American University Law Review

Volume 62 | Issue 5 Article 3

2013

Regulating Information Security in the Government Contracting Industry: Will the Rising Tide Lift All the Boats

Keir X. Bancroft

Regulating Information Security in the Government Contracting Industry: Will the Rising Tide Lift All the Boats

Keywords
America the Virtual: Security, Privacy, and Interoperability in an Interconnected World, United States. Paperwork Reduction Act of 1995, United States. Dept. of Defense, Government contractors -- Legal status, laws, etc., Data security failures, Computer security -- Law & legislation, Disclosure of information -- Law & legislation -- United States, Public contracts -- United States, Cyberspace -- Security measures -- Law & legislation

ARTICLES

REGULATING INFORMATION SECURITY IN THE GOVERNMENT CONTRACTING INDUSTRY: WILL THE RISING TIDE LIFT ALL THE BOATS?

KEIR X. BANCROFT*

The government is strengthening cyber and information security regulations to address increasing cybersecurity risks. These regulations will affect government contractors in many ways; for instance, contractors must apply new technologies to monitor cybersecurity threats and develop stronger information security protections. This "rising tide" of regulation should lift "all boats," namely members of the government contracts sector. Some small business contractors or larger contractors without experience working with the government, however, may not be equipped to fully comply with these strengthened regulations. The government may as a result lose a number of would-be competitors for contracts requiring cyber and information security protections. Alternatively, some contractors lacking resources and experience may compete for the contracts anyway, which could serve to weaken the security of government information and information systems. This Article gives an overview of existing and new regulatory requirements and analyzes

* Keir Bancroft practices law at Venable LLP in Washington, DC, where he regularly counsels clients in the government contracting industry on information security issues. Mr. Bancroft is the former Privacy Officer at the United States Department of the Treasury, Bureau of Engraving and Printing, where he advised the Bureau on matters pertaining to privacy and information security. The author would like to thank Peter Frechette, Andrew Hernacki, Estefania San Juan, and the members of the *American University Law Review* for inviting him to contribute this timely and important symposium, and their efforts in bringing this Article from concept to fruition.

the difficulties some contractors may have complying with them. This Article also suggests ways to ensure all contractors can effectively comply with the regulations. Federal agencies can develop incentives, protections, or training requirements for contractors. Agencies can also develop opportunities for information sharing, which would help smaller or larger, inexperienced contractors get involved in contracts requiring cyber and information security in a manner that better ensures compliance and mitigates security risk. The government may also want to develop an iterative process of regulation, which would help ensure all contractors can keep pace with the increases in cyber and information security regulation.

TABLE OF CONTENTS

INTRODUCTION

There is an oft-quoted aphorism that "a rising tide lifts all the boats."[1] It has often been used to support a variety of economic policies. President Kennedy used the analogy to support federal investment in a dam project in Arkansas. The rationale for the investment was that the benefit to a section of Arkansas would bear benefits to the states in general.[2] Thus, the resulting collective good—the "rising tide"—would benefit all individuals. In later years, President Reagan and other proponents of supply-side economics used the same phrase to support a philosophy that favorable economic conditions for business would spur economic growth, contribute to an overall stronger economy, and hence, benefit everyone.[3]

---

1. President John F. Kennedy, Remarks at the Dedication of Greers Ferry Dam, Heber Springs, Arkansas (Oct. 3, 1963), *available at* http://www.presidency.ucsb.edu/ws/index.php?pid=9455.

2. *Id.*

3. President Ronald Reagan, Address to the Nation on the Economy (Feb. 5, 1981), *available at* http://www.ronaldreaganmemorial.com/pdf/Address_Nation_the_Economy_020581.pdf.

In the context of cybersecurity regulation of the government contracting community, it appears the federal government is operating with the same philosophy. Steadily—though with varying degrees of speed—the federal government has raised standards for cyber and information security. Few would deny this is a positive trend.[4] The risk of harm arising from cybersecurity breaches and the exposure of sensitive information warrants increased vigilance and protection.[5] The means by which the federal government is mandating that protection, however, threatens to outpace the technology and resources available for subsets of the government contracting community, particularly small businesses. The regulations might also affect larger businesses just entering the government contracts industry or seeking work with new federal agencies; they may find that the cost of compliance outweighs the benefit of participating in the new market.[6] In that sense, the rising tide arguably lifts some "boats," but only those equipped with the technology and resources necessary to brave the waves of cyberthreats. It is difficult to see how some "boats" lacking the technology and experience to implement new protections can rise with the regulatory tide. They may not have the technology required to ensure the necessary cyber and information security protections required under new regulation.[7] Further, they may lack the experience necessary to ensure appropriate cyber and information security. In that respect, the rising tide does not promise to lift all

4. *See generally* Nat'l Sec. Counsel, *The Comprehensive National Cybersecurity Initiative*, WHITE HOUSE, http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative (last visited June 10, 2013) (noting that President Obama has indicated cybersecurity is one of the most important pressing challenges our nation faces).

5. *See, e.g.*, Adam Clark Estes, *Somebody, Probably Anonymous, Hacked the Fed During the Super Bowl*, ATL. WIRE (Feb. 5, 2013), http://www.theatlanticwire.com/technology/2013/02/somebody-probably-anonymous-hacked-fed-during-superbowl/61838 (discussing the recent breach of the Federal Reserve system).

6. For instance, the Federal Acquisition Regulation (FAR) states it is the policy of the federal government to "provide maximum practicable opportunities in its acquisitions" to all small business concerns, including the following: veteran-owned, small business; service-disabled, veteran-owned, small business; Historically Underutilized Business Zone ("HUBZone") small business; small disadvantaged business; and women-owned, small business concerns. FAR § 19.201(a) (2012). Further, these small business concerns "must also have the maximum practicable opportunity to participate as subcontractors in the contracts awarded by any executive agency, consistent with efficient contract performance." *Id.*

7. *See, e.g.*, Dietrich Knauth, *Obama's Cybersecurity Order Could Squeeze Contractors*, LAW 360 (Feb. 26, 2013), http://www.law360.com/articles/416900/obama-s-cybersecurity-order-could-squeeze-contractors (suggesting that President Obama's Executive Order asks too much of government contractors because of the fast pace at which hacker technology evolves).

boats. In fact, it appears some "boats" are at risk of foundering amidst waves that they are not equipped to navigate.

For example, information security protections previously reserved for classified information are now imposed on a much broader and amorphous species: controlled unclassified information (CUI). The problem is that the varying definitions of types of CUI make it difficult to ascertain what information must be protected as CUI. Further, the CUI paradigm imposes record handling and protection requirements on information to which a great many government contractors may have access. This increases the chance that government contractors previously unfamiliar with information security requirements will be thrust into a new regime requiring increased security and information security expertise.

In another example, Department of Defense (DoD) cyber and information security regulation has evolved over recent years, initially imposing broad information security protection requirements, and later scaling back those requirements to focus on the most basic information security protections. But in each instance, the DoD has made significant assumptions that the technology necessary to provide for such protections is readily available and (presumably) can be readily implemented by all government contractors, including small businesses. It is not clear that this is the case; consequently, small businesses which the federal government actively seeks to provide with contracting opportunities may be ill equipped to meet information security requirements. Other larger businesses that are new to the government contracting industry may determine that the costs of compliance are too prohibitive. This, in turn could reduce competition for government contracts. As competition helps to keep prices lower, the reduced competition for contracts could increase the costs of procurements.

Finally, the Federal Information Security Management Act of 2002[8] (FISMA), which was passed to regulate protection of government information, is being implemented and amended in such a way as to require investment in technologies that allow for constant monitoring for breaches.[9] This arguably represents a shift from the original, risk-based model that FISMA established. Until recently, FISMA dictated the degree of information security necessary for implementation based on the risk of an unauthorized release of

8. 44 U.S.C. §§ 3541–3549 (2006).
9. *Id.*

government information.[10] More recently, the Special Publications and upcoming FISMA amendments are dictating a more prescriptive approach, mandating technology such as continuous monitoring to ensure information security is maintained.[11] Again, the results of these new requirements could serve to inhibit small businesses from participation in certain opportunities with the government. Indeed, the requirements could also affect the ability of larger, more experienced contractors to comply. Larger businesses, be they established government contractors or business concerns with well-established commercial contracting practices seeking opportunities to contract with the federal government, may already have established information security practices. To the extent these larger contractors need to alter their information security infrastructure and practices to satisfy new regulatory requirements, the results may prove to be as prohibitive as they are for small businesses.

As the federal government mandates increased information security requirements, a dividing line may appear between those contractors with the size, experience, or resources[12] necessary to comply with those requirements, and those lacking those characteristics. On its face, the result could operate to restrict contracting opportunities to contractors who are already better equipped to address information security requirements and the changes thereto. More disconcerting, however, is the potential that certain business concerns, seeking to establish a foothold in the government market or seeking to work with a new agency,[13] may undertake information security responsibilities that they are not equipped to handle. The results could be disastrous. If a business undertakes too much security responsibility and then experiences a breach, it would implicate the privacy, safety, and security interests of the business itself, the federal customer, and potentially a variety of other individuals. In a case like this, the few boats that cannot rise with the tide may bring down the additional boats as well.

---

10. *See infra* Part I.F (demonstrating how previous acts based the degree of required security on the corresponding levels of risk).

11. *See infra* Parts II.B, III (examining present and proposed amendments mandating a more comprehensive approach to the security requirements).

12. In some cases, new market entrants or established business concerns seeking to work with the federal government or with new federal agencies may determine that the cost of altering their established information security infrastructure and policies to satisfy new regulation may prove prohibitive.

13. *See generally* Julia L. Rogers, *Winning Government Contracts: Five Things You Need to Know*, ENTREPRENEUR (Dec. 24, 2011), http://www.entrepreneur.com/article/217779 (explaining why the government contract market is lucrative for businesses and how businesses can enter the market).

This Article analyzes how small businesses and other inexperienced government contractors may be unable to effectively comply with increasing information security requirements. This Article also explores some possible solutions that could ameliorate the effects of the rising tide and ensure that small businesses and inexperienced government contractors continue to have a role in those projects calling for increased information security requirements.

The federal government can leverage tools already in place to help ensure that all government contractors are well equipped to safeguard information. One example is the mentor-protégé programs established at the Small Business Administration (SBA) and a number of other federal agencies.[14] Similarly, the "fifty percent rule," which mandates that small business prime contractors perform an established percentage of contracts, might be augmented to create carve-outs for large-business technology and information security specialists to contribute to the operations of small businesses.[15] Another solution may be an information security training requirement, similar to the privacy training mandated in October 2011,[16] which would help ensure all small businesses are keeping pace with changes in information security requirements.[17]

Further, agencies would do well to communicate and collaborate on matters pertaining to information security.[18] To the extent information security requirements are consistent across the DoD, DHS, and other civilian agencies, the chances for confusion are reduced. If contractors are complying with similar regulatory regimes, there is less chance that contractors who may not have experience working with a specific department or agency will miss particular requirements.

Finally, the federal government may seek to continue what it has already started with regulatory requirements—taking a smaller-scale, iterative approach to information security.[19] As can be seen from DoD regulation of information security and subsequent efforts to

---

14. *See infra* Part IV.A (describing and proposing amendments to the SBA's mentor-protégé programs). The federal government already incentivizes small businesses to enter into mentor-protégé arrangements with large businesses.

15. *See infra* Part IV.B (outlining a potential amendment to the fifty percent rule to increase collaboration between large and small business).

16. Privacy Training, 76 Fed. Reg. 63,896 (proposed Oct. 14, 2011) (to be codified at FAR pts. 24, 52).

17. *See infra* Part IV.C (discussing the privacy training mandate as a model that sets minimum standards but also provides contractors with an option to design their own programs).

18. *See infra* Part IV.D (identifying information sharing as one a successful initiative and encourage expanding the use of information sharing).

19. *See infra* Part IV.E (proposing an iterative approach to security requirements).

require more basic information security requirements, the move from a wider to a smaller-scale approach to regulation could make for a more viable set of requirements and make it relatively easier for government contractors to comply. The tide, in effect, would still be rising, but at a slower rate. This could help the "boats" rise along with it.

I. BACKGROUND ON INFORMATION SECURITY LAWS AND REGULATIONS

Though the broad concept of cybersecurity has brought the issue to the fore, information security legislation and regulation has been promulgated in a number of different laws throughout the past thirty years.[20] A brief overview of these laws demonstrates how information security requirements have evolved with technology and provides useful context for understanding the new cybersecurity regulations.

A. The Paperwork Reduction Act

In 1980, Congress passed the Paperwork Reduction Act,[21] recognizing agencies engaged in "collections of information" from the public, and authorizing the Office of Management and Budget (OMB) to regulate those activities.[22] The Paperwork Reduction Act recognized a systematic process by which federal agencies would collect information from persons and other nongovernmental organizations.[23] For example, the term "collection of information" calls for obtaining, soliciting, or requiring "the disclosure to third parties or the public, of facts or opinions by or for an agency, requiring either (1) answers to identical questions or identical reporting requirements imposed on ten or more persons or (2) answers to questions posed to "agencies, instrumentalities, or employees of the United States which are to be used for general statistical purposes."[24] The Act also established the Office of

20. *See, e.g.*, Computer Security Act of 1987, Pub. L. No. 100-235, 101 Stat. 1724 (codified as amended at 15 U.S.C. §§ 278g-3, 278g-4 (2006)); Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2006); Government Information Security Reform Act, 40 U.S.C. § 11103(a); Paperwork Reduction Act, 44 U.S.C. §§ 3501–3520 (2006 & Supp. IV 2010); Federal Information Security Management Act of 2002, 44 U.S.C. §§ 3541–3549 (2006); Clinger-Cohen Act of 1996, Pub. L. No. 104-106, 110 Stat. 679. *See generally* Daniel M. White, Note, *Federal Information Security Management Act of 2002: A Potemkin Village*, 79 FORDHAM L. REV. 369 (2010) (tracing the history of information security legislation).

21. Pub. L. No. 96-511, 94 Stat. 2812 (codified as amended at 44 U.S.C. §§ 3501–3521 (2006)).

22. 44 U.S.C. § 3506 (2006).

23. *Id.* § 3507.

24. *Id.* § 3502(3)(A).

