Assessing Federal Agencies' Acquisition Rules and Policies Governing Public-Sector Cybersecurity and the Cybersecurity Executive Order's Objective for Harmonization

I. Executive Summary

As one of the world's largest buyers, the federal government's acquisition rules and buying practices have a direct impact upon major segments of the U.S. and global marketplaces. This key federal role extends to information technology (IT) and cybersecurity where the federal government will spend $82 billion on IT products and services in Fiscal Year (FY) 2014 alone, use and oversee huge networks and data repositories, and guard vital information ranging from healthcare data and taxpayer returns to military technology and commercial trade secrets.

The Cybersecurity Executive Order recognizes that the acquisition process must be addressed as part of the overall federal strategy for enhancing cybersecurity. Currently, federal agencies and contractors do not have a unified government-wide acquisition regulation specifying what particular cybersecurity requirements apply to which federal procurements. Individual agencies have filled this void with their own unique choices of acquisition regulations and policies governing cybersecurity, resulting in a multiplicity of cyber regulatory regimes.

To address the regulatory process for federal acquisitions, the Cybersecurity Executive Order required that the acquisition regulators review the current landscape and "address what steps can be taken to harmonize and make consistent existing procurement requirements related to cybersecurity."[1] Fundamental federal acquisition and cybersecurity principles reinforce the Executive Order's call for harmony in cyber acquisition regulations.

- Regulatory Uniformity. As its core purpose, the Federal Acquisition Regulation (FAR) seeks "uniform policies and procedures for acquisition by all executive agencies."[2]

- Cost-Effective Cybersecurity. As a key principle, federal law requires that agencies' cybersecurity programs and risk analyses consider cost-effectiveness[3] – a factor likely to be enhanced by uniform acquisition regulations governing cybersecurity.

- Greater Competition. Like the FedRAMP objective for federal cloud cybersecurity ("approve once, use often"), uniform

---

1 Exec. Order No. 13636, 78 Fed. Reg. 11739, 11742 (Feb. 19, 2013).

2 FAR § 1.101; *see also* FAR § 1.302 (limiting agency-level regulations to those necessary to implement FAR policies and satisfy "specific needs of the agency."

3 44 U.S.C. § 3544 ("implementing policies and procedures to cost-effectively reduce risks to an acceptable level").

acquisition regulations for cybersecurity would reduce the burden for contractors – particularly small businesses – to compete more efficiently against a common government-wide cybersecurity baseline.[4]

- Better Cybersecurity. In response to the Cybersecurity Executive Order, both the Department of Defense (DoD) and the General Services Administration (GSA) acknowledged that harmonized acquisition regulations would enhance cybersecurity.[5]

Current federal acquisition rules governing cybersecurity lack harmony and transparency. Neither federal agencies nor contractors can turn to a single government-wide acquisition regulation to identify the applicable cyber acquisition requirements. Instead, both agency officials and federal contractors must search each agency's individual acquisition regulations and internal policies to identify such requirements. A review of these agency-level cyber regulations reveals a number of challenges.

- Regulatory Disharmony. Not surprisingly, different agencies have adopted different cyber rules and policies. Even within some agencies, inconsistencies exist for certain requirements, such as data breach notification.

- Internal Agency Policies. Nearly all agencies have acquisition requirements imposing internal agency policies and instructions upon contractors, even though these internal guidelines do not appear to be published for public comment as required by law.

- Non-Standard Cyber Requirements. Some agency acquisition regulations impose cyber requirements with minimal reference to government-wide standards for risk assessments, security controls, and other cybersecurity best practices.

In summary, the Cybersecurity Executive Order triggered a much-needed opportunity to address the agency-by-agency patchwork of acquisition regulations and policies governing cybersecurity. Harmonizing the cyber acquisition regulations would offer multiple benefits: (1) reducing agency-by-agency conflicts; (2) promoting greater competition based upon increased commonality in cyber rules; and (3) enhancing cybersecurity by leveraging best practices more cost-effectively across the federal government.

---

[4] The Competition in Contracting Act mandates that agencies "shall obtain full and open competition through the use of competitive procedures . . . ." 10 U.S.C. § 2304(a)(1)(A).

[5] Final Report of the Department of Defense and General Services Administration, *Improving Cybersecurity and Resilience through Acquisition,* p. 9 (Nov. 2013) (hereinafter "DoD/GSA Final Cybersecurity Report (Nov. 2013)").

II. The Federal Role in Regulating Public-Sector Cybersecurity

The Cybersecurity Executive Order focused primarily upon cybersecurity for critical infrastructure, including processes to enhance information sharing and develop a cybersecurity framework to assist the various critical infrastructure sectors.[6] However, cybersecurity for the public sector represented a vital component of the Executive Order. In fact, the public sector continues to be a ripe target for cyber attacks not only due to the vast critical infrastructure housed in the public sector, but also to the magnitude of information collected, used, and stored in federal data banks.

Critical Infrastructure Generally. Of the eighteen critical infrastructure sectors,[7] the public sector shares much of the responsibility, including for the Defense Industrial Base, Government Facilities, Healthcare and Public Health, National Monuments and Icons, and the Postal and Shipping sectors. The federal government conducts huge acquisitions in these sectors, such as the $16 billion DoD procurement covering 2.9 million TRICARE beneficiaries and vast amounts of sensitive healthcare and personal data.[8] Accordingly, the applicable acquisition regulations have a significant bearing upon cybersecurity in these sectors.

IT Infrastructure & the Public Sector. Information Technology (IT) represents another critical infrastructure sector – a sector that contributes over $1 trillion annually to the U.S. economy.[9] According to the Office of Management and Budget (OMB), the federal government represents "the largest buyer of IT on the planet."[10] For Fiscal Year 2014 alone, federal IT expenditures are planned at $82 billion.[11] The magnitude of federal IT purchases is illustrated by the Navy's $3.4 billion award for the Next Generation Enterprise Network contract covering

---

6 Exec. Order No. 13636, 78 Fed. Reg. 11739-44 (Feb. 19, 2013).

7 The first 17 sectors were expressly identified in the original Directive. HSPD 7, "Critical Infrastructure Identification, Prioritization, and Protection," ¶¶ 12, 16 (Dec. 17, 2003) (http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm#1). Under the authority granted by HSPD-7, the DHS Secretary added an eighteenth sector – "Critical Manufacturing" – in March 2008. DHS Website (http://www.dhs.gov/files/programs/gc_1189168948944.shtm).

