stolen at least 10 to 20 terabytes of data from U.S. government networks—the larger figure equal, by some estimates, to one-fifth of the Library of Congress's digital holdings." Ellen Nakashima & John Pomfret, *China Proves To Be an Aggressive Foe in Cyberspace*, WASH. POST (Nov. 11, 2009), http://www.washingtonpost.com/wp-dyn/content/article/2009/11/10/AR2009111017588.html.

171. Press Release, Internet Crime Complaint Center, IC3 2008 Annual Report on Internet Crime Released (Mar. 31, 2009), *available at* http://www.ic3.gov/media/2009/090331.aspx ("[O]nline crime hit a record high in 2008. IC3 received a total of 275,284 complaints, a 33.1% increase over the previous year."); *see* ROLLINS & HENNING, *supra* note 107, at 2 ("Threats to the U.S. cyber and telecommunications infrastructure are constantly increasing . . . .").

172. *See* RICE, *supra* note 1, at 219.

173. *See id.*; *see supra* note 159 and accompanying text.

174. *See* RICE, *supra* note 1, at 182; *see supra* notes 121–23 and accompanying text.

175. *See supra* notes 121–23 and accompanying text.

176. *See supra* note 161 and accompanying text.

177. Emily Kuwahara, Note, *Torts v. Contracts: Can Microsoft Be Held Liable to Home Consumers for Its Security Flaws?*, 80 S. CAL. L. REV. 997, 1015 (2007).

178. *See* RICE, *supra* note 1, at 218 ("[S]oftware manufacturers are better able to bear the financial burden of addressing software weaknesses than buyers of software. In short, it makes more sense to assign the task of securing software to a relatively small number of software manufacturers compared to burdening the software's 500 million potential users with the responsibility. It is also far cheaper in financial and social costs to make software manufacturers the least-cost avoider."). *But see* Rustad & Koenig, *supra* note 28, at 1605–06 (advocating negligence liability because there may be occasions where the plaintiff is the least-cost avoider).

179. *See* Zollers, *supra* note 163, at 769; *see also* RICE, *supra* note 1, at 232.

infrastructure."[180] Specifically, imposing strict liability would remove the first-to-market mentality with which the software industry operates,[181] and would shift the responsibility for adequately testing software from the consumer to the manufacturer.[182] Faced with strict liability, software manufacturers would be forced to take extra measures to protect themselves from future liability.[183]

2. Strict Liability: Limitations & Disadvantages

The previous section analyzed the argument that imposing strict products liability on the software industry is consistent with the larger rationales of strict liability. It also evaluated the argument that strict liability would incentivize software manufacturers to ensure adequate software quality assurance. This section assesses the doctrinal limitations that work to shield software manufacturers from strict products liability and then discusses perceived policy disadvantages that commentators believe would flow from subjecting software manufacturers to strict products liability.

a. Doctrinal Limitations

Despite the advantages of strict products liability[184] and the potential for the doctrine to incentivize better software quality assurance,[185] many believe that this is impossible to achieve in light of various doctrinal hurdles.[186] First, there is a debate over whether or not software constitutes a "product" for purposes of applying strict products liability.[187] Some point to the Restatement of Torts,[188] which defines "product" as "tangible personal property,"[189] and deliberately excludes "information" from the definition[190] as a reason why strict liability is not the appropriate vehicle to incentivize software manufacturers.[191] This interpretation is aided by the observance that, while courts generally extend the definition of "goods" to include "software" for purposes of applying the Uniform Commercial Code

180. *See* RICE, *supra* note 1, at 232.

181. *See id.* For an explanation of the specific motivating forces behind the "first-to-market" mentality, see *supra* notes 117–20 and accompanying text.

182. *See* RICE, *supra* note 1, at 232; *see* Zollers, *supra* note 163, at 771.

183. *See* RICE, *supra* note 1, at 232; *see also supra* note 160 and accompanying text.

184. *See supra* notes 158–83 and accompanying text.

185. *See supra* notes 179–83 and accompanying text.

186. *See infra* notes 187–201 and accompanying text.

187. *Compare* Rustad & Koenig, *supra* note 28, at 1581 ("Software is neither a good nor a product, but rather an intangible collection of digital information: code composed of 1s and 0s."), *with* Kuwahara, *supra* note 177, at 1018–20 (explaining how courts generally classify software as a "product" for purposes of applying the Uniform Commercial Code), *and* Zollers, *supra* note 163 at 760 (finding software sufficiently analogous to aeronautical charts and books to warrant classification as a "product").

188. RESTATEMENT (THIRD) OF TORTS: PRODUCTS LIABILITY § 19(a) (1998).

189. *Id.*

190. *Id.* § 19(a) cmt. d.

191. *See generally* David W. Lannetti, *Toward a Revised Definition of "Product" Under the Restatement (Third) of Torts: Products Liability*, 55 BUS. LAW. 799 (2000) (arguing that the current definition of "product" in the Restatement precludes software).