Information and Regulatory Affairs (OIRA) to supervise the use of information resources.[25] The Act charged the OIRA Director with providing direction and overseeing the agency management of information and records in order to protect the privacy of these materials and promote the proper use of information technologies.[26]

The Paperwork Reduction Act demonstrates the federal government's understanding that it often collects sensitive information requiring protection of the "privacy, confidentiality, security, disclosure, and sharing of information."[27] Further, the federal government recognized that the "acquisition and use of information technology" would be a key factor in the gathering and maintenance of information from the public.[28]

B. The Computer Fraud and Abuse Act

In 1984, Congress passed the first iteration of the Computer Fraud and Abuse Act,[29] criminalizing improper access to information on government computers. The Act criminalized the knowing or intentional, unauthorized access to certain computers for a number of reasons, including the following: gathering information related to national defense, foreign relations, or nuclear energy;[30] obtaining financial records, or otherwise accessing protected computers[31] within federal agencies;[32] accessing federal agencies' nonpublic computers without authorization;[33] accessing information maintained on federal agency nonpublic computers;[34] transmitting computer viruses for purposes of causing damage to the computer;[35] trafficking in computer access information, including passwords;[36] and extorting persons via threat to impair the confidentiality of information, or

25. *Id.* § 3504(a)(1).
26. *Id.* § 3504(a)(1)(B) (giving the director the power to control "agency dissemination of and public access to information," "records management activities," "privacy, confidentiality, security, disclosure, and sharing of information," and "the acquisition and use of information technology, including alternative information technologies that provide for electronic submission, maintenance, or disclosure of information as a substitute for paper and for the use and acceptance of electronic signatures").
27. *Id.* § 3504(a)(1)(B)(v).
28. *Id.* § 3504(a)(1)(B)(vi).
29. 18 U.S.C. § 1030.
30. *Id.* § 1030(a)(1).
31. "Protected computers" under the Act are defined as those exclusively for use of a financial institution or the United States government, or used in or affecting interstate or foreign commerce or communication. *Id.* § 1030(e)(2).
32. *Id.* § 1030(a)(2)(B).
33. *Id.* § 1030(a)(3).
34. *Id.*
35. *Id.* § 1030(a)(5)(A).
36. *Id.* § 1030(a)(6).

otherwise damaging a protected computer.[37] Furthermore, the Act provided federal grounds for prosecuting computer crimes, including the unauthorized access or use of nonpublic or confidential information.[38]

C. The Computer Security Act of 1987

In what could be described as a precursor to more recent risk-based information security legislation, the Computer Security Act of 1987[39] established minimum security practices to protect security and privacy of sensitive information on federal computer systems. Specifically, it directed the National Bureau of Standards to develop standards and guidelines to maintain and promote the security and privacy of sensitive information in federal computer systems.[40] Further, it required "establishment of security plans by all operators of Federal computer systems that contain sensitive information"[41] and required "mandatory periodic training for all persons involved in management, use, or operation of Federal computer systems that contain sensitive information."[42] Specifically, the Computer Security Act required the National Bureau of Standards to develop explicit technical, management, physical, and administrative standards and guidelines to protect sensitive information.[43] These standards and guidelines were to be submitted to the Secretary of Commerce along with recommendations as to the extent that they should be made compulsory and binding.[44] The Secretary, in turn, was authorized to issue standards, making them compulsory and binding to the extent necessary.[45] The Act also mandated that every federal agency, within one year of the Act's enactment, identify all computer systems under its supervision and create a plan for the security and privacy of each system identified.[46] The agency's plan was to be commensurate with the risk and magnitude of the consequences that would result from the loss, misuse, unauthorized access to, or modification of the

37. *Id.* § 1030(a)(7).
38. For a discussion of the Computer Fraud and Abuse Act, see generally Andrew T. Hernacki, Comment, *A Vague Law in a Smartphone World: Limiting the Scope of Unauthorized Access Under the Computer Fraud and Abuse Act*, 61 AM. U. L. REV. 1543, 1544 (2012), arguing for a narrow interpretation of unauthorized access.
39. Pub. L. No. 100-235, 101 Stat. 1724 (codified as amended at 15 U.S.C. §§ 278g-3, 278g-4 (2006)).
40. *Id.* § 2(b)(1).
41. *Id.* § 2(b)(3).
42. *Id.* § 2(b)(4).
43. *Id.* § 3.
44. *Id.*
45. *Id.* § 4.
46. *Id.* § 6.

information contained in its system.[47] A summary of the security plan was required to be included in each agency's five-year plan, and it was subject to the approval of the Director of OMB. Further, the plan was required to be revised annually.[48] Thus, the Act once again demonstrated the federal government's recognition of a need to protect sensitive information on its computers.

D. The Clinger-Cohen Act

Beginning in the mid-1990s, the Clinger-Cohen Act of 1996 invested the OMB Director with federal information technology responsibilities.[49] Those responsibilities required coordination with the Department of Commerce for development of "standards and guidelines pertaining to Federal computer systems . . . through the National Institute of Standards and Technology."[50] The OMB Director was also required to direct heads of federal agencies to establish capital planning processes for selecting, managing, and evaluating the results of all major investments in information systems.[51] The process involves a determination of whether the function to be supported by the system should be performed by the private sector, an executive agency, or some combination.[52] Even with the assignment of responsibilities to the OMB Director for implementation of federal information technology acquisition policy, the government has expressly considered the involvement of contractors in the development and implementation of information systems. Of course, agency heads are also required to "ensure that the information security policies, procedures, and practices are adequate."[53] Further, the OMB Director is required under Clinger-Cohen to "implement through the budget process periodic reviews of

47. *Id.*
48. *Id.*
49. Pub. L. No. 104-106, 110 Stat. 186 (1996). The Federal Acquisition Streamlining Act of 1994, Pub. L. No. 103-355, 108 Stat. 3243 (codified as amended in scattered sections of 26 U.S.C.), the Federal Acquisition Reform Act of 1996, Pub. L. No. 104-106, div. D, §§ 4001–4402, 110 Stat. 642, and the Information Technology Management Reform Act of 1996, Pub. L. No. 104-106, div. E, §§ 5001–5703, 110 Stat. 679 (1996), are now collectively known as the Clinger-Cohen Act. The Clinger-Cohen Act also repealed the central authority of the GSA Administrator for acquisitions of information technology, which had previously been authorized under Federal Property and Administrative Services Act. Clinger-Cohen Act § 5101.
50. Clinger-Cohen Act § 5112(d). The National Bureau of Standards was renamed the National Institute of Standards and Technology in 1988. 15 U.S.C. § 271(b)(1) (2006).
51. Clinger-Cohen Act § 5113(b)(2)(A).
52. *Id.* § 5113(b)(2)(B).
53. *Id.* § 5123.

selected information resources management activities of the executive agencies."[54]

Echoing the requirements of the Computer Security Act, the Clinger-Cohen Act authorizes the Secretary of Commerce "on the basis of standards and guidelines developed by the National Institute of Standards and Technology . . . [to] promulgate standards and guidelines pertaining to Federal computer systems."[55] It alsogives the Secretary discretion to make such standards mandatory when necessary to make the operations, security, or privacy of federal computer systems more efficient.[56] Essentially, the Act sought to standardize the federal government's information technology management policies while ensuring the maintenance of an adequate level of security and privacy.

E. OMB Circular A-130

To implement the requirements under these and related laws and manage federal information resources, the OMB promulgated Circular No. A-130.[57] More specifically, OMB under Circular A-130 establishes minimum controls for inclusion in federal automated information security programs; assigns federal agencies responsibilities for securing automated information; and links automated information security programs and management control systems within federal agencies.[58]

F. The Government Information Security Reform Act

Later, in 2000, Congress passed the Government Information Security Reform Act (GISRA).[59] GISRA established information security management program requirements for agencies controlling both unclassified and national security programs.[60] GISRA implemented risk-based policies, designed to both identify risks and

54. *Id.* § 5113(b)(4).
55. *Id.* § 5131(a)(1).
56. *Id.* § 5131(a)(2).
57. *See* OFFICE OF MGMT. & BUDGET, EXEC. OFFICE OF THE PRESIDENT, OMB CIRCULAR NO. A-130 (Revised) (2000) [hereinafter REVISED OMB CIRCULAR A-130], *available at* http://www.whitehouse.gov/sites/default/files/omb/assets/omb/circulars/a130/a130trans4.pdf (listing its authority for creating a policy for the management of federal information resources).
58. *Id.* app. III.
59. Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001, Pub. L. No. 106-398, tit. X, subtit. G, 114 Stat. 1654A-266 (2000).
60. *Id.* § 1061.

determine security needs commensurate with the level of risk.[61] GISRA was, however, time-limited by a two-year sunset provision.[62]

Two years later, FISMA made permanent many of the risk-based information security requirements established by GISRA. Given the federal government's history of legislation aimed at ensuring the security of its information, its most recent attempt at bolstering this security serves as the latest in a long line of legislation passed in recognition of the rising tide and the growing need to raise all of the boats.

II. THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT

The Federal Information Security Management Act (FISMA) passed in 2002.[63] FISMA had six stated purposes: (1) to provide a framework for ensuring the effectiveness of security controls; (2) to provide a comprehensive "governmentwide" security management system; (3) to develop minimum controls to protect federal information; (4) to improve oversight of information security programs; (5) to maintain a commercial focus and recognize the efficacy of information security measures developed in the private sector; and (6) to recognize agency discretion in selecting security solutions.[64]

Though FISMA is broad in scope,[65] it also applies a risk-based approach to information security and calls for agencies to provide security protections for information, which are to be commensurate with the potential risk of harm resulting from unauthorized access and other disturbances of information systems.[66]

As OMB underscored in its 2011 guidance to federal agencies, FISMA's broad reach applies to contractors as well as federal agencies.[67] In fact, FISMA applies to all organizations that possess federal information or have access to federal systems including

---

61. *Id.* ("Policies under this subsection shall . . . be founded on a continuing risk management cycle that recognizes the need to (i) identify, assess, and understand risk; and, (ii) determine security needs commensurate with the level of risk.").

62. *Id.* (amending 44 U.S.C. § 3536 to read, "[t]his subchapter shall not be in effect after the date that is two years after the date on which this subchapter takes effect").

63. 44 U.S.C. §§ 3541–3549 (2006).

64. *Id.* § 3541 (discussing, in detail, the purpose of FISMA).

65. *Id.* (stating that it is intended to provide "governmentwide" management, oversight, and coordination "throughout the civilian, national security, and law enforcement communities").

66. *Id.* § 3544(a).

67. *See* Memorandum from Jacob J. Lew, Office of Mgmt. & Budget, for Heads of Exec. Dep'ts & Agencies (Sept. 14, 2011), *available at* http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-33.pdf (explaining that FISMA applies to services that are partially or entirely provided by contractors).

contractors, local governments, and even software subscription services.[68]

A. Applying the Federal Information Processing Standard

The extent and effect of obligations on contractors derives from the Federal Information Processing Standard (FIPS) and the National Institute of Standards and Technology (NIST) Special Publications (SP) issued by NIST.[69] FIPS, subject to approval by the Secretary of Commerce, imposes mandatory standards on federal agencies and contractors (or any "other organizations") that possess federal information or operate federal information systems.[70] The basic FIPS-mandated standards and requirements include FIPS Publication 199: *Standards for Security Categorization of Federal Information and Information Systems*,[71] and FIPS Publication 200: *Minimum Security Requirements for Federal Information and Information Systems*.[72]

---

68. Memorandum from Roberta Stempfley, Acting Assistant Sec'y, Office of Cybersecurity & Commc'ns, for the Heads of Exec. Dep'ts & Agencies (Aug. 24, 2011), *available at* http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-33.pdf ("Because FISMA applies to both information and information systems used by the agency, contractors, and other organizations and sources, it has somewhat broader applicability than prior security law. That is, agency information security programs apply to all organizations (sources) which possess or use Federal information—or which operate, use, or have access to Federal information systems (whether automated or manual)—on behalf of a Federal agency. Other organizations may include contractors, grantees, State and Local Governments, industry partners, providers of software subscription services, etc. FISMA, therefore, underscores longstanding OMB policy concerning sharing Government information and interconnecting systems.").

69. *See Development Schedule for FISMA Implementation Project Publications*, NAT'L INST. OF STANDARDS & TECH. (Jan. 17, 2013), http://csrc.nist.gov/groups/SMA/fisma/documents/milestone-schedule-v55.pdf (setting forth the timeline for FISMA implementation).

70. 15 U.S.C. § 278g-3(a) (2006)(authorizing NIST to "develop standards and guidelines, including minimum requirements, for information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency, other than national security systems"); 40 U.S.C. § 11331 (establishing authority of the Secretary of Commerce to promulgate standards and guidelines pertaining to Federal computer systems); 44 U.S.C. § 3543 (directing the OMB Director to oversee agency information security policies and practices).

71. NAT'L INST. OF STANDARDS & TECH., DEP'T OF COMMERCE, FIPS PUB. NO. 199, STANDARDS FOR SECURITY CATEGORIZATION OF FEDERAL INFORMATION AND INFORMATION SYSTEMS 1 (2004) [hereinafter FIPS 199], *available at* http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf.

72. NAT'L INST. OF STANDARDS & TECH., DEP'T OF COMMERCE, FIPS PUB. NO. 200, MINIMUM SECURITY REQUIREMENTS FOR FEDERAL INFORMATION AND INFORMATION SYSTEMS, at iv (2006) [hereinafter FIPS 200], *available at* http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf.

1. FIPS publication 199: Standards for security categorization of federal information and information systems

FIPS 199 applies to information and information systems other than national security systems.[73] Information under FIPS 199 is categorized according to its information type.[74] An information type spans a range of categories; including privacy, medical, proprietary, financial, investigative, contractor-sensitive, and security management.[75] These types are generally defined by an organization; or by laws, directives, policies, regulations, or Executive Orders.[76] In accordance with FISMA, FIPS 199 defines three "security objectives" according to the ability of an information processor to ensure "confidentiality," "integrity," and "availability" of information.[77]

Explicitly defined under FIPS 199, a loss of confidentiality is the "unauthorized disclosure of information"; a loss of integrity is the "unauthorized modification or destruction of information"; and the loss of availability is the "disruption of access or use of information or an information system." The loss of any of these objectives as they pertain to information or an information system amounts to a security breach under FIPS 199. The effect of a security breach is determined on three levels of potential impacts on organizations or individuals falling under FISMA, and is determined in the context of the organization and the overall national interest. The impacts include the following:

> Low Impact (or Minor Harm): A low impact breach poses a "limited adverse effect on organizational operations, organizational assets, or individuals."[78] Low impact equates to "minor harm," a limited adverse effect—meaning that the loss of confidentiality integrity, or availability might result in the following: (i) a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) minor damage to organizational assets; (iii) minor financial loss; or (iv) minor harm to individuals.[79]
>
> Moderate Impact (or Significant Harm): A moderate impact breach poses a "serious adverse effect on organizational operations,

73. FIPS 199, *supra* note 71, at 1.
74. *Id.* at 1 n.1 ("Information is categorized according to its *information type*. An information type is a specific category of information . . . defined by an organization or, in some instances, by a specific law . . . .").
75. *Id.*
76. *Id.*
77. *Id.* at 2.
78. *Id.*
79. *Id.*

> organizational assets, or individuals."[80] This equates to "significant harm," meaning that the loss of confidentiality, integrity, or availability might result in the following: (i) a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) significant damage to organizational assets; (iii) significant financial loss; or (iv) significant harm to individuals that does not involve loss of life or serious life threatening injuries.[81]
>
> High Impact (or Severe Harm): A high impact breach poses a "severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals."[82] This equates to "severe harm," meaning that the loss of confidentiality, integrity, or availability might result in the following: (i) a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) major damage to organizational assets; (iii) major financial loss; or (iv) severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

Based on the security objectives of confidentiality, integrity, and availability, and the definition of potential impacts as either low, moderate, or high, NIST prescribes a method for developing security categorizations (SC) among information types (again, generally defined by organizations, laws, policy, regulations, guidelines, or Executive Orders) by employing a generalized format, which considers both the security objective and the level of impact.[83] For example, FIPS 199 maps out the risk related to a particular information type according to the magnitude of impact to each of its security objectives.[84] First, the potential security category information types are set forth, placing a separate security objective with its concomitant impact: "SC information type = {(confidentiality, *impact*), (integrity, *impact*), (availability, *impact*)}."[85] Next, the values, low, moderate, high, or not applicable (N/A) are applied.[86] FIPS 199 illustrates this system with examples.[87] For instance, an organization managing public information on a web server may determine that there is no potential impact from loss of confidentiality (i.e.,

80. *Id.*
81. *Id.*
82. *Id.* at 3.
83. *Id.*
84. *Id.*
85. *Id.*
86. *Id.*
87. *Id.*

confidentiality requirements are not applicable), moderate potential impact from a loss of integrity, and moderate potential impact from a loss of availability.[88]

FIPS 199 is a logical analysis because public information is, by definition, not confidential. Thus, even if that information were to be disclosed without authorization, it would not be confidential, and there would be no potential impact. In contrast, with information integrity, there is the possibility of significant harm. Even if the information in question is not confidential, there is a vested interest in its integrity, i.e., its veracity and authenticity. If there is a security breach affecting the integrity of the information, there could be significant questions about an organization's ability to secure the information, or simply questions about the organization itself. It also makes sense that a breach affecting the availability of the public information would have a moderate impact. If the public loses access to the organization's information, and there are doubts about its availability, there again can be questions about the organization's ability to secure the information. Further, the public may no longer look to obtain information from that organization.[89]

FIPS 199 maintains fidelity to FISMA's risk-based approach to information security by matching the security objectives with potential impacts. It provides a range of potential security categorizations, all of which involve matching security objectives with the potential impact a security breach would have on each of those objectives. The extent of the impact, if any, will be driven by the type of information and information system in question. Thus, FIPS 199 is consistent with FISMA because the information or the system itself, and the organization's evaluation of that information, is the driver of security categorizations under FISMA.