8 *See, e.g., Health Net Federal Services, LLC,* B-401652.3 *et al.*, Nov. 4, 2009, 2009 CPD ¶ 220.

9 *Cybersecurity: Next Steps to Protect Our Critical Infrastructure: Hearings before the Senate Comm. on Commerce, Science, & Transportation,* 111th Cong. (Feb. 23, 2010) (statement by Vice Adm. McConnell).

10 *Cloud Computing: Benefits and Risks of Moving Federal IT into the Cloud: Hearings Before the House Subcomm. on Government Management, Organization, and Procurement of the Comm. on Oversight and Government Reform,* 111th Cong., p. 10 (July 2010) (statement of Mr. Kundra, Federal CIO).

11 Government Accountability Office (GAO), *Information Technology: Leveraging Best Practices and Reform Initiatives Can Help Agencies Better Manage Investments,* p. 1 (May 7, 2014) (GAO-14-568T).

400,000 computers for 800,000 users in 2,500 locations.[12] As these IT expenditures and acquisitions confirm, public-sector procurements play a major role in both the IT critical infrastructure sector and cybersecurity associated with those IT products and services.

Federal Data Banks. The magnitude and sensitivity of data held by the federal government explain why federal networks and data banks continue to be a prime cyber target. As OMB has reported, "[t]he Federal government is the largest single producer, collector, consumer, and disseminator of information in the United States and perhaps the world."[13] Not only is the volume of data enormous, but much of the data is highly sensitive, including:

- Taxpayer returns (Internal Revenue Service);
- Healthcare information (Medicare, TRICARE, & VA),
- Private-sector proprietary data and trade secrets (FDA & EPA);
- Military technology (DoD & Intelligence community); and
- Personal data (Census Bureau; SSA).

Federal contractors handle, manage, or otherwise access much of this data. With the "Cloud First" policy, the volume of federal information in the hands of contractors will likely grow rapidly. For these reasons, the importance of cybersecurity requirements in federal acquisitions will assume even greater importance in the near future.

III. The Overall Legal Framework for Federal Cybersecurity

With the exception of "national security systems," the Federal Information Security Management Act (FISMA) generally governs federal agencies, their networks, and federal information.[14] While not providing detailed requirements on information security, the statute generally does require security policies and procedures, security controls (management, operational, and technical), periodic testing, incident detection and response, continuity of operations, and training. In addition, the statute applies to certain contractors that: (1) collect or maintain federal information; or (2) use or operate federal information on behalf of federal agencies.[15]

---

[12] Defense Media Activity, "Navy Announces Award of Next Generation Enterprise Network Contract," (June 27, 2013) (http://www.navy.mil/submit/display.asp?story_id=75100).

[13] OMB, *FY 2005 Report to Congress on Implementation of the E-Government Act of 2002*, p. 5 (Mar. 1, 2006).

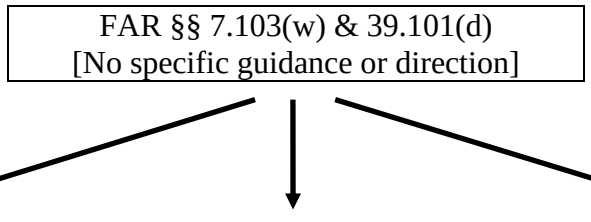
[14] 44 U.S.C. § 3541-49.

[15] 44 U.S.C. § 3544(a), (b).

For uniform guidance on cybersecurity in federal acquisitions, the FAR would be a logical place to look. However, little such guidance exists in the FAR:

> In acquiring information technology, agencies shall include the appropriate information technology security policies and requirements, including use of common security configurations available from the National Institute of Standards and Technology's Web site at *http://checklists.nist.gov*. Agency contracting officers should consult with the requiring official to ensure the appropriate standards are incorporated.[16]

Instead of government-wide guidance, the FAR has largely left cybersecurity implementation to each individual federal agency.[17] Graphically, the regulatory structure looks like this:



DoD DFARS § 204.73, § 239.7102	**GSA** GSAM § 539.7000, § 552.239-71	**DHS** HSAR § 3004.470, § 3052.204-70
NASA NASA FARS § 1804.470, § 1852.204-76	**HHS** HHS FARS § 339.7100, § 352.239-72	**State** DOSAR § 639.107-70, § 652.239-70 & 71
Commerce Commerce FARS § 1339.270, § 1352.239-72	**Transportation** TAR § 1239.70, § 1252.239-70	**HUD** HUD FARS § 2439.107, § 2452.239-70
Education DoEd FARS § 3439.702, § 3452.702	**Energy** DEAR § 904.404(d)(7), § 952.204-77	**VA** Formerly VAAR § 852.273-75 (currently withdrawn)

While not a comprehensive list of all federal agency regulations governing cybersecurity, this chart illustrates the problem. An agency official wishing to implement best practices for cyber acquisition regulations could not look to the FAR, but instead would need to wade through more than a dozen agency regulations to find where and how (if at all) another agency had implemented its acquisition regulations governing cybersecurity.

---

16 FAR § 39.101(d); *see also* FAR § 7.103(w) (requiring agency procedures ensuring that IT acquisitions comply with FISMA, OMB policy including OMB Circular A-130, and NIST guidance and standards).

17 Federal Acquisition Circular (FAC) 2005-06, 70 Fed. Reg. 57450 (Sept. 30, 2005).

Similarly, a government contractor doing business with several federal agencies would need a multi-step process:

- search multiple agency regulations (rather than just the FAR);
- review the contractor's current cybersecurity program against each separate security regime for each agency; and
- adapt the contractor's security program to each of these varying security requirements and policies.

In other words, the contractor would need to conduct multiple compliance reviews to determine initial compliance –and then redo these reviews periodically to assess whether and how any of these multiple agencies had revised their cyber acquisition regulations, thus triggering more changes to the contractor's cybersecurity program for federal contracts. For smaller businesses, such compliance burdens leave few good options – incur prohibitive overhead costs for compliance (making the company less competitive), absorb the risk and uncertainty of non-compliance with this multi-agency security burden (exposing the company to serious contract violations), or get out of the business (depriving federal agencies of competitive and innovative security solutions).