(U.C.C.),[192] courts have been reluctant to stretch this interpretation to permit a strict products liability theory of recovery against software manufacturers.[193]

Other problems also plague the application of the strict products liability doctrine to software manufacturers. Even if software were considered a "product" for purposes of allowing strict liability to attach, plaintiffs would still struggle to prove design defect. The issue of what criteria should be used when evaluating what constitutes a design defect is one of the most contested debates in products liability law.[194] Generally, the concepts of risk balancing, utility, and the availability of an alternative design are employed in some fashion.[195] At least one commentator feels that plaintiffs would likely lose if these concepts are employed when evaluating a software operating system design, such as Microsoft Windows.[196]

Finally, even if a plaintiff could prove that software was a product that was defectively designed, the economic loss rule effectively forecloses the possibility of drastically incentivizing software manufacturers. While actors are generally prohibited from engaging in behavior that may cause reasonably foreseeable damage to tangible property, "they have no such general obligation to avoid depriving persons of economic prospects."[197] Accordingly, deleted files,[198] damage caused by the misappropriation of data,[199] and damage caused by denial-of-service attacks would not constitute proper "damage" for purposes of recovery.[200] This economic loss rule reinforces the prevailing belief that software manufacturers should be shielded from liability for countervailing public policy reasons.[201]

---

192. *See* Kuwahara, *supra* note 177, at 1018–20 (explaining how courts generally apply the Uniform Commercial Code (UCC) Article 2 on the sale of goods to software and the rationale for courts doing so). *But see* Rustad & Koenig, *supra* note 28, at 1581 ("Software is licensed with restrictions on the conditions of use and is therefore unlike tangible products that can be used at the discretion of the purchaser. Network security software is frequently a hybrid of sales and services."). Although courts generally find software to be a "product," the decision to apply Article 2 of the UCC generally turns on whether the complex licensing agreements used by software manufacturers constitute a "sale." Kuwahara, *supra* note 177, at 1018.

193. *See* Farhah Abdullah, *Strict Versus Negligence Software Product Liability*, 2 COMPUTER & INFO. SCI. 81, 86 (2009).

194. *See* GOLDBERG ET AL., *supra* note 155, at 875.

195. *Id.*

196. *See* Kuwahara, *supra* note 177, at 1024 ("[T]he utility and productivity resulting from . . . product integration far outweigh[s] any risks. Given the complexity of building an operating system, showing a reasonable alternative to the court—in other words, designing a new operating system—would be a near impossible task.").

197. GOLDBERG ET AL., *supra* note 155, at 97; *see* Kuwahara, *supra* note 177, at 1025–26 ("The most common injuries in a cybersecurity case will be the loss of data, financial harm, dignitary injury, and an invasion of privacy—all damages that cannot be characterized as physical injuries or damage to 'other property.'"); *see also* NMP Corp. v. Parametric Tech. Corp., 958 F. Supp. 1536, 1546–47 (N.D. Okla. 1997) (rejecting software manufacturer liability based on the economic loss rule). See Rustad & Koenig, *supra* note 28, at 1580 for a detailed analysis of the *Parametric* case.

198. *See* Kuwahara, *supra* note 177, at 1026–29.

199. *Id.* at 1029–30.

200. *Id.* at 1030–31.

201. *Id.*; *see infra* notes 202–09 and accompanying text.

b. Policy Disadvantages

Many commentators believe that subjecting software manufacturers to strict products liability would be inconsistent with sound public policy even if Congress or the courts were to carve an exception to the limitations described above. First, it has been alleged that subjecting software manufacturers to strict products liability cannot solve the problem of defective software.[202] This is because any piece of software, and the interactions the software has with other software, is so complex that it is impossible to design and test a program that could operate as planned in an infinite number of environments.[203] This is, to some degree, supported by an empirical study that concluded that "[o]ne defect is injected for every 7 to 10 lines of new and changed [software] code produced."[204] However, critics dispute the ultimate meaning of software complexity. The same empirical study found that the top twenty Internet vulnerabilities are all caused by "poor coding, testing and sloppy software engineering . . . [and that] [t]echnical solutions exist to them all, but they are simply not implemented."[205]

In addition to potentially incentivizing solutions to a problem that cannot be fixed, critics also believe that strict liability would stifle innovation, over-deter risk taking, and stunt the growth of the software industry.[206] If one party bears all foreseeable and unforeseeable risk,[207] that party may avoid the benefits associated with innovation because they cannot accurately gauge the scope of the risk associated with innovation.[208] Even if software manufacturers did decide to continue producing innovative products in the face of uncertain legal liability, one disastrous injury could subject a manufacturer to "ruinous liability."[209] Critics counter that the software manufacturing industry is a multi-billion dollar industry dominated by a limited number of companies among product categories and is therefore mature enough to handle strict products liability exposure.[210]

---

202. *See* Zollers, *supra* note 163, at 769

203. *See id.* ("There are those who claim that there is no such thing as 'bug-free software.'").