2. FIPS 200: Minimum security requirements for federal information and information systems

Another key information security standard is FIPS 200.[90] FIPS 200, which is applicable to all unclassified information within the federal government, complements the FIPS 199 standards for security categorization.[91] Taken another way, FIPS 199 supplies the *what*, by

88. As a result of that analysis, the security categorization of the organization's public information is set forth as follows under FIPS 199: "SC public information = {(confidentiality, NA), (integrity, MODERATE), (availability, MODERATE)}." *Id.*

89. *Id.*

90. FIPS 200, *supra* note 72.

91. *Id.* at iv.

determining *what* level of security categorization applies to information types and information systems;[92] FIPS 200 supplies the *how*, by specifying the minimum level of security requirements that must be applied to meet the security categorizations established under FIPS 199 standards.[93] Under FIPS 200, NIST prescribes seventeen security-related areas that need to be addressed to confront "management, operational, and technical aspects of protecting federal information and information systems."[94] These broad prescriptions include several aspects of information management including controlling accessibility of information; ensuring that managers have a solid understanding of security risks; establishing contingency plans; and assessing potential risk. While FIPS 199 and 200 together identify information systems that require protection and specific security goals, the 800 Series of NIST Special Publications provides organizations with specific guidance on how to reach these goals.[95]

B. Following the 800 Series of NIST Special Publications

To satisfy FIPS 200 security specifications, federal agencies are required to follow the guidance under Special Publication (SP) 800-53: *Security and Privacy Controls for Federal Information Systems and Organizations*.[96] Using SP 800-53, organizations must take the security categorizations established pursuant to FIPS 199 and apply baseline

---

92. *Compare id.* at 1 (explaining that FIPS 200 is intended to specify minimum security measures), *with* FIPS 199, *supra* note 71, at 1 (explaining that FIPS 199 is intended to categorize information and information systems).

93. FIPS 200, *supra* note 72, at 1.

94. *Id.* at 2–4 (identifying the following categories: Access Control; Awareness and Training; Audit and Accountability; Certification, Accreditation and Security Assessments; Configuration Management; Contingency Planning; Identification and Authentication; Incident Response; Maintenance; Media Protection; Physical and Environmental Protection; Planning; Planning; Personnel Security; Risk Assessment; System and Services Acquisition; System and Communications Protection; and System and Information Integrity).

95. *Id.*

96. *See* NAT'L INST. OF STANDARDS & TECH., DEP'T OF COMMERCE, SPEC. PUB. NO. 800-53, REV. 4, SECURITY AND PRIVACY CONTROLS FOR FEDERAL INFORMATION SYSTEMS AND ORGANIZATIONS, at iv (2013) [hereinafter SP 800-53], *available at* http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf. It should be noted that the latest version of SP 800-53 is Revision 4, released in April 2013. Unless otherwise noted, all references to SP 800-53 are to Revision 4. *Id.* Special publications have been promulgated by NIST to complement and in this case, implement FIPS requirements. The special publications reflect outreach efforts on matters pertaining to computer security, and are reflective of NIST's collaborative activities with industry, government, and academic organizations. Pursuant to FIPS 200, "[f]ederal agencies must meet the minimum security requirements as defined herein through the use of the security controls in accordance with NIST Special Publication 800-53." FIPS 200, *supra* note 72, at v.

security controls, tailored to meet the specific organizational and security controls necessary to assure adequate security.[97] OMB defines adequate security as security "commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information."[98] Again, the focus of information security under FISMA is a risk-based regime, which provides a degree of flexibility and discretion to those charged with securing information and systems.[99]

Reflecting the security categorizations under FIPS 199, FIPS 200 requires organizations to establish baseline security controls under SP 800-53 to ensure adequate security appropriate to the level of risk. The baseline security controls are defined according to their level of impact.[100] Therefore, for low-impact information systems, an organization must "employ appropriately tailored security controls from the low baseline of security controls defined in [SP 800-53]" and "ensure that the minimum assurance requirements associated with the low baseline are satisfied."[101] Similarly, for moderate-impact information systems, the "moderate baseline" of security controls must be used for tailoring.[102] For high-impact information systems, a "high baseline" of security controls must be used for tailoring.[103] These controls are applied on a tiered approach, whereby risk is evaluated at different organizational levels.[104]

SP 800-53's flexibility permits organizations to customize their security control baselines to align with the goals of the particular entity.[105] These controls are designed to protect information from continuous and varied threats and "to demonstrate compliance with a variety of governmental, organizational, or institutional security requirements."[106]

---

97. FIPS 200, *supra* note 72, at iv–v.
98. REVISED OMB CIRCULAR A-130, *supra* note 57, app. III.
99. *See supra* note 68 (providing background on FISMA).
100. FIPS 200, *supra* note 72, at 1.
101. *Id.* at 4.
102. *Id.*
103. *Id.*
104. Those tiers include Tier 1: the Organization Level; Tier 2: the Mission/Business Process Level; and Tier 3: the Information System Level. From Tiers 1 to 3, the risks involved move from strategic in nature to tactical. SP 800-53, *supra* note 96, at 7 (explaining, in detail, the organization and structure of security controls).
105. *Id.* at vi (allowing "organizations to tailor the relevant security control baseline so that it more closely aligns with their mission and business requirements and environments of operations").
106. *Id.* at 4 (stating that the controls are also established to "protect information and information systems from traditional and advanced persistent threats in varied operational, environmental, and technical scenarios").

SP 800-53 establishes eighteen baseline security control families, with most families reflecting the FIPS 200 specifications for minimum security requirements.[107] Distinct from the security specifications under FIPS 200 is the Program Management security control family under SP 800-53. The Program Management family differs in its application, as it is applied on an organization-wide basis and not at a particular tier or in accordance with a particular level of risk.[108] Within each security control family are a range of baseline security controls which are prescribed to assure adequate security. For instance, under the Access Control family, there are up to twenty-two possible security control baselines to be utilized.[109]

Each security control is described in detail under SP 800-53, Appendix F,[110] including supplemental guidance for organizations to consider when developing and implementing such controls.[111] The security controls also include enhancements, which describe ways in which the organization can increase the functionality, specificity, and strength of a control.[112] The enhancements are layered on top of baseline security controls as necessary to add functionality or specificity to a control and increase the strength of a control in order to meet increasing levels of risk.[113] Thus, where a baseline security control may address a low level of risk, an enhancement may be necessary to address a moderate level of risk, and additional enhancements may be necessary to address a high level of risk.

---

107. *Id.* app. D tbl.D-2. The baseline security control families are "Access Control," "Awareness and Training," "Audit and Accountability," "Security Assessment and Authorization," "Configuration Management," "Contingency Planning," "Identification and Authentication," "Incident Response," "Maintenance," "Media Protection," "Physical and Environmental Protection," "Planning," "Personnel Security," "Risk Assessment," "System and Services Acquisition," "System and Communications Protection," "System and Information Integrity," and "Program Management." *Id.*

108. *Id.* apps. D tbl.D-2, G.

109. For example, the "Access Control" family contains the following security control baselines: "Access Control Policy and Procedures," "Account Management," "Access Enforcement," "Information Flow Enforcement," "Separation of Duties," "Least Privilege," "Unsuccessful Logon Attempts," "System Use Notification," "Previous Logon (Access) Notification," "Concurrent Session Control," "Session Lock," "Session Termination," "Permitted Actions without Identification or Authentication," "Security Attributes," "Remote Access," "Wireless Access," "Access Control for Mobile Devices," "Use of External Information Systems," "Information Sharing," "Publicly Accessible Content," "Data Mining Protection," "Access Control Decisions," and "Reference Monitor." *Id.* app. D tbl.D-2.

110. *See, e.g.*, *id.* app. F (describing the "Account Management" baseline under the "Access Control" family and detailing the minimum enhancements required for each of the three risk-tiers).

111. *Id.*

112. *Id.* at 12.

113. *Id.*

The most recent revision to SP 800-53 was released in April 2013 and aimed to tackle "the expanding threat space," featuring "the increasing sophistication of cyberattacks and the operations tempo of adversaries."[114] In response to the expanding threat space, NIST in this most recent revision incorporated new security controls and enhancements addressing a range of areas including "mobile and cloud computing; . . . trustworthiness, assurance, and resiliency of information systems; insider threat; [and] advanced persistent threat [APT]."[115] NIST also added new families of privacy controls "based on the internationally accepted Fair Information Practice Principles."[116] To provide organizations a means of implementing these new and expanded families of controls, NIST in the revised SP 800-53 introduced "overlays," which can be used, essentially, to fine-tune specialized security plans applicable to "specific missions/business functions, environments of operation, and/or technologies."[117] Using an overlay of these various security and privacy controls, NIST sought in its revision "to give organizations near real-time information that is essential for senior leaders making ongoing *risk-based* decisions affecting their critical missions and business functions."[118]

Though it is reasonable for NIST to update its information security and privacy controls, the move to implement a system of controls "to give organizations near real-time information that is essential for senior leaders making ongoing risk-based decisions affecting their critical missions and business functions"[119] poses a threat to government contractors that might not be in a position to implement such a robust system of controls, either from lack of resources, experience, or for which establishing these components could prove a greater cost than warranted by the benefit of doing business with the Government. These types of requirements, though not unfounded, represent a rising tide in information security regulation. Though it may help to ensure greater information security across information and systems subject to FISMA compliance, these requirements may increase the cost of compliance, in terms of components and experience in deploying those components, to a

114. *Id.* at xv.
115. *Id.*
116. *Id.*
117. *Id.*
118. *Id.*
119. *Id.*

degree that could force some contractors to avoid projects that call for FISMA compliance.[120]

NIST acknowledges that the security control baselines "address the security needs of a broad and diverse set of constituencies (including individual users and organizations)."[121] The baselines reflect some underlying assumptions regarding the functions served by and the threats posed to such information systems.[122] NIST also includes among the assumptions underlying the baselines within SP 800-53 that "[o]rganizations have the necessary structure, resources, and infrastructure to implement the controls."[123] As analyzed in this Article, that assumption is not always true, particularly for small business contractors, or larger businesses that have not had to implement information security protection as part of their prior work with the federal government or particular federal agencies. NIST concedes that although federal departments and agencies will easily satisfy this assumption, it is more problematic for local governments and small businesses.[124] The size of those entities and availability of resources may inhibit their ability to meet the minimum baseline requirements.[125] Presumably, if a small business contractor or another similarly situated organization lacks the resources necessary to provide the required range of security capabilities, it will ultimately have to avoid any work that calls for the application of security controls that are beyond its capacity or experience.

Among the new security controls are a series of controls prescribed under the program management family, including an insider threat program, an information security workforce, and testing, training, and monitoring security control.[126] In addition, new security controls are also included in other families such as the system and communications protection family and incident response family.

---

120. *But see* Andrew George Sakallaris, *Questioning the Sacred Cow: Reexamining the Justifications for Small Business Set Asides*, 36 PUB. CONT. L.J. 685, 696 (2007) (arguing that small businesses possess advantages over large firms that allow them to better comply with government requirements).

121. SP 800-53, *supra* note 96, at 29.

122. *Id.* ("Some *assumptions* that generally underlie the baselines . . . include, for example: (i) the environments in which organizational information systems operate; (ii) the nature of operations conducted by organizations; (iii) the functionality employed within information systems; (iv) the types of threats facing organizations, missions/business processes, and information systems; and (v) the type of information processed, stored, or transmitted by information systems.").

123. *Id.* at 30.

124. *Id.* at 30 n.64.

125. *Id.* ("Such entities may not be large enough or sufficiently resourced to have elements dedicated to providing the range of security capabilities that are assumed by the baselines. Organizations consider such factors in their risk-based decisions.").

126. *Id.* app. D.

1. Insider threat program

The Insider Threat Program requires a specific team that handles insider threats across multiple departments.[127] Its supplemental guidance states that "[i]nsider threat programs can leverage the existence of incident handling teams organizations may already have in place, such as computer security incident response teams."[128] Thus a contractor lacking an experienced computer security incident response team will lack one of the basic building blocks of an insider threat program. Further, NIST highlights the importance of human resource records in detecting malicious insider activity. Human resources records are especially important in this effort, as compelling evidence shows that insider crimes are sometimes "preceded by non-technical behaviors in the workplace (e.g., ongoing patterns of disgruntled behavior and conflicts with coworkers and other colleagues)."[129] These precursors can better inform and guide organizational officials in more focused and targeted monitoring efforts.[130]

Implementation of an Insider Threat Program poses a risk to organizations lacking experience in addressing issues such as disgruntled employee behavior and employee workplace disputes. Efforts to implement this security control could expose market participants to potential employee grievances and lawsuits based on civil liberty violations.[131] NIST appears to recognize this risk recommending that "[t]he participation of a legal team is important to ensure that all monitoring activities are performed in accordance with appropriate legislation, directives, regulations, policies, standards, and guidelines."[132] With that said, however, it is difficult to know whether existing legislation, regulations, or policies even address the types of employee behaviors that might signal an insider threat. Thus, implementing the Insider Threat Program security control, while addressing some risks, actually creates new ones specific to certain types of organizations.