IV. Challenges Posed by the Agency-by-Agency Patchwork of Security Rules

The Cybersecurity Executive Order contained an express directive for DoD and GSA to report on harmonization of acquisition regulations governing cybersecurity:

> Within 120 days of the date of this order, the Secretary of Defense and the Administrator of General Services, in consultation with the Secretary and the Federal Acquisition Regulatory Council, shall make recommendations to the President, through the Assistant to the President for Homeland Security and Counterterrorism and the Assistant to the President for Economic Affairs, on the feasibility, security benefits, and relative merits of incorporating security standards into acquisition planning and contract administration. The report **shall address** what steps can be taken to **harmonize and make consistent existing procurement requirements related to cybersecurity**.[18]

Despite this direction, the DoD/GSA report stated: "Furthermore, the recommendations do not explicitly address how to harmonize rules."[19] While the report did say it would address recommendations on "consistency in interpretation and application of procurement rules," it did not answer the Cybersecurity Executive Order's plain directive: "what steps can be taken to

---

[18] Exec. Order No. 13636, 78 Fed. Reg. 11739, 11742 (Feb. 19, 2013) (emphasis added).

[19] DoD/GSA Final Cybersecurity Report, p. 7 (Nov. 2013).

harmonize" the cyber acquisition requirements. Nor did the report respond to prior American Bar Association (ABA) comments by the Public Contract Law (PCL) Section that directly addressed the challenges resulting from the disharmony of an agency-by-agency approach to regulating cybersecurity in federal acquisitions:

> The variations in these statutes, regulations, and policies create significant compliance challenges for contractors doing business with the Government across the spectrum of federal agencies. As a core goal of establishing an information security framework for federal acquisitions, the Government should use this opportunity to provide more consistency and uniformity when applying such requirements and standards.[20]

The current acquisition approach – the agency-by-agency patchwork – lacks harmony and consistency. Not only do the cyber acquisition rules and approaches vary from agency to agency, but even the requirements within some agencies cannot be squared with other requirements.

Nor is the current cyber acquisition approach transparent. Many of the agency cyber acquisition regulations simply incorporate by reference a host of internal agency security policies. In most cases, these incorporated-by-reference internal policies then sweep in a second tier of internal agency policies that can only be found through hit-or-miss internet searches that may or may not turn up the current internal procedure. Unlike the acquisition regulations, these internal agency policies do not show any evidence of being published in accordance with the Administrative Procedures Act (APA) and other requirements for public notice and comment.

Nor is the current cyber acquisition approach consistent with the existing federal cybersecurity law under FISMA and its incorporated standards.[21] In the DoD/GSA Final Cybersecurity Report, both DoD and GSA acknowledge that "Federal agencies are required to use standards and guidelines that are developed and implemented through NIST."[22] However, a number of the agency regulations either fail to tie their security standards to NIST or only do so

---

[20] ABA Public Contract Law Section letter responding to GSA/DoD Request for Information (RFI) issued by the Joint Working Group on Improving Cybersecurity and Resilience through Acquisition (Notice-OERR-2013-01; 78 Fed. Reg. 27966) (May 13, 2013)) (http://www.americanbar.org/content/dam/aba/administrative/public_contract_law/Comments_on_Notice_OERR-2013-01.authcheckdam.pdf).

[21] FISMA expressly requires agencies to "ensure compliance . . . with policies and procedures as may be prescribed by the [OMB] Director, and information security standards promulgated under section 11331 of title 40." 44 U.S.C. § 3544(b)(2)(D). The referenced statute makes National Institute of Standards and Technology (NIST) security standards mandatory. 40 U.S.C. § 11331(b)(1)(C) (making NIST information security standards "compulsory and binding").

[22] DoD/GSA Final Cybersecurity Report, p. 8 (Nov. 2013).

in an occasional way. As a general rule, the agency-by-agency cyber rules do not appear to be reconciled with fundamental requirements under FISMA, OMB, and NIST standards for security safeguards based upon risk-based and cost-effective methods for securing federal networks and information.

A. Lack of Harmony and Consistency in Agency Cyber Regulations

Given the multiplicity of agency-level cyber acquisition regulations, this analysis does not attempt to address them all. However, a number of examples illustrate the many variances in approach taken by different agencies in imposing cyber acquisition requirements upon federal contractors.

1. Overview of Major Cyber Regulations at the Agency Level

Focusing solely upon the published acquisition regulations, only one common denominator appears to connect them – nearly all of these regulations incorporate internal agency policies by reference. A comparison of the larger acquisition agencies reflects the following variations in their contract provisions published in their acquisition regulations (versus in their internal policies).

Security Provision	**DoD § 239.7102[23]**	**GSA § 552.239-71**	**DHS § 3052.204-70**	**NASA § 1852.204-76**
Reference to Internal Policy	Yes (DoD Directive)	Yes (CIO IT Guide)	Yes (DHS 4300A)	Yes (CIO list)
Reference to NIST Standard	No[24]	Yes (800-116 & 37)	No ("Federal policies")	No ("FISMA")
Security Plan or Procedure	No (see Directive)	Yes	Yes	Yes
Security Controls	No (see Directive)	Some Controls (not NIST)	Some Controls (not NIST)	Some Controls (not NIST)
Security Audit & Access	No (see Directive)	Yes	Yes ("security test")	Yes
Incident Response Plan	No (see Directive)	No	No	No
Security Training	Yes (§ 252.239-7001)	No	No	Yes (NASA policy)

[23] The DFARS does have a narrow regulation for unclassified controlled technical information that does address NIST. DFARS § 252.204-7012. However, this regulation does not cover the broader class of DoD networks and data addressed by DFARS § 239.7102.

[24] DoD has recently issued DoD Instructions (8500.2 and 8510.01) that incorporate NIST standards. However, the DFARS does not currently incorporate these Instructions.

2. DoD Cyber Acquisition Regulations

With the exception of unclassified controlled technical information, DoD relies primarily upon internal DoD instructions and policies to regulate cybersecurity. The transparency issues with unpublished internal agency guidance are discussed in greater detail in Section B below. In addition to these transparency issues, questions about harmonization also exist in the DoD cyber acquisition rules.