204. Noopur Davis, *Developing Secure Software*, 8 SOFTWARE TECH NEWS (July 2005), http://www.softwaretechnews.com/stn_view.php?stn_id=2&article_id=34.

205. Davis, *supra* note 204. At least one critic believes the complexity of software coding actually supports the application of strict products liability because it relieves potential plaintiffs from having to prove negligence, which could be substantially more difficult. Zollers, *supra* note 163, at 769–70. Zollers also argues that the relative market monopoly software manufacturers gain through patents on specific technologies makes strict liability a small price to pay. *Id.* at 770–71.

206. *See* RICE, *supra* note 1, at 215–16. *But see* Zollers, *supra* note 163, at 771–73.

207. *See* RICE, *supra* note 1, at 215–16. This is one of the fundamental distinctions between strict liability and ordinary negligence.

208. *See* Rustad & Koenig, *supra* note 28, at 1579 ("In most cases, an empirically-based risk/benefit calculation is impossible because information concerning the foreseeable likelihood of a computer intrusion and the burden of risk-prevention measures is limited.").

209. Kuwahara, *supra* note 177, at 1030–31.

210. *See* Zollers, *supra* note 163, at 779–80. As Zollers explains, "The industry is consolidating and strengthening, and large market players have emerged as dominant forces in the economy. . . . These companies . . . have the . . . resources to devote to . . . extra

B. Negligence

The previous section analyzed the potential use of strict products liability to incentivize software manufactures to ensure heightened software quality assurance, as well as the perceived disadvantages to imposing such liability. This section examines the viability of applying negligence liability to incentivize software manufacturers. Specifically, this section explores the "Negligent Enablement of Cybercrime," a theoretical tort proposed by Professors Michael L. Rustad and Thomas H. Koenig in 2005.[211] Finally, this section examines the disadvantages to negligence-based liability rules.

1. The Negligent Enablement of Cybercrime

Due to the high risk of computer intrusions,[212] Rustad and Koenig proposed that courts embrace a modified duty of care[213] that would require software manufacturers to incorporate reasonable security measures into software.[214] Based on premise liability,[215] warranty,[216] and negligence-based products liability,[217] the negligent enablement of cybercrime tort would "provide injured consumers and users with remedies when defective software paves the way for cybercrime."[218]

According to Rustad and Koenig, a new cause of action for the negligent enablement of cybercrime would have several distinct advantages. First, the tort recognizes that software manufacturers are most capable and best

---

testing . . . [and] to pay for injuries that may result from defects." *Id.* at 782. Some commentators have cited the reform and success of the automobile industry in the face of strict products liability to support the imposition of strict products liability on software manufacturers. *See* RICE, *supra* note 1, at 219–20; Rustad & Koenig, *supra* note 28, at 1608. *See generally* CORNELIUS W. GILLAM, PRODUCTS LIABILITY IN THE AUTOMOBILE INDUSTRY 185–95 (1960) (explaining the successful reform brought about by subjecting the automobile industry to strict products liability).

211. *See* Rustad & Koenig, *supra* note 28, at 1553.

212. *See id.* at 1557; *supra* note 105 and accompanying text (highlighting the existence of 40,000 known software vulnerabilities).

213. Rustad and Koenig proposed that this modified duty be determined by the balancing of factors such as

> the foreseeability of the harm of computer viruses or other breaches of security; the degree of certainty between software vulnerabilities and harm; the connection between lax internet security practices and the injury suffered by a computer user; the policy of preventing future intrusions; the burden on the information industry and the consequences to the community of imposing a duty to maintain adequate security; and the availability, costs, and prevalence of security solutions and insurance.

Rustad & Koenig, *supra* note 28, at 1586. *But see* Kuwahara, *supra* note 177, at 1004 ("[Requiring foreseeability] makes it more difficult for plaintiffs who are not security experts to bring suit, while doing nothing to limit damages for a widespread . . . attack.").

214. *See* Rustad & Koenig, *supra* note 28, at 1557.

215. *See id.* at 1558. In their analysis, Rustad and Koenig argue that negligent software manufacturers expose their customers to "predators" not unlike a retail store that "fails to employ security guards in a high crime area." *Id.* at 1582.

216. *Id.* at 1558.

217. *Id.*

218. *Id.*

positioned to mitigate foreseeable cybercrime[219] and, as a result, reallocates the cost of foreseeable cybercrimes from the consumer to the manufacturer.[220] Rustad and Koenig believe that this would properly incentivize software manufacturers to "allocat[e] more resources to preventing cybercrime through better design, fortified product warnings, and more thorough testing."[221] The result of this reallocation of resources would be safer, more secure software, and less cybercrime.[222]

Second, Rustad and Koenig argue that a negligent enablement of cybercrime cause of action is preferable to a strict products liability rule.[223] This argument is rooted in the belief that courts would be more receptive to imposing a negligence-based liability rule on software manufacturers.[224] Contemporary products liability law is experiencing a "pronounced" shift away from strict liability and courts are once again favoring negligence.[225] Additionally, Rustad and Koenig believe that while courts have been unwilling to extend strict products liability to pure economic losses, courts may be more willing to "recognize a negligent enablement theory of product liability where prior similar computer intrusions signal a software manufacturer's ill-considered design decisions."[226]