---

127. *Id.* app. G.
128. *Id.*
129. *Id.*
130. *Id.*
131. *See, e.g.*, Raquel Aldana-Pindell, *The 9/11 "National Security" Cases: Three Principles Guiding Judges' Decision-Making*, 81 OR. L. REV. 985, 990 n.22 (2002) (noting that the Inspector General has the authority to review alleged civil liberties violations of federal employees).
132. SP 800-53, *supra* note 96, app. G.

2. Information security workforce

Another new security control in the Program Management family is the Information Security Workforce under which an organization must establish an "information security workforce development and improvement program."[133] Such programs must specify the requisite knowledge and experience and the standards for further developing skills necessary for performing certain security functions.[134] This is a security control reasonably related to assuring adequate information security. Again, however, organizations entering the market, or without an employee base possessing the knowledge and skills necessary to satisfy information security requirements, run the risk of falling behind established competitors that are better equipped to satisfy the necessary knowledge and skills.

3. Testing, training, and monitoring

NIST also prescribes the Testing, Training, and Monitoring security control. Under this control, an organization must develop, maintain, and execute a process to test, train, and monitor its information systems.[135] As the significance of constant monitoring continues to increase, so does the need to coordinate and consolidate organization-wide testing and monitoring of security controls.[136]

4. Security controls in other families

a. System and communications protection family

New security controls were established in other families as well. For example, NIST recommended the Operations Security (OPSEC) baseline security control under the System and Communications Protection family. This control calls for development of an OPSEC program, which would be created to "den[y] adversaries access to

133. *Id.*

134. *Id.* (noting that the "programs include, for example, (i) defining the knowledge and skill levels needed to perform information security duties and tasks; (ii) developing role-based training programs for individuals assigned information security roles and responsibilities; and (iii) providing standards for measuring and building individual qualifications for incumbents and applicants for information security-related positions").

135. *Id.*

136. *Id.* (clarifying that "[w]ith the increasing importance of continuous monitoring programs, the selection and implementation of security across the three tiers of the risk management hierarchy, and the widespread use of common controls, organizations need to coordinate and consolidate the host of testing and monitoring that are routinely conducted as part of ongoing organizational assessments supporting a variety of security controls").

information about capabilities and intentions."[137] To accomplish this, organizations would identify, control, and protect unclassified information related to planning and sensitive activities.[138] Developing an OPSEC program requires distinguishing critical information, analyzing threats and vulnerabilities, assessing risks, and taking proper countermeasures.[139] Again, the extent to which certain newer or small business government contractors get involved in managing federal information or information systems, it is not clear whether they would have the expertise to develop a compliant OPSEC Program.[140]

Another new set of security controls that falls under the System and Communications Protection family includes Concealment and Misdirection, Honeyclients, Distributed Processing and Storage, Out-of-Band Channels, Operations Security, Process Isolation, and Wireless Link Protection.[141] Implementation of these controls arguably requires a degree of sophistication and investment in infrastructure that could threaten to keep small businesses or newer market entrants from complying with these requirements.

For instance, Concealment and Misdirection calls for entities to use techniques to reduce the targeting capabilities of potential adversaries by purposely confusing and misleading them.[142] An example provided by NIST is the use of "virtualization techniques [to] provide organizations with the ability to disguise information systems, potentially reducing the likelihood of successful attacks without the cost of having multiple platforms."[143] Although this is presented as a cost-effective risk mitigation measure, organizations that lack the sophistication to employ virtualization techniques may indeed have to rely upon, and incur the additional costs of, multiple platforms.[144] Other techniques NIST suggests include employing

137. *Id.* app. F.
138. *See id.*
139. *Id.*
140. *But see* Sakallaris, *supra* note 120, at 689 (arguing that designing contract procurement requirements to specifically benefit small businesses goes against the most basic principles of government contracting).
141. SP 800-53, *supra* note 96, app. D.
142. *Id.* app. F.
143. *Id.*
144. *Explanation of Virtualization to a Non-Techie Person*, I-EVOLVE TECH. SERVICES (Nov. 10, 2009), http://blog.i-evolve.com/explaination-of-virtualization ("Virtualization is the creation of a virtual (rather than actual) version of something, such as an operating system, a server, a storage device or network resources . . . . Network virtualization is a method of combining the available resources in a network by splitting up the available bandwidth into channels, each of which is independent from the others, and each of which can be assigned (or reassigned) to a particular server or device in real time. The idea is that virtualization disguises the true complexity of the network by separating it

randomness, uncertainty, and virtualization to confuse and mislead adversaries.[145] Though these sound like viable means of mitigating adversaries' advances, the techniques need to be employed by experienced personnel.[146] An organization without access to these personnel would likely be rendered less competitive for its inability to employ concealment and misdirection programs.

Finally, the Distributed Processing and Storage baseline calls for spreading processing and storage resources across multiple physical locations.[147] This creates redundancy for organizations, which in turn increases the work required for adversaries to succeed in interfering with the organization's information systems.[148] The requirement to establish multiple physical locations would affect small businesses and, possibly, new market entrants lacking the infrastructure necessary to distribute processing and storage. Again, all of these requirements exemplify how certain cybersecurity regulations would burden small businesses and strain their resources. The regulations may also pose either a prohibitive costs or risk to larger, more established businesses that are just starting to work with the federal government or a new agency.

b. Incident response family

Further, the Information Spillage Response control was established under another family, the incident response family.[149] Properly responding to an information spill does not at first glance appear to require extensive additional skills.[150] The types of information spills contemplated under Information Spillage Response, however, could make instituting this security control difficult.[151] The issue with this type of information spillage is that information is being categorized differently now than it was just a few years ago. For example,

---

into manageable parts, much like [a] partitioned hard drive makes it easier to manage [] files."); *see also* Amy Newman, *Virtualization Technologies Lure Governments*, SERVERWATCH (July 28, 2010), http://www.serverwatch.com/virtualization/article.php/3895516/Virtualization-Technologies-Lure-Governments.htm (explaining that the high costs of implementing virtualization technologies is a common deterrent).

145. SP 800-53, *supra* note 96, app. F.

146. *See* Newman, *supra* note 144 (noting that half of those surveyed believed their IT staff were not experienced enough to manage other virtualization techniques).

147. SP 800-53, *supra* note 96, app. F.

148. *Id.*

149. *Id.* app. D.

150. *Id.* app. F (listing the reporting and reparation steps that must be taken when information has already been leaked).

151. *Id.* (mentioning situations in which the sensitivity of information either increases over time or is underestimated when initially introduced to a specific information system).

initiatives such as the movement to CUI[152] from former categories such as "For Official Use Only" or "Sensitive But Unclassified" present the risk that information that once may have been considered not to be sensitive has moved to a category of higher sensitivity.[153] According to the supplemental guidance under Information Spillage Response, such official and unofficial re-categorizations constitute information spillages requiring corrective action.[154] In an age in which information categorization is in flux, this new security control presents the potential for frequent information spillage. The Information Spillage Response control may need to be monitored to ensure it is not becoming a burdensome requirement that serves to capture only the most recent changes in information categories. Only then will such a security control work as an effective tool for information security.

III. PROPOSED UPDATES TO FISMA

A. The Federal Information Security Amendments Acts of 2012 and 2013

In April 2012, the House of Representatives passed a bill to update FISMA, titled the "Federal Information Security Amendments Act of 2012" (2012 Amendments).[155] The bill did not pass in the Senate,[156] but it provides insight into congressional intent to update FISMA requirements. The legislation was re-introduced in 2013 as the "Federal Information Security Amendments Act of 2013" and once again passed the House of Representatives (2013 Amendments).[157] Key among the proposed updates was the Amendments'[158] emphasis on continuous monitoring. One of the stated purposes of the Amendments was to "provide a mechanism for improved oversight of Federal agency information security programs and systems through a focus on automated and continuous monitoring of agency

152. See, for example, DFARS Case 2011-D039, stating that the Department of Defense Federal Acquisition Supplement (DFARS) does not presently address the safeguarding of unclassified information, and "addresses the safeguarding requirements specified in Executive Order 13556, Controlled Unclassified Information." Defense Federal Acquisition Regulation Supplement: Safeguarding Unclassified DoD Information (DFARS Case 2011-D039), 76 Fed. Reg. 38,089, 38,089–90 (proposed June 29, 2011) (to be codified at FAR pts. 204, 252).

153. Exec. Order No. 13,556, 3 C.F.R. 267 (2011) (consolidating certain unclassified designations into one category called "Controlled Unclassified Information").

154. SP 800-53, *supra* note 96, app. F.

155. Federal Information Security Amendments Act of 2012, H.R. 4257, 112th Cong..

156. Cybersecurity and Internet Freedom Act of 2011, S. 413, 112th Cong..

157. Federal Information Security Amendments Act of 2013, H.R. 1163, 113th Cong..

158. Unless otherwise specified, reference to "Amendments" means both the 2012 and 2013 Amendments.

information systems and regular threat assessments."[159] The Amendments define "automated and continuous monitoring" as "monitoring, with minimal human involvement, through an uninterrupted, ongoing real time or near real-time process used to determine if the complete set of planned, required, and deployed security controls within an information system continue to be effective over time with rapidly changing information technology and threat development."[160]

The Amendments call for deploying automated and continuous monitoring as part of minimum agency security operations requirements, and propose to task the Chief Information Officer (CIO) or Chief Information Security Officer (CISO) with overseeing and maintaining those automated monitoring systems.[161]

Further, the Amendments call for requiringagencies to develop information security programs and procedures for operations and assets supporting the agency, including those provided by contractors similar to those required for the agencies themselves.[162] The information and security programs and procedures will, if passed, require contractors and others to ensure oversight and training of their information security professionals with a very demanding level of frequency.[163]

The requirements of the proposed Amendments appear consistent in their application of automated and continuous monitoring requirements. They call for procedures, training, and programs that all address these new requirements. Further, they reasonably call for each agency's CIO to coordinate with outside security centers when handling information incidents that are beyond the agency's control.[164] It is sensible that Congress seeks collaboration between

159. H.R. 1163 § 2 (amending 44 U.S.C. § 3551(a)); H.R. 4257 § 2 (same).

160. H.R. 1163 § 2 (amending 44 U.S.C. § 3552(b)(2)); H.R. 4257 § 2 (same).

161. H.R. 1163 § 2 (amending 44 U.S.C. § 355a(a)(3) and specifying that the CIO or CISO would be responsible for managing system intrusions and vulnerabilities and for holding officials responsible for keeping information secure); H.R. 4257 § 2 (same).

162. H.R. 1163 § 2 (amending 44 U.S.C. § 3554(b)(1) and noting that such systems would be required to include "automated and continuous monitoring, when possible, of the risk and magnitude of the harm that could result from the disruption or unauthorized access, use, disclosure, modification, or destruction of information and information systems that support the operations and assets of the agency"); H.R. 4257 § 2 (same).

163. H.R. 1163 § 2 (amending 44 U.S.C. § 3554(b)(4) and requiring oversight and training "with a frequency sufficient to support risk-based security decisions, automated and continuous monitoring, when possible, for testing and evaluation of the effectiveness and compliance of information security policies, procedures, and practices"); H.R. 4257 § 2 (same).

164. H.R. 1163 § 2 (amending 44 U.S.C. § 3554(a)(3)(A)(iv)); H.R. 4257 § 2 (same).

agencies and their contractors to ensure that automated and continuous monitoring requirements are deployed appropriately so that proper levels of information security protection are maintained.

Again, however, it is not clear how the implementation of automated and continuous monitoring requirements may affect prospective small business contractors or those new to FISMA compliance requirements. It may be that organizations do not have the necessary resources and experience to deploy and consistently administer the requisite technology called for in ensuring automated and continuous monitoring. Further, the requirement to report security incidents to the Inspector General (IG) within twenty-four to forty-eight hours of discovery could have a chilling effect on these contractors,[165] because reporting could open them up to liability. Though reporting to an IG is no doubt a necessity to ensure information security is handled appropriately, it may be enough to prevent certain contractors, particularly those concerned about potential criminal liability arising from a security breach, from engaging in contracts that require information security.

B. Executive Order on Cybersecurity Protections of Critical Infrastructure

The 2012 Amendments, like most other significant cybersecurity-related[166] legislation, failed to pass in the 112th Congress. Following Congress's failure to pass cybersecurity legislation, President Obama issued an Executive Order ("the Order"), Improving Critical

165. 44 U.S.C. 3554(a)(3)(A)(v) (2006).

166. Among the higher-profile bills failing passage was the Cybersecurity Act of 2012, S. 2105, 112th Cong.. The bill, with backing in the Senate and the White House, provided for increased government oversight of private networks in the nation's critical infrastructure. Under the Act, the Department of Homeland Security (DHS) would determine which businesses would fall under critical infrastructure, but it would generally include sectors such as electric grids, water systems, and transportation. The Cybersecurity Act would have required the federal government to develop a comprehensive acquisition risk management strategy. The focus, like the FISMA Amendments Act, would call for automated and continuous monitoring of agency information systems and regular threat assessments, and DHS would have authority to streamline agency reporting requirements. Another proposed bill was the SECURE IT Act (short for Strengthening and Enhancing Cybersecurity Using Research, Education, Information and Technology Act). S. 3342, 112th Cong. (2012). Under SECURE IT, businesses would have been allowed to voluntarily share cyberthreat information. SECURE IT included provisions that limited liability for companies taking steps to protect their networks and restrictions on the types of information to be shared so as to protect personal privacy. Further, SECURE IT would have reformed federal cybersecurity standards, directing the Secretary of Commerce to issue policies and guidance governing agency cybersecurity. DHS would have been tasked with conducting ongoing security analyses and developing a timeline for establishing continuous monitoring of federal networks.

Infrastructure Cybersecurity, which was intended to address cybersecurity threats to the nation's critical infrastructure.[167]

Broadly defining the term "critical infrastructure,"[168] the Order places an emphasis on cybersecurity information sharing, calling for processes and systems to be developed that make it possible for the private sector and government agencies to share information about cyberthreats and to ensure that organizations that are under threat of a cyberattack are informed of such a threat.[169] The Order also directs the development of a cybersecurity framework, which will "include a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks."[170] This framework, which will be developed by NIST under the direction of the Secretary of Commerce,[171] will be similar to the development of FISMA implementation standards in that it will be risk-based in nature and "technology neutral" in order to enable technical innovation and account for organizational differences. As with other sections of the Order, private sector companies and organizations are expected to be involved in development of the framework by participating in a public notice and comment process.[172] From this standpoint, it appears that NIST will consider the needs of small businesses and larger new market entrants before finalizing the Cybersecurity Framework.