Inconsistency Between Regulation and Policy. The DoD acquisition regulation for "Security and Privacy for Computer Systems" incorporates the following requirement:

> Agencies shall ensure that information assurance is provided for information technology in accordance with current policies, procedures, and statutes, to include –
>
> (1) The National Security Act;
>
> (2) The Clinger-Cohen Act;
>
> (3) National Security Telecommunications and Information Systems Security Policy No. 11;
>
> (4) Federal Information Processing Standards;
>
> (5) DoD Directive 8500.1, Information Assurance;
>
> (6) DoD Instruction 8500.2, Information Assurance Implementation;
>
> (7) DoD Directive 8570.01, Information Assurance Training, Certification, and Workforce Management; and
>
> (8) DoD Manual 8570.01-M, Information Assurance Workforce Improvement Program.[25]

However, the primary references defining specific security controls and requirements (DoD Directive 8500.1 and DoD Instruction 8500.2) have been cancelled and superseded by DoD Instruction 8500.01 and DoD Instruction 8510.01 issued in March 2014. As a result, the DoD published acquisition regulation is now inconsistent with current DoD internal policy.

Inconsistent Data Breach Notification Requirements. For defense contractors, the DoD public laws, regulations, and internal policies impose a variety of different requirements for data breach notification, depending upon what type of data the contractor held or whether the data was compromised during the breach.

---

[25] DFARS § 239.7102-1(a).

- Cleared Defense Contractors. In the event of a "successful penetration" of a cleared defense contractor's network, that contractor must "rapidly report" the event to DoD, including the "technique or method used," a "sample of the malicious software," and a summary of DoD information on the system.[26]

- Technical Information. For unclassified controlled technical information, a defense contractor has 72 hours to report a "cyber incident involving possible exfiltration, manipulation, or other loss or compromise" of such data and to provide 13 categories of information to DoD regarding this incident.[27]

- Cloud Service Providers. For commercial cloud service providers, DoD has issued a policy memorandum requiring such contractors to report a "data breach" within 60 minutes.[28]

As a result, a DoD cloud service provider with a security clearance and DoD technical information could face three different reporting requirements – "rapid reporting" (still not defined in the regulations), 72-hour notice, and 1-hour notice – for the same security breach. Harmonization of DoD notice requirements would assist DoD contractors in determining what, when, and how notice should be provided to DoD in the event of a data breach involving DoD networks or information.

3. GSA Acquisition Regulations

The GSA acquisition regulations (exclusive of the internal policies) contain more detail than their DoD counterparts, but still reflect a number of anomalies.

Limited NIST References. In its final report in response to the Cybersecurity Executive Order, GSA acknowledged that "Federal agencies are required to use standards and guidelines that are developed and implemented through NIST."[29] The GSA acquisition regulations do refer to two NIST standards regarding personnel credentials (NIST Special Publication (SP) 800-116) and security authorization and risk assessments (NIST SP 800-37, Rev. 1). But conspicuous by

---

[26] 2013 National Defense Authorization Act, Pub. L. No. 112-239, Div. A, Title IX, Subtitle D, § 941, 126 Stat. 1889. While this requirement applies to "cleared defense contractors," it remains unresolved whether the notification requirement applies to both cleared and uncleared networks – or only classified networks.

[27] DFARS § 252.204-7012(d).

[28] DoD Chief Information Officer (CIO) Memorandum re Supplemental Guidance for the Department of Defense's Acquisition and Secure Use of Commercial Cloud Services (Dec. 16, 2013).

[29] DoD/GSA Final Cybersecurity Report, p. 8 (Nov. 2013).

their absence are other NIST standards for which the GSA regulation covers the subject matter (but does mention NIST) or omits both the subject matter and the NIST standards.[30]

- NIST Controls. The GSA regulations include certain security controls (*e.g.*, security plan, access controls, and audit), but do not mention the controlling NIST standards, such as NIST SP 800-53, Rev. 4.

- Continuous Monitoring. The regulations incorporate a continuous monitoring requirement and NIST SP 800-37, Rev. 1, but do not refer to the more current NIST standard (NIST SP 800-137) specifically addressing continuous monitoring for federal agencies.

- Incident Response. The regulations do not mention incident response requirements nor the applicable NIST standards (*e.g.*, NIST 800-61, Rev. 1 or NIST 800-53, Rev. 4).

Missing Cross-References. The GSA regulations incorporate an internal information security policy ("CIO IT Security Procedural Guide 09-48") and refer to an internet link for the guide: http://www.gsa.gov/portal/category/25690.[31] However, the referenced link takes the reader to a web page without the CIO IT Security Procedural Guide 09-48. Drilling down another layer, this Guide 09-48 still does not appear (http://www.gsa.gov/portal/content/104257) at the next level. While the Guide can eventually be found via an internet search, the GSAM cross references do not provide the expected link – or transparency – regarding this internal policy.

Audit Access. Imposing one of the most robust government audit access clauses, the GSA regulation requires that the contractor provide GSA with virtually open-ended access to the contractor's facilities, installations, operations, documentation, databases, IT systems and devices and personnel used in performance of the contract, regardless of the location."[32] However, many of GSA's procurements involve commercial products and services. The FAR imposes strict limits upon what contract terms and requirements may be imposed upon commercial item contractors.

- Commercial Terms. For commercial items, the terms and conditions are generally limited to a short list of clauses that best conform to commercial practices and limit the burdens that discourage commercial contractors from the federal marketplace.[33]

---

30 General Services Administration Acquisition Manual (GSAM) § 552.239-71.

31 GSAM § 552.239-71(b).

32 GSAM § 552.239-71(k).

33 FAR § 12.302(b) and 52.212-4.

- Commercial Practices. The FAR generally restricts commercial item clauses to those that are "[**d]etermined to be consistent with customary commercial practice**."[34]

- Order of Precedence. In the event of any conflict between the regulatory requirements for federal contracts generally and commercial item acquisitions specifically, the commercial item regulations "shall take precedence for the acquisition of commercial items."[35]

The GSA regulations leave an open question about whether the regulatory clause for cybersecurity audits reflects "customary commercial practice" in the commercial IT industry. If not, then the GSA regulation needs to be harmonized with the commercial item requirements that take precedence of the GSA audit clause.