Third, it is believed that a negligent enablement of cybercrime tort would reward socially responsible software manufactures,[227] which would have the effect of reshaping the software manufacturing industry.[228] Finally, a negligence-based liability rule recognizes that plaintiffs are occasionally in a better position to avoid or minimize the risk of cybercrime.[229] As a result, a negligence-based liability rule affords greater protection and flexibility to defendants by allowing contributory negligence, comparative negligence, and assumption of risk defenses.[230]

---

219. *Id.* at 1598; *see* Michael D. Scott, *Tort Liability for Vendors of Insecure Software: Has the Time Finally Come?*, 67 MD. L. REV. 425, 444 (2008) ("Because vendors (meaning developers and suppliers of the software) generally distribute only the machine-readable object code of their products, they are the only ones who know the actual level of security of their software and, therefore, are the only ones who can isolate and repair the problems.").

220. *See* Rustad & Koenig, *supra* note 28, at 1598.

221. *Id.* at 1608–09.

222. *See id.* at 1610.

223. *See infra* notes 225–26 and accompanying text.

224. *See infra* notes 225–26 and accompanying text.

225. *See* Rustad & Koenig, *supra* note 28, at 1609. As Professor William M. Landes and Judge Richard A. Posner explain, the costs associated with administering a liability rule may be divided into "information costs" and "claim costs." Information costs are empirically higher under a negligence rule, and claim costs are higher under a strict liability rule. However, because of the decline in information costs due to increased "literacy and knowledge of how the physical world operates" courts have moved away from strict liability and towards negligence as the "dominant rule of liability." WILLIAM M. LANDES & RICHARD A. POSNER, THE ECONOMIC STRUCTURE OF TORT LAW 65–66 (1987).

226. Rustad & Koenig, *supra* note 28, at 1580. *But see* Kuwahara, *supra* note 177, at 1003 ("Why courts may favor this negligence theory over strict products liability theory for the same purely economic damage remains unclear.").

227. *See* Rustad & Koenig, *supra* note 28, at 1610.

228. *See id.*

229. *Id.* at 1606.

230. *Id.* at 1604–07.

2. Disadvantages to a Negligence-Based Liability Rule

The previous section introduced and highlighted the purported advantages to the "Negligent Enablement of Cybercrime," a theoretical tort proposed by Rustad and Koenig in 2005. Putting aside that Congress has explicitly foreclosed any negligence-based liability for software manufacturers,[231] this section addresses common difficulties associated with a negligence-based liability rule, and the perceived policy disadvantages that commentators believe would flow from subjecting software manufacturers to negligence-based liability.

Rustad and Koenig admit courts may "grapple" with causation problems when adjudicating disputes where the negligent enablement of cybercrime is alleged.[232] Specifically, "redundant multiple causes would preclude liability under the 'but for' analysis."[233] Even the "substantial factor" test adopted by the Restatement of Torts[234] may prove difficult for courts to implement when multiple security flaws exist, or when security flaws on multiple networks are exploited in a cybercrime.[235] Furthermore, in the absence of empirical studies analyzing the frequency and cost of software exploitation, "it may prove difficult to evaluate the radius of the risk created by insecure software."[236] Thus, courts may also struggle to determine a meaningful standard by which to analyze proximate cause.[237] Increased uncertainty over the application of the negligent enablement tort could potentially disincentivize software manufacturers from implementing adequate software quality assurance standards.[238]

From a more general perspective, critics maintain that a negligence-based liability rule may disincentivize plaintiffs, which would fail to properly incentivize software manufacturers and could potentially lead to under-deterrence.[239] This is explained by the high administrative costs associated with proving negligence.[240] Plaintiffs must prove duty, breach, causation,

---

231. 18 U.S.C. § 1030(g) (2006); *see supra* note 126 and accompanying text.
232. *See* Rustad & Koenig, *supra* note 28, at 1601.
233. *Id.* (quoting JOHN DIAMOND, UNDERSTANDING TORTS 202 (1999)).
234. RESTATEMENT (SECOND) OF TORTS § 435 (1965).
235. *See* Rustad & Koenig, *supra* note 28, at 1601.
236. *See id.* at 1602.
237. *See id.*
238. *See* THOMAS J. MICELI, ECONOMICS OF THE LAW 45 (1997) ("[U]ncertainty about the due standard may result in . . . too little care compared to the social optimum."). Professor Miceli identifies two areas of uncertainty that may disincentivize software manufacturers: (1) uncertainty by injurers about the due standard, and (2) errors by the court in determining compliance with the negligence standard. *Id.* at 45–46. According to Miceli, both have the possibility of leading to either over-deterrence or under-deterrence. *Id.; see* LANDES & POSNER, *supra* note 225, at 234–51 (using an economic approach to torts to prove situations where uncertainty over causation could lead to over or under-deterrence).
239. *See* RICE, *supra* note 1, at 216–17 ("[T]he expense of pursuing a negligence suit can act as a disincentive to plaintiffs that should otherwise be willing to file suit for actual harm. This can result in under-deterrence . . . ."); *see also* MICELI, *supra* note 238, at 43 (explaining how litigation costs interact with a manufacturer's incentive to comply with the standard of due care).
240. *See* RICE, *supra* note 1, at 216.