Another provision of the Order, however, could operate to bar small businesses and new government contractors from commenting on issues pertaining to cybersecurity. Under the provision, the Secretary of Defense and the Administrator of General Services must recommend the "feasibility, security benefits, and relative merits of incorporating security standards into acquisition planning and contract administration."[173]

---

167. Exec. Order No. 13,636, 78 Fed. Reg. 11,737 (Feb. 19, 2013).

168. *Id.* at 11,739. Critical infrastructure is defined as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." 42 U.S.C. § 5195c(e) (Supp. IV 2011).

169. Exec. Order No. 13,636, 78 Fed. Reg. at 11,739, 11,742.

170. *Id.* at 11,740–41.

171. *Id.* (noting that the Framework is to be "consistent with voluntary international standards when such international standards will advance the objectives of this order, and shall meet the requirements of the National Institute of Standards and Technology Act, as amended, the National Technology Transfer and Advancement Act of 1995, and OMB Circular A-119, as revised" (citations omitted)).

172. *Id.* at 11,741.

173. *Id.*

This effort could compound the relative inexperience or lack of resources of small businesses or even larger businesses seeking to do business with the federal government. These entities may already be at a competitive disadvantage through their inability to comply with evolving cybersecurity standards.[174] If a new set of security standards are incorporated into acquisition planning and contract administration, small businesses, or new market entrants may be further disadvantaged if they cannot satisfy these recommended standards. It is possible that the effects of the new standards may not be so severe, as the Report must "address what steps can be taken to harmonize and make consistent existing procurement requirements related to cybersecurity."[175] But, if the DoD and GSA determine that security standards must be significantly overhauled in acquisition planning and contract administration, no amount of harmonization will help small businesses or new market entrants.

Section 6 of the Order, which requires the Secretary of Homeland Security to establish a "consultative process," could possibly exacerbate the problem.[176] Section 6 directs the Secretary to use the Critical Infrastructure Partnership Advisory Council (CIPAC) to facilitate information from Sector Coordinating Councils (SCC) and critical infrastructure owners and operators, as well as other government agencies.[177] Therefore, existing private sector organizations that are already part of CIPAC,[178] and those already

174. *See supra* Part II.B (discussing the updated security controls under SP 800-53 issued by NIST).

175. *See supra* Part II.B.

176. Exec. Order No. 13,636, 78 Fed. Reg. at 11,740.

177. *Id.*

178. CIPAC is a partnership between the government and critical infrastructure/key resources (CI/KR) owners created by DHS to "facilitate an effective defense of our Nation's critical infrastructure" through collaboration of all key stakeholders. Critical Infrastructure Partnership Advisory Council, 71 Fed. Reg. 14,930, 14,930, 14,932 (Mar. 24, 2006) (notice). CIPAC membership is structured around "critical infrastructure sectors" initially designated by Homeland Security Presidential Directive 7 (HSPD-7) and expanded upon by DHS. *See id.* at 14,932–33 (noting fifteen sectors outlined in HSPD-7 and DHS' authority to form new sectors); *Council Members, Critical Infrastructure Partnership Advisory Council*, DEP'T OF HOMELAND SEC., http://www.dhs.gov/council-members-critical-infrastructure-partnership-advisory-council (last visited June 10, 2013) [hereinafter *Council Members*] (listing the twenty current sectors). Each critical infrastructure sector is composed of (1) a government coordinating council (GCC) consisting of a lead Federal agency and "all relevant Federal, state, local, tribal, and/or territorial government agencies;" and (2) a sector coordinating council (SCC)—independent and self-governed bodies comprised of private sector players or their representatives. The Critical Infrastructure Partnership Advisory Council, 77 Fed. Reg. 64,818, 64,819 (Oct. 23, 2012) (membership update). The roster of CIPAC membership is published on the CIPAC website. *Council Members, supra.* HSPD-7 was revoked by a presidential policy directive issued the same day as the Order. Directive on Critical Infrastructure Security and Resilience, Presidential Policy Directive/PPD-21, 2013 DAILY COMP.

participating in SCCs likely have a seat at the table in discussing the relative merits of incorporating security standards into acquisition planning and contract administration. This arrangement could threaten to deprive small businesses and new market entrants of the opportunity to share concerns about a potential competitive imbalance that the incorporation of the security standards might bring.

Another related requirement that might also affect small businesses and new market entrants is Presidential Policy Directive (PPD-21), Critical Infrastructure Security and Resilience.[179] PPD-21 was issued the same day as the Executive Order and serves as a companion of sorts, clarifying the "policy of the United States to strengthen the security and resilience of its critical infrastructure against both physical and cyber threats."[180] Paragraph 6 of PPD-21 requires the General Services Administration to coordinate with other agencies, including the DoD and DHS to "provide or support government-wide contracts for critical infrastructure systems and ensure that such contracts *include audit rights for the security and resilience of critical infrastructure*."[181] It is not yet known what audit rights GSA and other agencies might seek to include in critical infrastructure systems contracts. The possibility that certain contracts will expressly include audit rights may chill small businesses or other inexperienced contractors from competing for critical infrastructure systems contracts. A compliance requirement may prove daunting enough to some contractors, but the express right of the government to audit compliance undoubtedly compounds a contractor's compliance risk. Though the audit rights established under PPD-21 will help foster security of critical infrastructure, they could prove to thin the market of businesses that might otherwise compete for critical infrastructure systems contracts.

The provisions of the Order, like those of the failed cybersecurity legislation preceding it, are helpful because they provide insight into the thoughts of policy makers who are in the process of enacting official policy requirements and standards. The effects and consequences of these policies and standards will be felt by the government contracting sector, especially those members of the sector that are small or inexperienced and lack the resources to

---

PRES. DOC. 1 (Feb. 12, 2013) [hereinafter PPD-21]. As stated in the directive, however, "[p]lans developed pursuant to HSPD-7 shall remain in effect until specifically revoked or superseded." *Id.* at 10.

179. PPD-21, *supra* note 178.

180. *Id.* at 1.

181. *Id.* at 5 (emphasis added).

establish and maintain robust cybersecurity and information security protections. These changes may also affect larger businesses that possess more resources, but may view the new standards as too much of a compliance risk to justify the effort to do business with the federal government or a new federal agency.

C. Development of CUI Requirements

The development of information security requirements has evolved with technology. As the capability to access, handle, store, process, and utilize information has increased in the federal government, more comprehensive security measures have been developed to guard against unauthorized access, use, and distribution of information.

The scope of what information needs protection has evolved as well. In recent years, efforts to better define, utilize, and ensure the protection of CUI in the federal government have taken large strides. A key moment in the development of CUI was President Obama's issuance of Executive Order 13,556.[182] The Executive Order created an "open and uniform program" for managing CUI—information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies.[183] The Executive Order addressed a system characterized by "executive departments and [agencies] employ[ing] ad hoc, agency-specific policies, procedures, and markings to safeguard and control [CUI]."[184] Much of the unclassified information safeguarded under the existing system, characterized in the Order as a "confusing patchwork [that] has resulted in inconsistent marking and safeguarding of documents," was known as Sensitive But Unclassified (SBU).[185] One particular concern noted in the Order was that agency-specific policies for information safeguarding were "often hidden from public view."[186] This only aggravated the inconsistent marking and safeguarding practices, called for "unnecessarily restrictive dissemination policies, and created impediments to authorized information sharing."[187]

---

182. Exec. Order No. 13,556, 3 C.F.R. 267 (2011)..
183. *Id.* The definition of CUI excludes information that is classified under Executive Order 13,526 or the Atomic Energy Act. *Id.*
184. *Id.* Executive Order 13,556 provided the following examples of CUI: "information that involves privacy, security, proprietary business interests, and law enforcement investigations." *Id.*
185. *Id.*
186. *Id.*
187. *Id.*

To address these issues, the Order established a program for managing all unclassified information in the Executive Branch that required safeguarding or dissemination controls.[188] President Obama designated the National Archives and Records Administration (NARA) as the executive agent (EA) for developing, implementing, and managing the CUI Program.[189] Guidance issued by NARA ("CUI Office Notice"), under its authority pursuant to the Order, requires the designation of CUI information to fall under agency-developed categories and subcategories.[190] The CUI Office Notice also requires "safeguarding measures and controls to protect CUI from unauthorized access, and to manage the risks associated with the processing," handling, and storage.[191]

These designations were developed into an initial public registry of fifteen CUI categories and eighty-eight subcategories in November 2011.[192] A year later, the CUI Registry expanded to twenty-two categories[193] and one-hundred-and-one subcategories, illustrating the broad scope of areas containing unclassified information in need of safeguarding and control.[194]

Streamlining the manner in which CUI is safeguarded and disseminated by creating a uniform categorization system will impact the way in which information is shared between federal agencies and contractors. Such a system will undoubtedly create more clarity about what information may be disseminated. Clarity, in turn, makes it likely that individuals with access to information will not

188. *Id.*
189. *Id.*
190. CONTROLLED UNCLASSIFIED INFO. OFFICE, NAT'L ARCHIVES, CONTROLLED UNCLASSIFIED INFORMATION (CUI) NOTICE 2011-01: INITIAL IMPLEMENTATION GUIDANCE FOR EXECUTIVE ORDER 13556, at 1–2, 7 (2011), *available at* http://www.archives.gov/cui/documents/2011-cuio-notice-2011-01-initial-guidance.pdf.
191. *Id.* at 4.
192. CONTROLLED UNCLASSIFIED INFO. OFFICE, NAT'L ARCHIVES, 2011 REPORT TO THE PRESIDENT (2011); *Controlled Unclassified Information (CUI): The CUI Registry Is Out!*, DATA CLASSIFICATION (Nov. 14, 2011), http://www.dataclassification.com/en/component/k2/item/191-controlled-unclassified-informationcui-the-cui-registry-is-out; *CUI Registry*, NAT'L ARCHIVES, http://www.archives.gov/cui/registry/category-list.html#categories (last visited June 11, 2013).
193. The current CUI registry categories consist of the following: (1) Agriculture; (2) Copyright; (3) Critical Infrastructure; (4) Emergency Management; (5) Export Control; (6) Financial; (7) Foreign Government Information; (8) Geodetic Product Information; (9) Immigration; (10) Information Systems Vulnerability Information; (11) Intelligence; (12) Law Enforcement; (13) Legal; (14) North Atlantic Treaty Organization; (15) Nuclear; (16) Patent; (17) Privacy; (18) Proprietary; (19) SAFETY Act Information; (20) Statistical; (21) Tax; and (22) Transportation. *CUI Registry*, *supra* note 192.
194. *See id.* (listing the 101 broad subcategories).

unreasonably withhold information because the propriety of sharing the information will be easily ascertained.

As already seen after one year, however, the number of categories and subcategories is prone to proliferation.[195] This may call into question the accuracy of information categorized under a particular category or subcategory. Suppose a new category or subcategory is established that creates a better home for previously designated information. Whether the government is required to re-categorize the already designated information is unclear. Moreover, if information designated under a particular category or subcategory more appropriately falls under a new category or subcategory established subsequently, how is it to be treated? Will it have to be re-categorized? If not, how are two sets of information to be treated if they are similar but categorized differently simply by virtue of the passage of time?

Further, the question of how contractors will be able to comply with these requirements remains. Will a contractor ever have to designate certain information under a particular category or subcategory, or protect and disseminate information in accordance with those particular categories? If so, how will the contractor make that determination? Further, what if the contractor involved is a small business or a new contractor inexperienced with the types of information in question? Will there be consequences or penalties if the contractor fails to manage the information in accordance with the government's directive? Some of those questions have been addressed under subsequent efforts by the DoD to regulate the handling and protection of CUI, and the Federal Acquisition Regulatory (FAR) Council to address contractor management and protection of information systems.

D. DoD Efforts To Regulate Controlled Unclassified Information, and Information Security in General

In addition to FISMA requirements and the federal government's efforts to categorize and coordinate treatment of CUI, the DoD has taken steps to regulate contractor handling and protection of unclassified information. For instance, as part of its Safeguarding Unclassified DoD Information rule (DFARS Case 2011-D039), the DoD proposed new rules under the Defense Federal Acquisition Regulation Supplement (DFARS) that would govern contractor

195. *See supra* notes 192–94 and accompanying text.

safeguarding of unclassified DoD information.[196] The DoD issued the proposed rule to "implement adequate security measures to safeguard unclassified DoD information within contractor information systems from unauthorized access and disclosure, and to prescribe reporting to the DoD with regard to certain cyber intrusion events that affect DoD information resident on or transiting through contractor unclassified information systems."[197] Further, the DoD explained that its proposed rule "addresse[d] the safeguarding requirements specified in Executive Order 13556, Controlled Unclassified Information[,]" but allowed that changes implemented by NARA regarding CUI "may also require future DFARS revisions in this area."[198]

1. An analysis of the proposed requirements related to controlled unclassified information in the DoD

The DFARS Case 2011-D039 proposed rule sought to create a two-tiered approach through the use of basic and enhanced safeguarding measures in order to (1) avoid disclosure of DoD information resident on or transiting through unclassified computer networks, (2) prevent the exfiltration of DoD information on such systems, and (3) prescribe reporting of certain cyberintrusion events to the DoD.[199] Aside from the obvious benefit of safeguarding information, the DoD stated an additional objective of the reporting requirements would be to help the DoD "[a]ssess the impact of loss; [b]etter understand methods of loss; [f]acilitate information sharing and collaboration; and [s]tandardize procedures for tracking and reporting intrusions."[200]

The DoD sought to apply its rule on a broad scope, covering any information already classified or defined under existing directives and regulations, including (1) "critical program information"

196. Defense Federal Acquisition Regulation Supplement: Safeguarding Unclassified DoD Information, 76 Fed. Reg. 38,089, 38,089, 38,091 (proposed June 29, 2011) (to be codified at FAR pts. 204, 252).

197. *Id.* at 38,090.

198. *Id.* In fact, the DoD's efforts to address safeguarding of unclassified information pre-date Executive Order 13556. An advance notice of proposed rulemaking was published in the federal register in March 2010. *See* Defense Federal Acquisition Regulation Supplement: Safeguarding Unclassified Information, 75 Fed. Reg. 9563, 9563 (proposed Mar. 3, 2010) (to be codified at FAR pts. 204, 252). The Executive Order was published later, in November 2010. That fact notwithstanding, the DoD clarified in its proposed rule that it was promulgated to address the requirements of the Executive Order.

199. Defense Federal Acquisition Regulation Supplement: Safeguarding Unclassified DoD Information, 76 Fed. Reg. at 38,090.

200. *Id.*

pursuant to DoD Instruction 5200.39;[201] (2) "critical information" under DoD Directive 5205.02;[202] (3) information restricted under International Traffic in Arms Regulations[203] (ITAR) and Export Administration Regulations[204] (EAR); (4) information exempt pursuant to DoD regulations regarding the Freedom of Information Act (FOIA);[205] (5) information already labeled in a way indicating "controlled access and dissemination";[206] (6) Information considered "technical data [or] computer software" and any technical information identified pursuant to DoD Directives 5230.24[207] and 5230.25;[208] and (7) "personally identifiable information" such as

201. DEP'T OF DEF., INSTRUCTION NO. 5200.39, CRITICAL PROGRAM INFORMATION (CPI) PROTECTION WITHIN THE DEPARTMENT OF DEFENSE, at 1 (2010), *available at* http://www.dtic.mil/whs/directives/corres/pdf/520039p.pdf.