4. Homeland Security Acquisition Regulations

The Homeland Security Acquisition Regulations (HSAR) include brief treatment of information security, but reserve most of the security guidance for an internal Department of Homeland Security (DHS) policy (DHS Sensitive System Policy Publication 4300A). Comparing only the regulations (exclusive of the internal policies), DHS offers more guidance in its regulations than some, but less than others (*e.g.*, GSA or HHS regulations).

NIST Standards. The DHS regulations include general references to security controls (*e.g.*, security plan, security test and evaluation, and continuity of operations plan), but no specific reference to NIST standards, such as NIST SP 800-53, Rev. 4 ("Security and Privacy Controls").[36]

Personnel Access. The DHS regulations generally limit personnel access to federal IT systems to U.S. citizens.[37] This provision does not appear to be harmonized with the recommendations made in the DoD/GSA Final Report issued in response to the Cybersecurity Executive Order:

> In general, implementation must be harmonized with, and be built upon as appropriate, existing **international** and consensus based standards, as well as statutes and regulations applicable to this

---

34 FAR 12.301(a) (emphasis added); *see also* Federal Acquisition Streamlining Act of 1994, Pub. L. No. 103-355, § 8002, *reprinted in* 1994 U.S.C.C.A.N. 3386 (same).

35 FAR § 12.102(c).

36 HSAR § 3052.204-70.

37 HSAR § 3052.204-71(k), Alternate I.

> field, including the Federal Information Security Management Act of 2002 (FISMA) . . . .[38]

Whether international standards generally impose nationality standards is not addressed by the DHS regulations. Nor is it clear that this "U.S. only" limitation can be harmonized with competitive requirements to avoid unduly restrictive specifications or to comply with international free-trade obligations and agreements.[39] At a minimum, the Cybersecurity Executive Order's objective for harmonized cyber acquisition regulations would presumably encompass their harmony and consistency with statutory competition mandates and international free-trade obligations.

* * *

Quite simply, the cyber acquisition regulations have yet to be harmonized. Given that FISMA, OMB, and NIST cybersecurity standards admittedly apply to federal networks and information (other than national security systems), the Cybersecurity Executive Order's objective "to harmonize and make consistent existing procurement requirements related to cybersecurity" could be substantially achieved simply by applying these standards in the FAR. This approach would provide greater uniformity in a single regulation. Even better, FAR coverage would substantially obviate the need for each agency to create its own unique set of regulations. The agency-by-agency regulatory regime seems particularly unnecessary where FISMA, OMB and NIST already establish mandatory security standards common to all federal agencies, networks, and systems (other than national security systems).

B. Lack of Transparency in Agency Cyber Acquisition Rules

Transparency represents a fundamental principle underpinning the law governing both federal information policy and acquisition regulations. Some federal rules governing cyber acquisition requirements meet these standards. But nearly all federal agencies have incorporated internal agency policies by reference, imposing these internal policies upon the private sector without documenting compliance with the federal transparency laws mandating public notice and comment. Without the transparency benefits of published regulations built upon public notice and comment, both federal agencies and contractors face serious challenges:

- Unenforceability. Federal agencies may be unable to enforce cybersecurity requirements that hinge upon internal agency policies because federal courts may find such policies invalid and unenforceable.

---

[38] DoD/GSA Final Cybersecurity Report, p. 8 (Nov. 2013).

[39] *See* Competition in Contracting Act, 10 U.S.C. § 2305(a)(1)(C) (requiring contract requirements to be support "full and open competition"); FAR § 11.002(a) (same); *Technosource Information Sys., LLC; TrueTandem, LLC,* B-405296 *et al.*, Oct. 17, 2011, 2011 CPD ¶ 220 at 4 (agency agreed to international data center locations due to U.S. Trade Representative's advice that "a U.S. data center limitation impermissibly restricted free trade").

- Compliance Burdens. Public-sector contractors face significant compliance burdens of finding, tracking, and implementing a multitude of internal agency policies that can change without notice, thus increasing the risk of noncompliance.

- Best Security Practices. Agencies imposing internal policies may miss the opportunities to gain valuable public input from security experts, standards-setting organizations, and the private sector that would enhance the resulting security rules and better tailor them to current best practices.

1. Agency Incorporation of Internal Policies

For cyber acquisition requirements, federal agencies impose internal security policies upon contractors in two ways. First, the agency cyber acquisition regulations typically incorporate an internal agency policy by reference. Second, many of the incorporated internal policies then, in turn, incorporate second-tier internal policies by reference, thus pyramiding the burden of finding, reviewing, and complying with these multi-tiered requirements pushed down by policies-within-policies.

The table below represents only a subset of the agency internal policies regarding cybersecurity. First, the table only includes some of the larger acquisition agencies that have regulations specific to cybersecurity. Second, for that subset of federal agencies, the table covers only the internal policies expressly incorporated into the agency's acquisition regulation (not the second-tier policies incorporated by reference in the first-tier policies). Even with these limitations, the table illustrates the basic fact that federal agencies have chosen to regulate cybersecurity requirements primarily by imposition of internal agency policies, rather than published agency regulations.

Federal Agency	Agency Acquisition Regulation	Internal Agency Policy Incorporated by Reference
DoD	DFARS § 239.7102-1	DoD Directive 8500.1; DoD Instruction 8500.2;[40] DoD Manual 8570.01-M
GSA	GSAM § 552.239-71	CIO IT Security Procedural Guide 09-48 (17 pages)
DHS	HSAR § 3052.204-70	DHS Sensitive System Policy Publication 4300A (133 pages)
NASA	NASA FARS § 1852.204-76	Applicable Documents List (ADL) http://ww.nasa.gov/offices/ocio/security/index.html
HHS	HHS FARS § 352.239-72	HHS Information Security Program Policy (8 HHS IT security and privacy policies listed)[41]
State	DOSAR § 652.239-71	Foreign Affairs Manual (FAM) and Foreign Affairs Handbook (FAH) excerpts (not currently available)[42]
Commerce	DOC FARS § 1352.239-72	DOC Information Technology Management Handbook (not currently available)[43]
Transportation	DOT FARS § 1252.239-70	Departmental Information Resource Management Manual (DIRMM) and associated guidelines

As reflected above, the referenced agency policies present a host of compliance difficulties: (1) some have been superseded (*e.g.*, DoD); (2) others are voluminous (*e.g.*, the DHS policy spanning 133 pages); (3) several policies cannot be readily located from the information in the agency regulation (State, Commerce, and Transportation); and (4) at least one is ambiguous about which policy applies (HHS). Such disconnects are generally inconsistent with the fundamental purpose of a contractual relationship – to tell each party who bears what specific obligations.