and damages.[241] Demonstrating that a software manufacturer was negligent could become exceedingly expensive because an individual piece of software's development lifecycle may not include legal process constraints, and the development process may need to be evaluated from "meager process documentation."[242] Consequently, high administrative costs function to discourage potential plaintiffs and may result in under-deterrence because software manufacturers are not "bearing the full cost of their risky activities."[243] Finally, imposing a standard of care on software manufacturers too early in the development stage may stifle innovation and deter software manufacturers from pursuing innovative approaches to improve security.[244]

C. Contract Remedies

Parts II.A and II.B analyzed incentive systems rooted in tort liability. This section evaluates the potential for contract law to incentivize software manufacturers to ensure adequate software quality assurance. This section examines the current state of contract law with respect to software licensing agreements. Finally, this section analyzes potential solutions designed to incentivize software manufacturers through contract law.

1. The Software Licensing Agreement: Disincentivizing Software Manufacturers

Contract law applies to a substantial majority of software cases because they involve pure economic loss.[245] While courts initially struggled to classify software as a "good" for the purposes of applying the U.C.C.,[246] modern courts have generally determined that software is a "good," and therefore that the U.C.C. does apply.[247] Consequently, the U.C.C. allows

241. *See* GOLDBERG ET AL., *supra* note 155, at 48. For a further explanation of the specific criteria that may be used to construct the duty element, see *supra* note 213.

242. *See* Clark Savage Turner & Foaad Khosmood, Rethinking Software Process: The Key to Negligence Liability 1–2 (2007) (unpublished manuscript), *available at* http://users.csc.calpoly.edu/~csturner/rethinking.pdf. "Process documentation" describes documents that are generated during the software development process to record the process by which software is created and maintained. Thus, when software manufacturers develop software in an environment free of regulations designed to ensure compliance with applicable legal standards, plaintiffs must rely on process documentation. *Id.* at 1–3.

243. RICE, *supra* note 1, at 216. *But see* LANDES & POSNER, *supra* note 225, at 64 (arguing that strict liability will not cause manufacturers to take any more due care than a negligence liability rule).

244. *See* Kuwahara, *supra* note 177, at 1004.

245. *See* Zollers, *supra* note 163, at 764.

246. *See* Kuwahara, *supra* note 177, at 1018. The initial difficulty stemmed from software that was custom-made for a consumer. Courts generally found such software to be a "service" and thus subject to common law negligence and contracts doctrines. *Id.*

247. *See* Zollers, *supra* note 163, at 765; *see also* Kuwahara, *supra* note 177, at 1020 (speculating various rationales for courts finding software to constitute a "good"). Another potential obstacle manifests itself in the license agreement and whether or not the agreement constitutes a "sale." Courts have traditionally found that software-licensing agreements constitute a sale. *See* Zollers, *supra* note 163, at 765–66. It should be noted that this analysis excludes the Uniform Computer Information Transaction Act (UCITA) because only two

software manufacturers to disclaim nearly all warranties[248] and to limit damages for unforeseeable liability.[249] Consider the following licensing agreement:

> THIS SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.[250]

This hypothetical licensing agreement is representative of the typical software license agreement.[251] Courts traditionally uphold such contracts.[252] Thus, "[t]he software user, by agreeing to the language in a software license, forgoes any right to pursue legal action against the seller and accepts the full weight and burden of risk for using the software."[253] This functions as a disincentive for software manufacturers to ensure adequate software quality assurance.[254]

---

states have currently adopted UCITA. *See* Kuwahara, *supra* note 177, at 1020. However, were UCITA to be broadly adopted, it is unlikely that software manufacturers would ever face liability. *Id.* at 1020–21.

248. U.C.C. § 2-316 (2005). Indeed, the U.C.C. seems to encourage the disclaimer of warranties. *See* R. Joseph Barton, Note, *Drowning in a Sea of Contract: Application of the Economic Loss Rule to Fraud and Negligence Misrepresentation Claims*, 41 WM. & MARY L. REV. 1789, 1826 (2000); *see also* KNAPP ET AL., PROBLEMS IN CONTRACT LAW 507 (2007).