202. DoD Directive 5205.02 created the Operations Security (OPSEC) program. DEP'T OF DEF., DIRECTIVE NO. 5205.02E, DOD OPERATIONS SECURITY (OPSEC) PROGRAM 1 (2012), *available at* http://www.dtic.mil/whs/directives/corres/pdf/520502e.pdf. The OPSEC program involves "identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities." DEP'T OF DEF., JOINT PUB. NO. 1-02, DEPARTMENT OF DEFENSE DICTIONARY OF MILITARY AND ASSOCIATED TERMS 209 (2013), *available at* http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.

203. The ITAR regulate exports of items and services that are specifically designed for military applications, such as tanks, fighter aircraft, nerve agents, and defensive equipment. 22 C.F.R. §§ 120–130 (2012).

204. The EAR regulate exports of commercial items that may have a potential impact on military applications including electronics, computers, and lasers and sensors. 15 C.F.R. §§ 730–774.

205. *See* DoD Freedom of Information Act (FOIA) Program, 32 C.F.R. § 285 (establishing the general FOIA policy for the DoD and dictating roles and responsibilities of the DoD components); DoD Freedom of Information Act Program Regulation, *id.* § 286 (providing guidance on processing FOIA requests).

206. Some examples of such labels include "for official use only," "sensitive but unclassified," "limited distribution," "proprietary," "originator controlled," and "law enforcement sensitive." Defense Federal Acquisition Regulation Supplement: Safeguarding Unclassified DoD Information, 76 Fed. Reg. 38,089, 38,090 (proposed June 29, 2011) (to be codified at FAR pts. 204, 252).

207. DoD Directive 5230.24 creates a framework for marking and managing technical documents generated or managed by defense-funded research, development, test and evaluation programs. The scope of documents affected by the Directive range from technical manuals and computer software to "any . . . technical information that can be used or be adapted for use to design, engineer, produce, manufacture, operate, repair, overhaul, or reproduce any military or space equipment or technology concerning such equipment." DEP'T OF DEF., INSTRUCTION NO. 5230.24, DISTRIBUTION STATEMENTS ON TECHNICAL DOCUMENTS, 1–2 (2012), *available at* http://www.dtic.mil/dtic/pdf/submit/523024p.pdf.

208. DoD Directive 5230.25 provides the policies, procedures, and responsibilities with regard to withholding data marked under DoD Directive 5230.24 limited to "technical data that disclose critical technology with military or space application." DEP'T OF DEF., DIRECTIVE NO. 5230.25, WITHHOLDING OF UNCLASSIFIED TECHNICAL DATA FROM PUBLIC DISCLOSURE 1 (1995), *available at* http://www.dtic.mil/whs/directives/corres/pdf/523025p.pdf.

information covered in the Privacy Act[209] and the Health Insurance Portability and Accountability Act[210] (HIPAA).

The proposed rule would have added a definition of "DoD information" and "nonpublic information."[211] DoD information was defined by the proposed rule as "any nonpublic information that (1) [h]as not been cleared for public release [under the applicable] DoD directive . . . and (2) is [either] (i) [p]rovided by or on behalf of the [DoD] to the Contractor or its subcontractor(s); or (ii) [c]ollected, developed, received, transmitted, used, or stored by the Contractor or its subcontractor(s) in support of an official DoD activity."[212] The proposed rule also defined nonpublic information as "any Government or third-party information that [was either] (1) . . . exempt from disclosure under [FOIA] or otherwise protected from disclosure by statute, Executive order or regulation; or (2) [information that] [h]as not been disseminated to the general public, and the Government has not yet determined whether the information can or will be made available to the public."[213] Thus under the rule, information would be handled in accordance with its definition, including the new definitions for DoD information and nonpublic information.

The rule would have established two new clauses under the DFARS. The first clause provided for "Basic Safeguarding of Unclassified DoD Information" by implementing "first-level protection measures."[214] The DoD stated that first-level protection measures would protect government information and help in deterring "unauthorized disclosure, loss, or exfiltration by employing first-level information technology security measures."[215] These first-level security measures would include updated virus protection and installing the latest security software patches.[216]

---

209. The Privacy Act protects individuals from the government disclosing personal identifying information, such as their name or social security number. Privacy Act of 1974, 5 U.S.C. § 552a(a)(5), (b) (2006).

210. Pub. L. No. 104-191, 110 Stat. 1936 (codified in scattered sections of 18, 26, 29, and 42 U.S.C. (2000)). HIPAA protects personal health information held by certain entities. *Understanding Health Information Privacy*, DEP'T OF HEALTH & HUMAN SERVICES, http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html (last visited June 11, 2013).

211. Defense Federal Acquisition Regulation Supplement: Safeguarding Unclassified DoD Information, 76 Fed. Reg. at 38,092 (revising DFARS clause 252.204-7000, Disclosure of Information).

212. *Id.*

213. *Id.*

214. *Id.* at 38,090.

215. *Id.*

216. *Id.*

The second clause provided for "Enhanced Safeguarding of Unclassified DoD Information."[217] The enhanced measures would apply to the "encryption of data for storage and transmission, network protection and intrusion detection, and cyber intrusion reporting."[218] The clause required a contractor to implement the enhanced safeguarding measures in its "project, enterprise, or company-wide unclassified information technology system(s)."[219] To satisfy the requirement, a contractor would, at a minimum, have to comply with certain specified NIST SP 800-53 security controls under the proposed rule.[220] The DoD provided some discretion to contracting officers in controlling the application of security controls, allowing that "tailoring in scope and depth appropriate to the effort may be used as authorized in the contract."[221] For those controls not implemented, the contractor would be required to prepare a written determination for the contracting officer explaining how the required security control is inapplicable, or how an alternative control or protective measure would be used to achieve equivalent protection.[222] The language appeared to provide the contracting officer with some degree of discretion in how to apply the minimum security controls for enhanced security. The reference, however, to "tailoring," indicates that the contracting officer's discretion would likely be limited.[223] Further, enhanced security measures would require contractor personnel to "procure and use only DoD-approved identity authentication credentials for authentication to DoD information systems."[224]

The enhanced measures also imposed cyber-incident reporting requirements, which would help in assessing the impact and methods of loss, and allow for the use of that information to improve protection. The reporting requirements called for reporting any discovery of a "cyber-incident" to the DoD within seventy-two hours.[225]

---

217. *Id.*
218. *Id.*
219. *Id.* at 38,094.
220. *Id.* (listing recommended security controls for federal information systems and organizations under NIST SP 800-53 and dividing into the following families: Access Control; Awareness and Training; Audit and Accountability; Configuration Management; Contingency Planning; Identification and Authentication; Incident Response; Maintenance, Physical and Environmental Protection; Program Management; System and Communication Protection; and System and Information Integrity).
221. *Id.*
222. *Id.*
223. *Id.*
224. *Id.*
225. *Id.*

The proposed rule provided two examples of a "reportable cyber-incident": (1) incidents where DoD information residing on or "transiting through" a contractor's, or its subcontractors', unclassified information systems is compromised, such as through "possible data exfiltration or manipulation"; and (2) all other incidents that allow unauthorized access to information systems where DoD information is located or "transiting through."[226]

In preparing a cyber-incident report, the DoD was prescriptive in the steps that contractors would be required to take to support forensic analysis and a preliminary damage assessment. It mandated that contractors: (1) perform "an immediate review of its unclassified network for evidence of intrusion;" (2) review all compromised information to specifically determine what information presented a threat to "DoD programs, systems, or contracts, including military programs, systems, and technology;" (3) preserve and protect any images of compromised information systems and "monitor/packet capture data" until the DoD determined; (4) work together with the DoD Damage Assessment Management Office to identify any compromised systems; and (5) "[p]rovide points of contact to coordinate damage assessment activities."[227]

The DoD required under the proposed rule that any contractor or subcontractor involved in a cyber-incident would have to mark attribution information reported or provided to the Government.[228] It qualified that the government would be restrained in its use of the attribution information, for instance restricting disclosure "only to authorized persons for cyber security and related purposes."[229] The DoD also clarified that any attribution information shared outside of the Department would be only to those entities with a need to know for cybersecurity and related activities, including support contractors, but only to the extent they were subject to confidentiality requirements.[230]

Nothing in the proposed clause would limit the government's ability to carry out its duties to further its interest in national security, such as law enforcement and counterintelligence activities.[231] Furthermore, the proposed rule authorized the use of information

226. *Id.*
227. *Id.* at 38,095.
228. *Id.*
229. *Id.* (providing the following examples as authorized purposes: forensic analysis, incident response, compromise, or damage assessments, law enforcement, counterintelligence, threat reporting, and trend analyses).
230. *Id.*
231. *Id.*

derived from any of the enhanced safety measures to support "an investigation and prosecution of any person or entity."[232]

The DoD also clarified that contractors would be obligated to coordinate with third parties to provide information that might otherwise be barred by terms of a non-disclosure agreement (NDA). The DoD specified that contractors would have to seek written permission from "the owner of any third-party data believed to be contained in images or media that may be shared with the Government."[233] If the contractor were unable to obtain written permission, the DoD allowed that the third-party information owner could have the right to pursue legal action against the contractor or its subcontractors with "access to the nonpublic information for breach or unauthorized disclosure."[234]

To the extent that some of the proposed FISMA Amendments calling for reporting to an IG might have a chilling effect on would-be small businesses and other inexperienced contractors, the DoD proposed rule would have had an even greater effect. The DoD expressly authorized the government to seek criminal prosecution of those seeking to "infiltrate or compromise information on a Contractor information system."[235] Such a prosecution might undoubtedly have affected contractor or subcontractor employees seeking to obtain unauthorized access to their company's systems and information. The specter of prosecution is, of course, a powerful deterrent. What remained unclear was how the government could bring a criminal investigation or prosecution against the contracting or subcontracting entity itself. Further, the DoD made clear that contractors or subcontractors might be subject to civil liability for breaching NDAs applying to third-party information.[236] This too could likely serve as a powerful deterrent to small businesses and inexperienced contractors seeking to work with DoD agencies.

Adding to the burden that would be imposed under the proposed rule, the DoD clarified that for both information security and reporting requirements, its requirements would be supplementary and therefore insufficient to satisfy any other information security

232. *Id.*
233. *Id.*
234. *Id.*
235. *Compare id.* (requiring contractors to report certain cyber-security incidents to DoD within seventy-two hours of discovery), *with supra* text accompanying note 165 (noting the "chilling effect" on small businesses imposed by new FISMA amendments requiring a contractor to report security incidents to the IG within twenty-four to forty-eight hours of discovery).
236. Defense Federal Acquisition Regulation Supplement: Safeguarding Unclassified DoD Information, 76 Fed. Reg. at 38,095.

and reporting requirements.[237] Thus, for the enhanced security measures clause, the proposed rule would impose additional security and reporting requirements.

2. The DoD's initial regulatory flexibility analysis demonstrated the adverse effects on small businesses

Per the requirements of the Regulatory Flexibility Act (RFA),[238] DoD developed an Initial Regulatory Flexibility Analysis (IRFA) to analyze the economic impact the rule would have on small entities.[239] The DoD concluded as part of its analysis that first-level protection providing for basic guard would not have a significant cost impact on contractors because these measures "are typically employed as part of the routine course of business."[240] This did not outweigh the "enormous detriment" the DoD and contractor businesses might experience in the event of a cyber-incident, either in the form of reduced system performance, the loss of valuable information, or both.[241]

A much more significant impact would be brought about by the enhanced security protections under the proposed rule. The DoD estimated the rule would apply to nearly 49,000, or approximately 76% of DoD's small business contractors, as they would be required to provide protection of DoD information at the enhanced level.[242] The DoD acknowledged that "large contractors handling sensitive information already have sophisticated information assurance programs and can take credit for existing controls with minimal additional cost."[243] That, the DoD stated, would not be true for most small and mid-sized businesses with less sophisticated programs, and which would as a result incur costs in meeting the additional requirements.[244] The DoD calculated that "a reasonable rule of

237. *Id.* at 38,094. More specifically, the DoD clarified that contractors would remain responsible for safeguarding and reporting incidents affecting all other unclassified DoD information, including Critical Program Information, Operations Security, ITAR, Export Administration Regulations, FOIA, information described as For Official Use Only, Sensitive But Unclassified, Limited Distribution, Proprietary, Originator Controlled, Law Enforcement Sensitive, PII, Privacy Act, and HIPAA. *Id.*

238. The RFA requires a federal agency to prepare an Initial Regulatory Flexibility Analysis if it determines that a proposed rule could have an impact on a substantial number of small entities. Regulatory Flexibility Act of 1980, 5 U.S.C. § 603(a) (2006).

239. Defense Federal Acquisition Regulation Supplement: Safeguarding Unclassified DoD Information, 76 Fed. Reg. at 38,090.

240. *Id.* First-level protective measures include updated virus protection, security patch updates, etc. *Id.*

241. *Id.*

242. *Id.* at 38,091.

243. *Id.*

244. *Id.*

thumb for small businesses is that information technology security costs are approximately 0.5% of total revenues. Because there are economies of scale when it comes to information security, larger businesses generally pay only a fraction of that estimated cost as a percentage of total revenue."[245]

The DoD in its IRFA summary did not indicate whether it calculated the prospective costs that small business contractors might incur in the event they had to defend against potential civil or criminal prosecution arising from reports and compelled third-party information sharing necessitated as part of its cyber reporting obligations. As with the basic costs of information security, large businesses would enjoy economies of scale compared to small businesses in such cases. Small businesses would no doubt incur significantly more relative cost in defending against prosecution or civil suits arising from cyber-incidents. Consequently, the DoD's IRFA summary made clear that if its proposed rule were to be finalized, the rising tide of cybersecurity would indeed have an immense effect on a significant portion of its small business contractors.