The NASA acquisition regulation illustrates multiple problems. The primary contract clause states that "Applicable requirements, regulations, policies, and guidelines are identified in the Applicable Documents List . . . ."[44] However, the referenced website takes the reader to a list

---

[40] DoD Directive 8500.1 and DoD Instruction 8500.2 have been cancelled and superseded by DoD Instruction 8500.01 (59 pages) and DoD Instruction 8510.01 (47 pages) issued in March 2014. The DFARS has not yet been updated to incorporate the latter two instructions.

[41] The HHS acquisition regulation is not specific about which internal policy applies. If it refers to HHS-OCIO-2011-0003, that policy is 71 pages long.

[42] The State Department acquisition regulation provides an internet link to the FAM and FAH (http://foia.state.gov/Regs/Search.asp), but a search produced a "Page Not Found" response.

[43] The Commerce Department acquisition regulation refers to the OCIO website, but a search produced an "Error" notice.

[44] NASA Acquisition Regulation § 1852.204-76(b) citing to the NASA Chief Information Officer (CIO) website (http://www.nasa.gov/offices/ocio/itsecurity/index.html).

of 56 separate directives, technical requirements, handbooks, and standards. Once on this website, the public does not know which of these many NASA policies actually govern security requirements for NASA acquisitions. Nor can the public access these internal policies without making a specific request for them from a NASA employee:

> For IT Security related documents (*e.g.*, IT Security Handbooks, Standards, Memoranda, and Archived Documents), contact Mr. Howard Whyte to request a copy.[45]

These transparency problems multiply when the referenced agency policies, in turn, incorporate even more second-tier security policies by reference. For example, the internal policy referenced in the GSA regulation spans 17 pages (exclusive of Appendix), but it then imposes 9 additional internal policies not mentioned in the text of the acquisition regulation itself:[46]

> All GSA contractors must comply with the GSA policies below (these documents are all referenced within the GSA IT Security Policy).
> - GSA Information Technology (IT) Security Policy, CIO P 2100.1E.
> - GSA Order CIO P 2181.1 "GSA HSPD-12 Personal Identity Verification and Credentialing Handbook", dated October 20, 2008.
> - GSA Order CIO 2104.1, "GSA Information Technology (IT) General Rules of Behavior", dated July 3, 2003.
> - GSA Order CPO 1878.1, "GSA Privacy Act Program", dated October 27, 2003.
> - GSA IT Security Procedural Guide 04-26, "FISMA Implementation"."
> - GSA IT Security Procedural Guide 06-29, "Contingency Plan Testing"."
> - GSA IT Security Procedural Guide 06-30, "Managing Enterprise Risk."
> - GSA IT Security Procedural Guide 08-39, "FY 2009 IT Security Program Management Implementation Plan."
> - GSA IT Security Procedural Guide 09-44, "Plan of Action and Milestones (POA&M)."

Thus, a contractor must find each second-tier policy, compare the requirements against the contractor's existing security baseline, and assure compliance with ten different sets of security requirements – none of which appear to be published in the Federal Register or otherwise conform to statutory requirements for public notice and comment.

2. Federal Laws Mandating Transparency

Statutes governing federal administrative, acquisition, and security law generally favor transparency.

Administrative Law. The Administrative Procedures Act (APA) contains an explicit requirement for federal agencies to publish specific guidance in the Federal Register:

---

[45] NASO CIO website (http://www.nasa.gov/offices/ocio/itsecurity/index.html).

[46] GSA Security Language for IT Acquisition Efforts: CIO-IT Security-09-48 (9/10/09) (http://www.gsa.gov/graphics/pbs/CIO_Policy.pdf).

> (1) Each agency shall separately state and currently publish in the Federal Register for the guidance of the public –
>
> * * *
>
> (D) substantive rules of general applicability adopted as authorized by law, and statements of general policy or interpretations of general applicability formulated and adopted by the agency; . . . .[47]

By imposing internal security policies upon public-sector contractors, federal agencies would be hard-pressed to argue that such requirements represented mere housekeeping guidelines, rather than "substantive rules of general applicability" or "statements of general policy." Without proof of publication of such rules in the Federal Register, such agencies cannot demonstrate compliance with the APA's mandate for public notice and transparency.

Acquisition Law. In addition to the APA, federal acquisition law mandates Federal Register publication before procurement policies, regulations, or procedures take effect:

> (1) Required comment period.— Except as provided in subsection (d), a **procurement policy**, regulation, **procedure**, or form (including an amendment or modification thereto) may not take effect until 60 days after it is published for public comment in the Federal Register pursuant to subsection (b) if it—
>
> (A) relates to the expenditure of appropriated funds; and
>
> (B) (i) has a significant effect beyond the internal operating procedures of the agency issuing the policy, regulation, procedure, or form; or
>
> (ii) has a significant cost or administrative impact on contractors or offerors.
>
> (2) Exception.— A policy, regulation, procedure, or form may take effect earlier than 60 days after the publication date when there are compelling circumstances for the earlier effective date, but the effective date may not be less than 30 days after the publication date.[48]

---

47 5 U.S.C. § 552(a)(1)(D).

48 41 U.S.C. § 1707(a) (emphasis added); *see also* FAR § 1.301 (generally requiring publication of acquisition regulations in the Federal Register).

The agency policies discussed above readily fall within the scope of this statute. For example, the GSA policy incorporated by reference in its acquisition regulation plainly qualifies as a "procurement policy" when it states that "[a]ll GSA contractors must comply with the GSA policies below [listing 9 specific policies]."[49] Without publication in the Federal Register, such procurement policies would fail to comply with the governing statute and regulation.