249. U.C.C. § 2-316(4) (2005).

250. RICE, *supra* note 1, at 179.

251. *Id. Cf.* Apple iTunes Software Product Agreement, http://images.apple.com/legal/sla/docs/itunes.pdf, at 1 (last visited Sept. 23, 2010) ("APPLE . . . HEREBY DISCLAIM[S] ALL WARRANTIES . . . EITHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES AND/OR CONDITIONS OF MERCHANTABILITY . . . OF FITNESS FOR A PARTICULAR PURPOSE . . . APPLE DOES NOT WARRANT . . . THAT THE OPERATION OF THE APPLE SOFTWARE OR SERVICE WILL BE UNINTERRUPTED OR ERROR-FREE, OR THAT DEFECTS IN THE APPLE SOFTWARE OR SERVICES WILL BE CORRECTED. NO ORAL OR WRITTEN INFORMATION OR ADVICE GIVEN BY APPLE . . . SHALL CREATE A WARRANTY.").

252. *See* Kuwahara, *supra* note 177, at 1023; *see also* RICE, *supra* note 1, at 182 ("The current legal trend in the United States is to enforce one-sided software agreements as long as the user has an opportunity to read and 'manifest assent' to the terms."). Software license agreements generally contain a minimal remedy to avoid being declared unconscionable. *See* Kuwahara, *supra* note 177, at 1023.

253. RICE, *supra* note 1, at 180.

254. *See supra* notes 127–29 and accompanying text.

2. A Proposed Solution Rooted in Contract Law

Many commentators have dismissed the idea that contract law could be used as a vehicle to properly incentivize software manufacturers[255] given the obstacles erected by licensing agreements.[256] However, at least one commentator believes contract law has the potential to properly incentivize software manufacturers should specific reform be enacted. These reforms center on the imposition of a "mandatory warranty" that would "restrict software vendors' ability to disclaim liability, while capping damages to a predetermined amount."[257] The mandatory warranty would allow for the recovery of consequential damages[258] in the event that a security flaw within the software caused the damages.[259]

A mandatory warranty is claimed to have the ability to incentivize software manufacturers for one primary reason: unlike strict products liability or negligence, a "breach of warranty claim permits recovery for economic losses."[260] The mandatory warranty encourages consumers to maintain reasonable security while also incentivizing software manufacturers to produce software with fewer vulnerabilities because the consumer's conduct may be considered in warranty disputes.[261] Hence, the mandatory warranty promotes the "same policy goals that drive the desire to impose tort liability . . . while appropriately limiting liability."[262] Finally, a mandatory warranty is alleged to be easier to implement than a negligence or strict liability rule because it circumvents the need to analogize software to tangible products[263] or carve out exceptions to the economic loss doctrine.[264]

Of course, it is theorized that a mandatory warranty would be burdened by several perceived disadvantages. Demonstrating causation with respect to consequential damages could prove difficult.[265] This could present a "high bar" for potential plaintiffs.[266] Additionally, quantifying damages may also prove difficult.[267] Finally, drawing appropriate lines of liability may prove to be a complicated endeavor.[268] Due to these limitations, it has

255. *See* RICE, *supra* note 1, at 179–85; Rustad & Koenig, *supra* note 28, at 1562–67; Zollers, *supra* note 163, at 757–58.
256. *See supra* Part II.C.1.
257. Kuwahara, *supra* note 177, at 1032.
258. *Id.* Consequential damages are defined by the U.C.C. to include "injury to person or property proximately resulting from any breach of warranty." U.C.C. § 2-715(2)(b) (2005).
259. *See* Kuwahara, *supra* note 177, at 1032.
260. *Id.* at 1032; *see* Scott, *supra* note 219, at 453–54. *See generally* Barton, *supra* note 248 (identifying and explaining the various exceptions carved out in the economic loss rule).
261. *See* Kuwahara, *supra* note 177, at 1032–34.
262. *Id.* at 1034.
263. *Id.* at 1032.
264. *Id.*
265. *Id.*
266. *Id.*
267. *See id.* at 1033.
268. *Id.*

been suggested that damages should be capped at a pre-determined amount, and revisiting the cap approximately every two years for reevaluation.[269]

III. THE TIME IS NOW FOR REFORM: FISMA REFORMS THAT MANDATE A NARROW EXPRESS WARRANTY WOULD PROPERLY INCENTIVIZE SOFTWARE MANUFACTURERS AND INCREASE NATIONAL AND ECONOMIC SECURITY

Part I of this Note introduced FISMA, the federal statutory scheme designed to increase federal information security and deter cyber attacks. Part I also described common criticisms of FISMA, including the charge that FISMA is fundamentally flawed because it treats information security as a technological problem and not an economic problem. Specifically, FISMA attempts to impose technological safeguards designed to mitigate weaknesses caused by software vulnerabilities, while ignoring the root cause of software vulnerabilities, which is inadequate software quality assurance on the part of software manufacturers. Part II analyzed proposed solutions designed to incentivize software manufacturers to ensure adequate software quality assurance. Part II evaluated proposals rooted in strict products liability, negligence liability, and contract remedies. Part III outlines a plan, premised on the framework provided by FISMA, and a mandatory express warranty, that incentivizes software manufacturers to ensure adequate software quality assurance. Finally, Part III highlights the advantages and disadvantages to such an incentive scheme.