The DoD solicited comments on the proposed rule, and certain responses highlighted the increased burden that the rule would impose. For example, the National Defense Industrial Association[246] (NDIA) pointed out that the proposed rule would "conflict with the existing CUI guidance and fundamental principles of the CUI Executive Order," by extending the "safeguarding and dissemination controls to non-sensitive information."[247] This would "impede information sharing by omitting 'risk' as the primary determinate for applying safeguards."[248] To further illustrate the issue, the NDIA noted that though the "identified subset of NIST SP 800-53 standards and controls improve clarity and consistency, they are not risk-based and as such, pose an unnecessary and unjustified burden on the industry."[249] Essentially, the prescriptive approach imposed under

245. *Id.*
246. *See About Us: Who We Are—What We Offer*, NAT'L DEF. INDUS. ASS'N, http://www.ndia.org/AboutUs/Pages/default.aspx (last visited June 11, 2013) (explaining that NDIA is a defense industry association that lobbies and coordinates with the federal government).
247. Letter from Major Gen. Barry Bates, Vice President, Nat'l Def. Indus. Ass'n, to Julian Thrash, Office of Under Sec'y of Def. for Acquisition, Tech, & Logistics, Dep't of Def. 2 (Dec. 14, 2011) [hereinafter NDIA Comment Letter], *available at* http://www.regulations.gov/contentStreamer?objectId=0900006480f839f0&disposition=attachment&contentType=pdf.
248. *Id.*
249. *Id.*

the DoD's proposed rule would supersede the risk-based method of applying SP 800-53 security controls under FISMA.[250]

Under the DoD's prescribed rule, not only were contractors prevented from undertaking a risk-based analysis to ascertain the appropriate application of security controls, contracting officers were also restricted in the discretion they could apply in accepting alternative security measures in the place of the SP 800-53 controls.[251] The NDIA also refuted the DoD's assumptions that most Defense Industrial Base (DIB) contractors already have systems in place that comply with NIST SP 800-53 and that imposing the requirements would impose a minimal cost. Based on their experience and subcontracting relationships with small businesses, NDIA argues that DIB small business contractors would have to incur a considerable cost because most do not have "NIST controls in place and are under-resourced."[252]

NDIA proposed, instead, establishing an objective standard for risk-based safeguards, and allowing the contractor flexibility in achieving that standard.[253] Within the NDIA proposal, while the sponsoring government agency has discretion to audit individual contractor's safeguards based on risk, the default position would be to allow contractors to demonstrate that they meet the standard.[254]

The NDIA pointed out from experience the reality that cybersecurity regulation could have a disproportionate effect on small businesses and inexperienced contractors unfamiliar with the application of security controls within the FISMA context.[255] The cost of implementing the infrastructure, hiring personnel experienced with the high level of information security necessary to ensure compliance, and having the wherewithal to work with the DoD in the event of a cyberintrusion could all prove to be prohibitive to a number of small businesses and new market entrants.

---

250. *See id.* ("Proper selection and application of the NIST SP 800-53 controls must be driven by the sensitivity of the information and the impact of compromise or loss. Such a correlation is absent, or at least not apparent, in the rule's selection of this particular subset of NIST SP 800-53 controls and tables.").

251. Defense Federal Acquisition Regulation Supplement: Safeguarding Unclassified DoD Information, 76 Fed. Reg. 38,089, 38,094 (proposed June 29, 2011) (to be codified at FAR pts. 204, 252) ("[T]ailoring in scope and depth appropriate to the effort may be used as authorized in the contract").

252. NDIA Comment Letter, *supra* note 247, at 2.

253. *Id.*

254. *Id.*

255. *Id.*

E. Efforts To Provide For Information Security Through the Federal Procurement System

In August 2012, the Department of Defense, the GSA and NASA proposed a new rule to update the FAR, which prescribed Basic Safeguarding of Contractor Information Systems.[256] The proposed rule, issued as FAR Case 2011-020, requires a set of safeguards for government contractor information systems that contain or process non-public information provided by or generated for the government.[257] The safeguards are required to address a number of basic information security requirements.[258]

The safeguards are new protections under the FAR. They are being prescribed pursuant to a newly proposed FAR subpart 4.17, Basic Safeguarding of Contractor Information Systems,[259] and applied under a new FAR clause by the same name to be incorporated into all federal contracts under which a contractor's information system may "contain information provided by or generated for the Government (other than public information)."[260] The new FAR clause is intended to be widely applied, even allowing contracting officers discretion to apply the safeguarding requirements at levels under the relatively low dollar-value simplified acquisition threshold[261] when inclusion is determined to be appropriate.

1. Analysis of the Proposed Basic Information Security Requirements

Similar to the DoD proposed rule, this proposed rule does not apply to public information, which an agency "discloses, disseminates, or makes available to the public."[262] It instead applies to information,

---

256. Federal Acquisition Regulation: Basic Safeguarding of Contractor Information Systems, 77 Fed. Reg. 51,496 (proposed Aug. 24, 2012) (to be codified at FAR pts. 4, 7, 12, 42, 52).

257. *Id.* at 51,497.

258. *See id.* at 51,499 (including the restriction of information; protection of electronic, voice, and fax transmissions; apply minimum physical and electronic security requirements; ensure sanitization of media used for processing information; applying intrusion protection such as anti-virus, spyware, and software patches; and limiting transfers to subcontractors needing information necessary for contract performance).

259. *Id.* at 51,498.

260. *Id.*

261. The simplified acquisition threshold is $150,000. *See* Federal Acquisition Information: Inflation Adjustment of Acquisition-Related Threshold, 75 Fed. Reg. 53,129, 53,130 (Aug. 30, 2010) (to be codified at FAR pts. 1–3, 5–8, 12–13, 15–17, 19, 22–23, 28, 32, 36, 42, 50, 52).

262. *Compare* Federal Acquisition Regulation: Basic Safeguarding of Contractor Information Systems, 77 Fed. Reg. at 51,497–98 (citing 44 U.S.C. § 3502 (2006)) (stating the applicability of the proposed rule does not cover public information), *with* Defense Federal Acquisition Regulation Supplement: Safeguarding Unclassified DoD Information, 76 Fed. Reg. 38,089, 38,091–92 (proposed June 29, 2011) (to be

defined by the Committee on National Security Systems Instruction 4009 as "any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual."[263]

The DoD, GSA, and NASA expressly stated that the requirements proposed in the rule are "an extension of the requirements, under [FISMA], for Federal agencies to provide information security for information and information systems that support the operations and assets of the agency, including those managed by contractors."[264] The proposed rule expressly applies to subcontractors as well.[265]

Under the proposed rule, a contractor must apply basic safeguarding requirements to protect applicable information.[266] The basic requirements are a mix of prescriptive minimum safeguards, as well as more broadly worded references to "best" levels of security. For instance, the basic safeguarding procedures for protecting information on public computers or Web sites require a contractor to process the applicable information on non-public computers or computers that have access control and to only post information on websites that restrict public access.[267] The requirement is very prescriptive, stating a clear prohibition on the use of public computers lacking access control, but allowing for the posting of information to websites that control access by user ID and password or user certificates, among other security technologies.[268] In transmitting electronic information, however, the requirements are more broadly stated in that when such information is transmitted, technology and processes that "provide the best level of security and privacy available" satisfy the basic safeguarding requirements.[269]

---

codified at FAR pts. 204, 252) (explaining that the scope of the proposed rule extends to unclassified "DoD information," which is defined as "any nonpublic information that . . . [h]as not been cleared for public release").

263. Federal Acquisition Regulation: Basic Safeguarding of Contractor Information Systems, 77 Fed. Reg. at 51,497.

264. *Id.* at 51,497 (citing 44 U.S.C. § 3544(a)(1)(A)(ii)).

265. *See id.* ("This proposed rule applies to all Federal contractors and appropriate subcontractors regardless of size or business ownership.").

266. *Id.*; *see also supra* note 258 (describing the applicable information and areas in which that information shall be protected).

267. Federal Acquisition Regulation: Basic Safeguarding of Contractor Information Systems, 77 Fed. Reg. at 51,499. This provision explains that "public computers" are "those available for use by the general public in kiosks, hotel business centers." *Id.* In addition, web sites may restrict public access by means of "user ID/password, user certificates, or other technical means, and that provide protection via use of security technologies." *Id.*

268. *Id.*

269. *Id.*

This "best level" requirement, however, is much less specific. There is no definition of what technology or processes provide the "best level of security and privacy available."[270] Further, there is no directive as to how that "best level" is to be determined with the "given facilities, conditions, and environment."[271] It would be difficult for any contractor, much less a small business or inexperienced contractor, to know whether it was complying with this requirement. Interestingly, the requirements for transmitting voice and fax information is tailored with relatively more specificity, requiring that a contractor ensure that it transmits information "via voice and fax only when the sender has a reasonable assurance that access is limited to authorized recipients."[272] It is not clear why the requirements for voice and fax transmission are more process-oriented than transmitting e-mails, text messages, or blog posts. Arguments can be made that an e-mail transmission, which by its nature will go directly to one recipient, is more secure than a fax transmission, which may be addressed to a particular recipient, but which generally arrives to a centralized queue to which many others have access. Despite the arguments that can be raised, there are clearly differences in the safeguards prescribed for electronic transmissions versus voice and fax transmissions.

For physical and electronic barriers, the requirement is, again, prescriptive. It requires that information must be protected "by at least one physical and one electronic barrier (e.g. locked container or room, login and password) when not under direct individual control."[273] Unlike the requirements for the safeguarding of electronic transmissions, calling for consideration of "facilities, conditions, and environment," physical and electronic protections are prescribed as basic minimums.[274] Arguably, it would be reasonable for a contractor to consider the same variables (facilities, conditions, and environment) when determining whether to add more levels of physical and electronic protections.

The requirements on intrusion protection are similar. They require a contractor to provide "at a minimum" two protections

---

270. *Id.*
271. *Id.*
272. *Id.*
273. *Id.*
274. *Compare id.* ("Transmit email, text messages, blogs, and similar communications . . . using technology and processes that provide the best level of security and privacy available, given facilities, conditions, and environment."), *with id.* ("Protect information . . . by at least one physical and one electronic barrier . . . when not under direct individual control.").

against computer intrusions and data compromise: one for current malware protection, the other for security-related software upgrades.[275] The prescriptions are basic, but unlike the safeguarding requirements applicable to electronic transmissions, they do not address whether and under what circumstances additional safeguards should be considered and applied.

2. The basic requirements appear not to be burdensome, but also appear inconsistent

In the IRFA summary to this proposed rule, the DoD, NASA, and GSA clarified that it would apply to both small and large businesses.[276] The cost of the rule was not considered significant, since the first-level protective measures (including virus protection and software patches) are typically employed as part of the regular course of doing business.[277] It was also concluded that the "prudent business practices designed to protect an [IT] system are typically a common part of everyday operations."[278]

The DoD, GSA, and NASA expressly state that the proposed FAR changes "may be altered as necessary to align with any future direction given in response to ongoing efforts led by the National Archives and Records Administration in the implementation of Executive Order 13556 . . . on 'Controlled Unclassified Information'"[279] It is possible that soon after the proposed rule is implemented, it will have to change to accommodate the implementation of the new approach to identifying and safeguarding CUI throughout the government. In that respect, the proposed rule may present additional compliance burdens that exceed the basic steps necessary to ensure that government information is safeguarded.

The proposed rule also clarifies that the new clause "is not intended to implement any other, more specific safeguarding requirements, or to conflict with any contract clauses or requirements that specifically address the safeguarding of information or information systems."[280] While it may be helpful to clarify that these

275. *Id.* ("Provide at a minimum the following protections against computer intrusions and data compromise: (i) Current and regularly updated malware protection services, e.g., anti-virus, antispyware. (ii) Prompt application of security-relevant software upgrades, e.g., patches, service-packs, and hot fixes.").
276. *See id.* at 51,497–98 (stating that this proposed rule applies to contractor and subcontractors "regardless of size or business ownership").
277. *Id.* at 51,497.
278. *Id.*
279. *Id.*
280. *Id.*

basic safeguards are intended to supplement and not supersede any other contract requirements, the characterization of these safeguards as an "extension" of FISMA requirements might lead a contractor to conclude that meeting these basic requirements is sufficient to satisfy any and all FISMA requirements that may be incorporated into a particular contract. The fact remains that the information security requirements under FISMA have expressly applied to contractors handling federal information and information systems since FISMA's passage.[281] Thus, contract clauses already exist that require FISMA compliance for a contractor seeking to work with federal information or information systems.[282] The requirements under FISMA call for a more risk-based approach to determining the appropriate level of information security than the prescriptive approach established under the proposed rule.[283] Thus, characterizing the proposed rule as an "extension" of FISMA presents a risk that small business contractors or inexperienced contractors unfamiliar with FISMA compliance may mistakenly rely only on the basic safeguards prescribed, without appreciating or addressing the additional considerations under FISMA. It is therefore important for federal contracting professionals to incorporate all FISMA-related requirements in applicable contracts.

IV. HOW TO BETTER ENSURE ALL BOATS WILL RISE WITH THE TIDE

Much of this Article has discussed the tension between the government's need to ensure robust information security and the potential for new information security requirements to overwhelm small business contractors or other contractors inexperienced in information security requirements. If information security compliance becomes too cumbersome, the government risks contractors choosing to forego contracting opportunities to avoid the risk of liability that may arise from breaches or noncompliance.

There are some potential avenues within the federal procurement system that could both account for the government's need to ensure higher levels of information security and help ensure that all contractors have an opportunity to compete in such an environment.

---

281. *See* Federal Information Security Management Act of 2002, 44 U.S.C. §§ 3541–3549 (2006) (stating that the purpose of the Act is to "provide for development and maintenance of minimum controls required to protect Federal information and information systems").

282. *See* Federal Acquisition Regulation: Basic Safeguarding of Contractor Information Systems, 77 Fed. Reg. at 51,497 (discussing that the FISMA requires information security compliance from contractors).

283. *See generally* 44 U.S.C. § 3544(a)–(b) (requiring the level of information security provided be based on risk and magnitude of potential harm).

These avenues involve either augmenting federal mentor-protégé programs or adjusting some of the subcontracting limitations established under the FAR to account for higher levels of information security.

A. Amend Mentor-Protégé Programs To Provide for Information Security and Cybersecurity Compliance Assistance

Mentor-Protégé programs have been established under the SBA and a number of other federal agencies to encourage large "mentor" businesses to provide various forms of business development assistance to "protégé" firms,[284] usually members of the SBA's 8(a) Business Development program.[285] In exchange for business development assistance, mentors are eligible to enter into joint ventures with their small business protégés to pursue certain small business and 8(a) set-aside contracts for which the large businesses would normally be ineligible.[286]

Each mentor-protégé agreement, required to be in written form, must provide an assessment of the protégé's needs, a detailed description of the way in which the mentor will address those needs, and a timeline for the delivery of the mentor's assistance.[287] Assistance provided under the SBA program includes "management and/or technical assistance, loans and/or equity investments, cooperation on joint venture projects, or subcontracts under prime contracts being performed by the mentor."[288] Under the DoD Program, a developmental program devised for the protégé concern will describe how the mentor's assistance will not only increase the protégé's ability to participate in federal and commercial contracts

284. *See generally* 13 C.F.R. § 124.520 (2012) (explaining the rules governing SBA's Mentor/Protégé program).

285. To be a participant in the SBA's 8(a) Business Development program, a concern must be a small business that demonstrates potential for success and is unconditionally owned and controlled by one or more socially and economically disadvantaged individuals. *See id.* § 124.101. The regulations governing the 8(a) Business Development program also govern the SBA's mentor-protégé program. *See id.* § 124.520(c)(2) ("Only firms that are in good standing in the 8(a) [Business Development] program . . . may qualify as a protégé."). Mentor-protégé programs have been established in twelve other federal agencies in addition to the SBA. *See* WILLIAM B. SHEAR, U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-11-548R, MENTOR-PROTÉGÉ PROGRAMS HAVE POLICIES THAT AIM TO BENEFIT PARTICIPANTS BUT DO NOT REQUIRE POSTAGREEMENT TRACKING 1 (2011). Of note, the Department of Defense has a mentor-protégé program that allows large business mentors to work with 8(a) Business Development program participants in order to gain access to certain small business set-aside requirements. The Department of Defense mentor-protégé program regulations are found in Appendix I to DFARS. FAR § 219.7101.