Federal Information Law. Transparency also stands as a core principle in federal statutes governing information law. One of the express statutory purposes under FISMA is to: "(4) improve the quality and use of Federal information to strengthen decision-making, accountability, and **openness in Government and society.**"[50] Similarly, the e-Government Act of 2002 sets forth multiple legislative objectives for transparency, including assuring "citizen-centric Government information," promoting "access to high quality Government information," and making "the **Federal Government more transparent** and accountable."[51] Finally, a number of the agency cyber regulations and policies cite OMB Circular A-130, but this same Circular also emphasizes the importance of transparency:

> Because the public disclosure of government information is essential to the operation of a democracy, the management of Federal information resources should **protect the public's right of access to government information**.[52]

Invalidity of Unpublished Procurement Rules. When federal agencies violate federal transparency requirements for public notice and comment, the courts may refuse to enforce the agency rules and procedures. In rejecting an agency's attempt to impose an internal operating procedure upon a contractor, the Federal Circuit held that procedure to be unlawful:

> The Supreme Court has emphasized that it will not condone the Government's use of unpublished regulations to affect adversely the substantive rights of individuals. *Morton v. Ruiz,* 415 U.S. 199, 94 S.Ct. 1055, 39 L.Ed 2d 270 (1974); *accord Alaniz v. Office of Personnel Management,* 728 F.2d 1460, 1470 (Fed. Cir. 1984) ("agency actions effected in violation of the notice and comment procedures are void"). Explaining the policy behind § 552, the Court stated, "The [APA] was adopted to provide, *inter alia,* that administrative policies affecting individual rights and obligations be promulgated pursuant to certain stated procedures so as to avoid the inherently arbitrary nature of unpublished *ad hoc*

---

49 GSA Security Language for IT Acquisition Efforts: CIO-IT Security-09-48, p. 6, § 1.1 (Sept. 10, 2009) (http://www.gsa.gov/graphics/pbs/CIO_Policy.pdf).

50 44 U.S.C. § 3501(b) (emphasis added).

51 Pub. L. No. 107-374, § 2, 116 Stat. 2900 (2002) (emphasis added).

52 OMB Circular No. A-130, § 7(f) (emphasis added); *see also id.*, § 7 ("The free flow of information between the government and the public is essential to a democratic society").

> determinations." *Morton* at 232, 94 S.Ct. at 1073 (citations omitted).[53]

In short, multiple federal statutes require transparency. Failure to comply may invalidate an agency's attempt to enforce unpublished rules and policies, thus undermining the very purpose for imposing security requirements in the first place. For these reasons, both federal agencies and contractors would benefit from a movement away from unpublished internal policies in favor of published acquisition regulations that establish legally enforceable ground rules for accessing federal networks and information.

C. Lack of Harmony Between Security Standards and Agency Cyber Rules

Rather than establishing a common baseline of cyber acquisition rules consistent with the FAR's objective of "uniform policies and procedures," the agency-level regulations have resulted in a diversity of cyber rules and approaches. This diversity cuts against basic security requirements and policies governing federal procurements.

- Risk Assessments. As an initial step in determining appropriate security safeguards, a federal agency must perform a security risk assessment – but the wide variation in agency-level cyber rules raises questions about which rules have been supported by weighing risks relating to the nature of the data, threats, and applicable laws.

- Cost-Effectiveness. Federal security law incorporates a cost-effectiveness standard, but the lack of uniformity and ready availability of agency-level security standards compound compliance burdens, thus making any given level of security more burdensome and expensive.

- Federal Harmonization. Both the Cybersecurity Executive Order and the FAR recognize the value of harmony and uniformity in acquisition rules, but the current diversity and diffusion of agency-level cyber rules fall short of these objectives.

By harmonizing federal cyber acquisition requirements, the Government could best serve all of these objectives: (1) targeting security safeguards to the highest-priority data and threats; (2) achieving more security bang-for-buck by reducing compliance burdens and refocusing agency and contractor resources on high-payoff security measures; and (3) improving security by selecting best practices from current agency-level regulations and policies and harmonizing them in a published and unified FAR regulation built upon the best ideas collected through public review and comment.

---

53 *NI Indus., Inc. v. United States*, 841 F.2d 1104, 1107 (Fed. Cir. 1988).

1. The Requirement for Risk-Based Security Safeguards

Like nearly every other information security standard, federal cybersecurity law, standards, and policy require that security programs be built upon risk assessments that weigh the nature of the data, threats, and applicable rules of behavior. For example, FISMA establishes a series of mandatory ("shall") requirements for federal agencies and contractors, including a duty to weigh and assess risks to networks and information:

> The head of each agency shall – . . .
>
> (1) be responsible for—
>
> (A) providing **information security protections commensurate with the risk and magnitude of the harm** resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of [federal information or information systems];
>
> * * *
>
> (2) ensure that senior agency officials provide information security for the information and information systems that support the operations and assets under their control, including through—
>
> (A) **assessing the risk and magnitude of the harm** that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of such information or information systems; . . . .[54]

While the agency-level cyber regulations and policies vary considerably, they do not link these variations to differences in risks between the agencies. Specifically, why does one agency levy one set of security protocols, while another agency employs a much different set of such protocols? While different risks could potentially justify different security protocols for each agency, neither the agency regulations nor policies suggest that such differences account for the type and magnitude of the current agency-level regulatory variations.

In summary, federal agencies should tailor their security requirements based upon their specific risk profiles and assessments. However, if each agency cannot link its unique security protocols to differences resulting from that agency's own assessment of different risks justifying different security rules, such variations would appear to be out-of-step with the risk-based approach mandated by FISMA and its implementing OMB and NIST standards.

---

[54] 44 U.S.C. § 3544(a) (emphasis added); *see also* Federal Acquisition Circular (FAC) 2005-06, 70 Fed. Reg. 57450-51 (2005) ("information security protections" must be "commensurate with security risks").

2. The Requirement for Cost-Effectiveness in Security

FISMA requires adequate security, rather than security at any cost. In particular, FISMA establishes a "cost-effectiveness" standard for federal information security, requiring federal agencies to implement security "**policies and procedures to cost-effectively reduce risks** to an acceptable level."[55] The NIST standards confirm cost-effectiveness as an integral part of the security program.[56]

The current agency-by-agency regulatory approach to cyber acquisition rules cuts against cost-effective safeguarding of federal networks and information.