A. Together With a Mandatory Express Warranty, FISMA Provides a Useful Framework Capable of Incentivizing Software Manufacturers

No statutory or legislative scheme designed to increase federal cybersecurity can succeed absent a liability rule that incentivizes software manufacturers to ensure adequate software quality assurance. Thus, FISMA and NIST should be used as a vehicle to incentivize software manufacturers. This could be accomplished by mandating that federal agencies only procure from the private sector software that contains a security certification that assures the product is free of all vulnerabilities identified on the SANS Institute Top Twenty list.[270] Such a certification would create an express warranty that FISMA would deny manufacturers from disclaiming or limiting in any way. A timetable would be created for federal agencies to fully implement the described procurement requirements, which would be designed to give software manufacturers an

269. *Id.*

270. *See Top 20 Internet Security Problems, Threats and Risks*, SANS INSTITUTE http://www.sans.org/top20 (last visited Sept. 23, 2010). In this scenario, the software manufacturers would be self-certifying their own software. Of course, the SANS Institute Top Twenty list (now referred to as the "SANS Top Cyber Security Risks") need not be the exact list used, but the list provides an unbiased assessment of the most frequently exploited software vulnerabilities from some of the most respected organizations in the industry, and the list is updated annually to maintain relevancy. *Id.* For an evaluation of software manufacturers' abilities to comply with this list, see Davis, *supra* note 204.

adequate amount of time to implement necessary changes to the design process.

FISMA could properly incentivize software manufacturers to ensure adequate software quality assurance if it were to require federal agencies to only procure software that was free of the top twenty Internet vulnerabilities, and mandate that such software be backed by a non-disclaimable express warranty. Such a requirement would allow federal agencies to seek consequential damages for damages caused by software vulnerabilities listed in the SANS Institute's Top Twenty list.[271] Should the software manufacturer fail to honor the warranty, as opposed to strict products liability[272] and negligence-based liability rules,[273] federal agencies would have the power to file a breach of express warranty claim, which circumvents the economic loss rule.[274] This would have the effect of reallocating the risk of defective software to the software manufacturer and providing monetary incentives to develop software free of the most dangerous Internet vulnerabilities. As a result, real cybersecurity within federal agencies would exponentially increase without most of the difficult implementation problems[275] or ineffective, burdensome reporting requirements FISMA currently imposes.[276]

Importantly, implementing the latter system through FISMA would have numerous ancillary benefits while overcoming or avoiding many of the disadvantages associated with strict products liability,[277] negligence-based liability rules,[278] and the mandatory warranty scheme articulated in Part II.C.[279] First, implementation through the FISMA framework affords a tremendous level of predictability for software manufacturers. This is because liability would be tied to a predictable standard of care that manufacturers could build into the software development process from the earliest stages of development. Every vulnerability on the SANS Institute Top Twenty list "is a result of poor coding, testing and sloppy software engineering"[280] where solutions exist but are simply not implemented.[281] Thus, software manufacturers are not being forced to develop costly new solutions to software vulnerabilities, but rather to implement procedural safeguards to prevent problems with known solutions.

Implementing a mandatory express warranty through FISMA would provide additional predictability to software manufacturers due to the limited scope of liability. FISMA regulates federal agencies. As opposed to any of the sweeping proposals described in Part II, software

271. *See supra* note 258 and accompanying text.
272. *See supra* notes 197–201 and accompanying text.
273. *See supra* note 226 and accompanying text.
274. *See supra* note 260 and accompanying text.
275. *See supra* Part I.B.1.
276. *See supra* Part I.B.2.
277. *See supra* notes 184–210 and accompanying text.
278. *See supra* notes 231–44 and accompanying text.
279. *See supra* notes 265–69 and accompanying text.
280. Davis, *supra* note 204.
281. *Id.*

manufacturers would only be liable for the most egregious breaches that occur within federal agencies, and because of the nature of the underlying information being protected, such liability is justified. This not only limits the breadth of potential liability and the number of claims a software manufacturer may face, but also is consistent with good public policy.[282] Additionally, the certainty afforded by limiting the breadth of potential liability to federal agencies and premising a standard of care on the SANS Institute Top Twenty list mitigates any concern over manufacturers becoming too risk-averse to continue developing innovative software.[283]

Federal agencies would be expected to maintain reasonable security so as not to void the express warranty. However, in contrast to the mandatory warranty analyzed in Part II.C, implementing a mandatory express warranty through FISMA would have the added advantage of a pre-existing standard by which to measure the "reasonableness" of a federal agency's security maintenance. The pre-existing standard would take the form of applicable NIST protocols, which federal agencies are mandated by FISMA to comply with.[284] Should a federal agency violate an applicable protocol, it would void the express warranty and relieve the software manufacturer of liability. This would incentivize federal agencies to comply with FISMA.