286. 13 C.F.R. § 124.520(d).

287. *Id.* § 124.520(e).

288. *Id.*

and subcontracts, but also increase subcontracting opportunities for small businesses in industries where small firms are less dominant.[289]

In recent years, mentor-protégé programs have expanded throughout the government.[290] Aside from the DoD, which established its mentor-protégé program in 1991, twelve other federal agencies have since established mentor-protégé programs.[291] Further, the National Defense Authorization Act for Fiscal Year 2013 recently directed the SBA to establish a mentor-protégé program aimed at assisting not just 8(a) small businesses, but all small businesses.[292] Consequently, the mentor-protégé program has a significant presence in the federal acquisition system.

One way to ensure small businesses are not left behind by new information security regulations is to add an element to mentor-protégé agreements that expressly calls for large business mentors to provide investment, training, and technical assistance geared to ensuring the small business is well-equipped to satisfy information security requirements. If the SBA and other federal agencies added this type of assistance to their mentor-protégé program agreements, they would likely increase the incentives already found in mentor-protégé programs. Agencies would have stronger assurance that their small business protégés were receiving guidance, resources, and training to ensure information security compliance. Mentors would continue to have access to small business set-aside contracts.

A mentor working with a protégé as part of a joint venture would likely position itself well in competitions for contracts requiring information security and cybersecurity compliance. The mentor would also have the benefit of knowing if flow-down information security requirements were being satisfied in virtue of its close connection with the small business protégé. The nature of the mentor-protégé relationship would thus allow for a more free-flowing exchange of information between the parties. In the event of a breach or any other information security-related issues, the mentor would be in a position to help the protégé address the issues immediately and appropriately.

---

289. FAR app. I-107(f).

290. *See* SHEAR, *supra* note 285, at 15 (listing the years in which each federal mentor-protégé program was implemented).

291. *Id.*

292. *See* National Defense Authorization Act for Fiscal Year 2013, Pub. L. No. 112-239, sec. 1641, § 45(a)(2), 126 Stat. 1632, 2077 (to be codified at 15 U.S.C. § 657r (amending the Small Business Act § 45 to authorize establishment of "a mentor protégé program for all small business concerns").

A mentor-protégé program that expressly provided for information security and cybersecurity investment and assistance in protégés would likely be a significant incentive to small businesses. It would put them in a position to compete for requirements calling for information security and cybersecurity compliance through the aid of a large business mentor. With the assistance of a mentor-protégé program, small businesses would have an introduction to information security and cybersecurity requirements, and learning from these opportunities they could further develop expertise in the field. Doing so would help foster competition for federal agencies requiring information security and cybersecurity compliance from contractors, while at the same time helping to ensure that competitors are well-versed in all of the requirements necessary to assure adequate levels of security.

B. Amend the Fifty Percent Rule To Accommodate Contracts Requiring Information Security and Cybersecurity Compliance to Foster Increased Small Business Involvement

Another potential manner to foster small business participation in contracts calling for information security and cybersecurity protections involves adjusting the levels under the fifty percent rule. The fifty percent rule is based in the provisions of FAR clause 52.219-14, Limitations on Subcontracting.[293] Under the clause, at least fifty percent of the contract performance must be reserved for the concern where the contract or a portion of the contract for services or manufacturing of supplies has been set aside for small businesses or 8(a) concerns.[294]

Generally under small business set-aside contracts, a small business must perform work for at least fifty percent of the cost of contract performance for employees or manufacturing of supplies.[295] This helps to ensure that subcontractors are performing substantial portions of the work under a set-aside contract rather than being treated merely as pass-through business concerns. Further, the small business regulations administered by the SBA require that small business prime contractors perform substantial work.[296] This

293. FAR § 52.219-14.
294. *Id.* § 52.219-14(b).
295. *See id.* A contract for services requires "[a]t least 50 percent of the cost of contract performance incurred for personnel shall be expended for employees of the concern." A contract for supplies calls for the concern to "perform work for at least fifty percent of the cost of manufacturing the supplies, not including the cost of materials." *Id.*
296. *See* 13 C.F.R. § 121.103(h)(4).

requirement, referred to as the "ostensible subcontractor rule" prevents a large business subcontractor from performing "primary and vital requirements of a contract."[297] The ostensible subcontractor rule also applies to a subcontractor on which a small business prime is "unusually reliant."[298] In that case, all aspects of the relationship are considered, including, but not limited to; contract management, technical responsibilities, and the percentage of subcontracted work.[299]

There are some instances, however, where the restrictions of the fifty percent rule do not apply.[300] As can be seen from construction contracts, certain types of contracts necessitate a change in the percentage breakdown. Those contracts, under which general contractors perform a lower percentage of the work relative to their aggregated subcontractors' work, require much less of a work share for subcontractors.[301] This reflects a reality of the construction industry and is an equitable means of ensuring subcontractors perform their necessary share of set-aside contracts, but not more than would be regularly expected in the industry.

The same could be applied to small business prime contractors on contracts with information security or cybersecurity-related requirements. It may be that percentages could be developed that would limit a small business prime contractor's work share to a percentage lower than fifty percent, and would not include requirements for information security and cybersecurity compliance.[302]

Further, the "ostensible subcontractor rule" might be altered to allow a carve-out for those responsibilities for information security and cybersecurity compliance. Doing so would reduce the risk of the SBA finding a large business is an "ostensible subcontractor," based on its efforts to ensure compliance with information security and cybersecurity requirements.

Though such an approach would not foster the degree of hands-on engagement between large business mentors and small business protégés under a mentor-protégé program, it could help incentivize

297. *Id.*
298. *Id.*
299. *Id.*
300. *See* FAR § 52.219-14(b)(3) (describing the percentage breakdown for general construction contracts).
301. *Id.* (requiring the contractor to perform a smaller percentage of general construction and construction by special trade contractors).
302. The large business subcontractor would be responsible for ensuring compliance.

small businesses and large businesses to enter into teams to compete for set-aside procurements, which would allow the large business contractor to address information security and cybersecurity compliance. In that respect, federal agencies would still be able to include small businesses in procurements requiring information security and cybersecurity compliance. Small businesses, in turn, would be less constrained from competing for these requirements, knowing that they would not have to face the compliance issues alone. Further, large businesses would have an incentive to team up with small businesses, as they would be able to capture more than fifty percent of a set-aside contract. This would likely foster a trade-off for large businesses. In exchange for dedicating resources to assuring information security and cybersecurity compliance for itself and its small business partner, the large business would have more than a fifty percent share of the work awarded under the contract.

C. Establish Information Security Training Requirements Similar to Recent Privacy Training Mandates

A direct means of ensuring that small businesses and larger businesses lacking experience working with the federal government could be prepared to comply with information security and cybersecurity requirements would be to mandate compliance training. This would reflect FAR Case 2010-013, Federal Acquisition Regulation; Privacy Training, 2010-13.[303] The rule was proposed to require privacy training for contractors.[304]

Agencies proposed minimum requirements for privacy training to ensure consistency across the government. The rule intended to ensure that contractors, regardless of the agency they were servicing, were cognizant of seven mandatory elements of privacy.[305] Privacy Training mandated that although agency-provided privacy training would be sufficient, the contractor itself could develop the training package.[306] Either way, any contractor employee involved in handling information protected under the Privacy Act would be aware of the minimum requirements necessary to safeguard the information.

---

303. Privacy Training, 76 Fed. Reg. 63,896 (proposed Oct. 14, 2011) (to be codified at FAR pts. 24, 52).

304. *Id.* at 63,897 (proposing "to ensure that contractors identify employees who require access to a Government system of records, handle personally identifiable information, or design, develop, maintain, or operate a system of records on behalf of the Federal Government, and who therefore, are required to complete privacy training initially upon award of the procurement and at least annually thereafter").

305. *Id.*

306. *Id.*

The same model might be developed for ensuring satisfaction of information security and cybersecurity compliance requirements. The requirements to ensure adequate information security and cybersecurity protections are arguably broader than Privacy Act compliance requirements. Incorporating a training mandate to cover at least a basic level of security requirements might help put small business and inexperienced larger business contractors on a more level playing field with other government contractors. The training might not immediately equip a contractor to comply with information security or cybersecurity requirements. It might, however, train those contractors on the steps necessary to ensure compliance with all relevant requirements. For instance, if a training gave contractors information on the review, consideration, and application of security controls under NIST SP 800-53, it may not put them in a position to immediately comply with information security and cybersecurity requirements. But it might give them the tools to move toward a posture of compliance.

The recently proposed basic safeguarding requirements under FAR Case 2011-020 represent a possible step in the direction toward a training mandate. But the steps required would likely be less geared toward what specific actions to take in achieving adequate security[307] and more geared toward what considerations to make. Under a risk-based mitigation scheme, such as that established under FISMA, a training giving contractors the tools to understand what types of risk-based analyses to undertake would help ensure small businesses and inexperienced contractors have more information available so as to ascertain how they could compete for requirements necessitating information security protections.

D. Continue Information Sharing To Clarify Information Security Compliance

Some of the more positive steps taken in information security and cybersecurity in recent years are: the emphasis on information sharing and the consistent application of protections across the government.[308] To date, the proposed rules prescribe requirements that government contractors must follow in order to properly ensure

307. For example, ensuring one physical security and one electronic security element.

308. *See generally* Federal Acquisition Regulation: Basic Safeguarding of Contractor Information Systems, 77 Fed. Reg. 51,496 (proposed Aug. 24, 2012) (to be codified at FAR pts. 4, 7, 12, 42, 52); Defense Federal Acquisition Regulation Supplement: Safeguarding Unclassified DoD Information, 76 Fed. Reg. 38,089 (proposed June 29, 2011) (to be codified at FAR pts. 204, 252).

information security. None of the rules, however, require contracting officers across departments or agencies to share information about compliance requirements. It could be that efforts to share that type of information could establish some consistency in the application of information security or cybersecurity requirements. It could vary from contracting officer to contracting officer as to what actions or protections established by a contractor might amount to adequate compliance. The more inconsistency in the system, the more a particular contractor will find it difficult to comply across departments and agencies. This could limit the ability of a contractor to seek out other departments and agencies to provide relevant services.

If there is some consistency, however, a contractor can more easily seek out work with other departments and agencies in an effort to diversify and increase its share of contracts. Small businesses and larger inexperienced contractors would benefit from this consistency in particular, as it would lower both the cost and the risk of enduring varying compliance standards across different agencies. Even these basic efforts could help cultivate the involvement of small businesses and larger inexperienced contractors in their efforts to keep up with the rising tide of cybersecurity regulations.

E. Consider an Iterative Approach to Compliance Requirements

The movement from the DoD's proposed rule on handling CUI to the more general proposed rule from the DoD, GSA, and NASA requiring basic information security requirements serves as a helpful model for allowing more contractor involvement in compliance efforts. The DoD proposed rule was broad in scope and, by its own analysis, threatened to impose a disproportionate cost of compliance on small businesses. The subsequent rule establishing basic information security requirements was almost the opposite. It was intended to be applied to many government contractors, but prescribed very basic minimum requirements. Though the proposed rule for basic protections represents a tide that rises much more gradually, it would more likely lift all "boats." That is to say, it would allow for greater compliance from a greater number of contractors, including small businesses and inexperienced contractors.

If information security and cybersecurity regulations are established in a more iterative process, it may allow for more government contractors to keep pace and ensure compliance for all. Iterative steps could be imposed in a number of ways. They might first be applied under contracts exceeding a certain dollar value,

which would help build familiarity with a requirement before it could be applied to a broader range of contracts. Steps might also be applied prescribing increasingly stringent levels of protection. For example, agencies might build on the minimum basic requirements under the recent proposed rule for most contractors by introducing a basic class of high-level protections (some of which were reflected under the DoD proposed rule). The high-level protections might focus on one aspect of information security compliance, in an effort to lower the relative cost and risk for small businesses and inexperienced contractors to bear. This more iterative approach would help keep contractors involved in the regulatory process and prevent small businesses from falling behind in compliance efforts.

In conclusion, the few proposed changes in this section present an opportunity and an incentive for the government and its contracting community to engage in information security and cybersecurity compliance. All parties would benefit from these changes. Small businesses and larger inexperienced contractors would have access to opportunities they might otherwise avoid for lack of resources and experience. Large businesses would have access to set-aside contracting opportunities and would have the chance to foster further development of small business partners. They would also have a hand in ensuring that their joint ventures or teams were compliant, given the nature of interaction fostered in significant amount by mentor-protégé requirements and to a lesser degree in the context of an augmented fifty percent rule, allowing for greater large-business subcontractor involvement. The government would have an incentive to share information between and among agencies, as it would help ensure the agencies' respective contractors were consistent in their compliance efforts. The government would also have an incentive to require information security and cybersecurity training, as it would help ensure all contractors were cognizant of basic information security requirements. Through these proposed steps, the government would be able to satisfy its increasing need for information security and cybersecurity compliance. It could prescribe greater degrees of security as cyber risks grow more prevalent, while also remaining assured that no segments of the contracting community are left behind.

CONCLUSION

As this Article has explored, the government has had to increase information security and cybersecurity regulation in order to keep pace with ever-changing technology and increased frequency and

damage brought about by cyberattacks and information leaks. Though the government has not had success across the board in implementing more stringent regulations, it is clear that both the legislative and the executive branches are intent on ensuring that information security and cybersecurity are addressed, particularly within the government contracts industry.

Absent from the laws and regulations proposed to date has been significant consideration for the effects increased security requirements will have on small businesses or larger, relatively inexperienced contractors that are just getting involved in contracts with the federal government or new federal agencies calling for information security compliance. The result of this trend is a rising tide of increased security requirements, which leads to better information security and cybersecurity protections. The rising tide, however, threatens to leave behind any contractors not equipped with the resources or the experience to keep pace with the many new requirements.

The key issues presented are twofold: 1) either small business and larger inexperienced businesses will not have the opportunity to compete for an increasing number of contracts, or 2) these businesses will try to comply with the requirements, but the lack of resources and experience to do so may leave themselves vulnerable to security breaches.

With that being the case, federal agencies should consider incorporating incentives, protections, or training requirements, and increased opportunities for information sharing that would help small businesses and larger inexperienced businesses get involved in contracts, even where information security and cybersecurity compliance are necessities. Further, the government may want to engage in an iterative process of information security and cybersecurity regulation. That will help ensure the rising tide of regulatory requirements is not so steep as to cut out potential small businesses or other inexperienced contractors. But in any event, the solutions should be structured to incentivize the involvement of all parties in opportunities that call for increased levels of information security and cybersecurity. In so doing, the government will be developing strength throughout all segments of the federal contracting community and ensuring that all boats have the ability to rise with the tide.