- Regulatory Multiplicity. Under virtually any scenario, complying with a dozen different regulatory schemes will impose greater compliance burdens than a single set of regulations reflecting a harmonized federal acquisition approach to cybersecurity.

- Policy Proliferation. Searching dozens of agency cyber policies, performing dozens of gap analyses, and tracking periodic policy changes inevitably diverts cybersecurity dollars away from updating cyber safeguards to meet the latest threats.

- Submerged Policies. For agency policies not referenced in agency regulations or readily available on agency websites, contractors incur costs simply due to the time spent searching for the policies and verifying that they reflect the agency's latest requirements.

For agency-level cyber regulations and policies, more is actually less. More agency regulations and policies mean more agency resources devoted to regulatory upkeep – and less to sharpening and updating cyber defenses against the latest threats. For contractors, the diffusion and diversity of agency-level cyber rules force contractors to devote more resources to identifying variations between agency cyber rules, adapting corporate compliance to multiple agency requirements, and tracking any updates across all agencies.

In response to a Request for Information (RFI) from DoD and GSA triggered by the Cybersecurity Executive Order, the ABA's Public Contract Law (PCL) Section submitted comments underscoring the impact of the current agency-by-agency approach to cyber regulation and the need for greater harmonization:

> The variations in these statutes, regulations, and policies create significant compliance challenges for contractors doing business with the Government across the spectrum of federal agencies. As a

---

55 44 U.S.C. § 3544(a)(2)(C) (emphasis added).

56 *See, e.g.,* NIST Special Publication (SP) 800-37, Rev. 1, at 2 ("cost effective, risk-based decisions").

> core goal of establishing an information security framework for federal acquisitions, the Government should use this opportunity to provide more consistency and uniformity when applying such requirements and standards.[57]

Whether characterized as cost-effectiveness or bang-for-buck, federal agencies must adhere to FISMA's mandate to deploy "policies and procedures to **cost-effectively** reduce risks to an acceptable level."[58] Harmonized cyber acquisition regulations serve this mandate. With harmonized regulations, federal agencies and contractors can focus cyber resources on the security practices with the highest payoff, while saving dollars now spent on complying with the diverse and diffuse agency-level approach to regulating cybersecurity.

3. The Federal Policy for Harmonization

Different agencies have different missions and needs. However, the current federal framework (FISMA/OMB/NIST) builds in the flexibility for agencies to conduct their own assessments of threats and risks, select the security controls and practices that best counter these risks, and adapt to the changing threat environment based upon continuous monitoring. Indeed, agencies do not need their own individual cyber acquisition rules to use this approach because both statute and regulation require federal agencies to follow it.[59] As reflected in the recent report, "Federal agencies are required to use standards and guidelines that are developed and implemented through NIST."[60]

Given that federal agencies must follow the same security standards and guidelines, harmonization of cyber acquisition regulations makes sense. Such harmonization is also consistent with the FAR's core purpose to provide "uniform policies and procedures for acquisition by all executive agencies."[61] Finally, harmonization is consistent with the Cybersecurity Executive Order's directive that federal regulators "address what steps can be

---

57 ABA PCL Section letter to GSA re Notice-OERR-2013-01 (June 12, 2013) (http://www.americanbar.org/content/dam/aba/administrative/public_contract_law/Comments_on_Notice_OERR-2013-01.authcheckdam.pdf).

58 44 U.S.C. § 3544(a)(2)(C) (emphasis added).

59 *See, e.g.,* 44 U.S.C. § 3544(b)(2)(D) (requiring agency compliance with OMB guidance); 40 U.S.C. § 11331(b)(1)(C) (making NIST standards "compulsory and binding" for federal agencies); FAR § 7.103(w) (requiring compliance with OMB Circular A-130 and NIST guidance and standards).

60 DoD/GSA Final Cybersecurity Report, p. 8 (Nov. 2013).

61 FAR § 1.101; *see also* FAR § 1.302 (limiting agency-level regulations to those necessary to implement FAR policies and satisfy "specific needs of the agency").

taken to harmonize and make consistent existing procurement requirements related to cybersecurity."[62]

Harmonization serves yet another fundamental purpose – better cybersecurity. In their final report, DoD and GSA acknowledged the value of harmonization:

> In general, implementation must be harmonized with, and be built upon as appropriate, existing international and consensus based standards, as well as statutes and regulations applicable to this field [citing FISMA and other federal statutes]
>
> * * *
>
> While it is not the primary goal, implementing these recommendations may contribute to **increases in cybersecurity across the broader economy**, particularly if changes to Federal acquisition practices are adopted consistently across the government and concurrently with other actions to implement the Cybersecurity Framework.[63]

Federal harmonization would lead to such "increases in cybersecurity" for a host of reasons.

- Federal Best Practices. The harmonization process would drive federal agencies to focus upon the security practices with the highest payoff and greatest effectiveness.

- Public Input. Federal transparency requirements would infuse input from standards-setting organizations, security experts, and the private sector, thus reinforcing the selection of best practices conforming to "existing international and consensus based standards."[64]

- Improved Compliance. Without dozens of agency-level regulations and policies, the private sector can perform more cost-effective gap analyses, understand the federal cyber requirements better, and train more effectively to unified standards rather than the multitude of agency-level rules.

---

62 Exec. Order No. 13636, 78 Fed. Reg. 11739, 11742 (Feb. 19, 2013).

63 DoD/GSA Final Cybersecurity Report, p. 9 (Nov. 2013) (emphasis added); *see also id.*, p. 13 (increased "consistency with which it applies standards to requirements in its contracts" will increase value to Government).

64 DoD/GSA Final Cybersecurity Report, p. 9 (Nov. 2013).

V. Conclusion

The Cybersecurity Executive Order has opened an opportunity for federal regulators to address "what steps can be taken to harmonize and make consistent existing procurement requirements related to cybersecurity." Such harmonization serves multiple federal and private sector interests: better cybersecurity, enhanced cost-effectiveness, greater transparency, and improved uniformity and compliance.

Given that the federal government represents one of the largest IT buyers and greatest users of networks and data in the world, harmonization of the federal acquisition process holds the prospect of delivering a substantial payoff – and thus deserves attention from both the public and private sectors.

David Z. Bodenheimer
Crowell & Moring LLP

DCACTIVE-28834456.2