Finally, implementing a mandatory warranty through FISMA would potentially have a spillover effect into the private consumer market. Software products developed to meet FISMA requirements could be made available to the private consumer market. This would provide increased security to consumers at no extra cost. Software security across the private sector would increase and software manufacturers would avoid the unlimited liability they would face under a strict products liability rule.[285]

B. Potential Roadblocks to Success

Despite a host of advantages, there are at least two problems that could derail the effectiveness of the incentive system detailed in the previous section. A primary concern is the federal government's market power.[286] Transacting with the federal government and providing software to federal agencies is a voluntary activity. Should FISMA require software manufacturers to ensure heightened software quality assurance to conduct business with the federal government, it is entirely possible, and likely, that some manufacturers would simply stop transacting with the federal government. However, several considerations minimize the risk that a materially significant number of manufacturers would stop transacting with the federal government. First, all of the software vulnerabilities on the SANS Institute Top-Twenty list have known solutions that are all capable of being prevented through heightened software quality assurance.[287] Thus,

282. *See supra* notes 168–73 and accompanying text.
283. *See supra* notes 206–10 and accompanying text.
284. *See supra* note 85 and accompanying text.
285. *See supra* note 207 and accompanying text.
286. *See supra* note 112 and accompanying text.
287. *See supra* note 204 and accompanying text.

the risk of incurring actual liability is severely diminished, yet still real enough to warrant guaranteed compliance. Mature software manufacturers would have little difficulty complying with this standard. Second, if software manufacturers still felt the risk of incurring actual liability was too high, they would have the ability to purchase insurance to hedge their risk.[288] Finally, even assuming a sizeable number of software manufacturers ceased conducting business with the federal government for fear of liability, other willing software manufacturers, would fill the new demand created by manufacturers who left the supply market. Of course, whether these new manufacturers would provide the same level of software sophistication is questionable.

In addition to the federal government's questionable market power, as with the incentive solution outlined in Part II.C, quantifying damages could prove difficult.[289] Quantifying the monetary value of stolen electronic documents or databases, proprietary information, classified information, disabled networks, or critical infrastructure and the resulting collateral damage could potentially bankrupt even the most solvent software manufacturer. For this reason, damages could be capped at a pre-determined amount. This amount would be commensurate to the designated FISMA risk level determined by the relative worth of the information or interests being protected by the system utilizing the software containing the vulnerability.[290] This would further shield software manufacturers from excessive liability while still providing an incentive to ensure adequate software quality assurance. The increased predictability would also further deter software manufacturers from ceasing to conduct business with the federal government.

CONCLUSION

In its current form, FISMA has outlived its usefulness and is no longer efficiently enhancing federal cybersecurity. FISMA is marred with implementation difficulties.[291] Furthermore, FISMA reporting requirements do not accurately measure the strength of operational security, and provide little incentive to do so.[292] However, FISMA's greatest transgression is that it treats information security as a technological problem that demands technological solutions. In doing so, FISMA causes federal agencies to spend millions of dollars imposing technological safeguards designed to mitigate weaknesses caused by software vulnerabilities, while ignoring the root cause of software vulnerabilities,

288. *See* Kuwahara, *supra* note 177, at 1010–12 (explaining the rise of cyberinsurance); *see also* Dan Briody, *Full Coverage*, INC. (Apr. 1, 2007), http://www.inc.com/magazine/20070401/technology-insurance.html (providing a consumer-oriented explanation of cyberinsurance).

289. *See supra* note 267 and accompanying text.

290. *See supra* note 46 and accompanying text.

291. *See supra* Part I.B.1.

292. *See supra* Part I.B.2.

which is inadequate software quality assurance on behalf of software manufacturers. Thus, even if FISMA were perfectly implemented by federal agencies, actual cybersecurity would increase only minimally.

This is not to say that FISMA cannot be reformed. Requiring federal agencies to purchase software containing an express warranty, and not allowing software manufacturers to disclaim that warranty, could meaningfully increase federal cybersecurity. Such an incentive scheme would improve federal cybersecurity with minimal cost to the federal government, and without most of the difficult implementation problems or ineffective, burdensome reporting requirements FISMA currently imposes. Additionally, such an incentive system would more reasonably balance the concerns of software manufacturers with the need for a liability-based incentive system.[293]

The threat of national and economic catastrophe due to a cyberattack from a hostile state or individual actor is dramatically increasing. Cyberattacks can be used in place of nearly any traditional medium of attack or espionage.[294] Oftentimes, cyberattacks are preferable to a traditional attack because of the ease with which cyberattacks may be executed, and the intrinsic difficulties associated with identifying actors responsible for an attack.[295] Consequently, the threat of cyberattack poses the greatest threat to America's critical infrastructure, military capabilities, and national sovereignty since the advent of weapons of mass destruction. The time is now for reform. FISMA reforms that mandate a narrow, predictable express warranty would properly incentivize software manufacturers and meaningfully increase national and economic security.

293. *See supra* Part III.A.
294. *See supra* notes 13–16 and accompanying text.
295. *See supra* notes 13–16 and accompanying text.