Bloomberg BNA

Privacy and Security Law Report®

Federal Contracting Security

It's not just DOD contractors that must pay attention to cybersecurity issues as civilian U.S. agencies should move towards requiring assurance that sensitive federal information will be protected against loss or compromise when shared with contractors who sell through General Services Administration contracts, the author writes.

Improving Cyber and Supply Chain Security in GSA Schedule Contracting

BY ROBERT S. METZGER

The federal government purchases more than $30 billion of goods and services annually through various General Services Administration (GSA) Multiple Award Schedule (MAS) contracts. Today, when federal agencies purchase information and communication technology (ICT) using GSA contracting vehicles, there are no generally applicable requirements to protect against cyber or supply chain threats. This will change–and should. Federal agencies, including the Department of Defense, use GSA contract vehicles to acquire information systems, solutions, hardware, and software. Federal agencies need assurance that sensitive federal information will be protected against loss or compromise when shared with contractors who sell through GSA vehicles. Similarly, GSA needs to minimize exposure to counterfeit or corrupted hardware when purchased through its contracts.

Cybersecurity and supply chain security are related, but distinct. In the contemporary threat environment, both are crucial national objectives. As used here, the objective of cybersecurity is the *protection of information* and *information systems* against attacks which have their principal purpose the unauthorized extraction (theft) of sensitive and valuable federal information. Representative cyberattacks may be executed against vulnerable networks, weaknesses in information systems, or through manipulation of connected devices. Supply chain security, among other purposes, seeks to assure the integrity and functionality of hardware. Counterfeit electronic parts are among the threats addressed by supply chain security, because they can cause electronic equipment to experience premature failure or degraded performance. Active electronic parts also are exposed to an emerging threat of tainted or maliciously encoded control software, which can create or exploit cyber vulnerability as well as damage the physical operations of affected systems.

This article finds that the national interest dictates that GSA adopt new measures to better protect against both cyber and supply chain threats to information technology equipment and services that are purchased through its MAS vehicles. These threats endanger the ability of federal agencies to perform their missions, expose sensitive federal and contractor information to unauthorized exfiltration or other compromise, and could impair the reliability of electronic systems that are es-

Robert S. Metzger is a shareholder and heads the Washington office of Rogers Joseph O'Donnell PC. This article presents his individual views and should not be attributed to any client of the firm or to any organization with which Metzger is or may be affiliated.
He acknowledges with appreciation the insight of several reviewers of the draft of this article, including his law firm colleague, Brian D. Miller, who served as Inspector General of the GSA from 2005-2014.

sential to the functioning of both civil and defense functions of government. Addressing these threats by changes to MAS contracting practices will be daunting. But strategies and methods can be identified and must be pursued. GSA can add baseline cyber and supply chain security requirements to master Schedule contracts. It also can establish a range of new, standardized contract terms, to add to its procurement regulations and for reference in Schedule contracts. These would be optional at the Schedule Contract level but available for agencies to use to adjust or add security at the Task or Delivery Order level. GSA can isolate certain supplies or services, where risk is greatest, into new Schedules and SINs that are subject to elevated security requirements. At the same time, GSA will have to weigh its actions carefully and seek input from the large and diverse base of commercial companies who hold Schedule contracts. GSA should refrain from imposing unnecessary obligations that add expense or unduly restrict competition.

Many Cyber and Supply Chain Security Initiatives

There are multiple, concurrent initiatives underway to better protect federal information and information systems against both cybersecurity and supply chain threats. These have been accelerated as agencies react to the Office of Personnel Management (OPM) cyber breach and similar events. By and large, GSA has been outside the recent initiatives.

■ The National Archives and Records Administration (NARA) is nearing completion of a new federal regulation that will govern all forms of ''controlled unclassified information'' (CUI).[1] The NARA rule will distill more than 100 types of sensitive but unclassified federal information into 23 categories and 82 subcategories of CUI. It will apply across all federal agencies, provide rules on designation and marking of controlled information, and guide agencies on public access rights and on allowable dissemination. The NARA rule also will establish baseline measures for both physical and electronic safeguarding of CUI.

■ The National Institute of Standards and Technology (NIST) has issued a new Special Publication, NIST SP 800-171, specifically intended to inform companies who operate nonfederal information systems on how they should protect CUI.[2]

■ Through a revised Interim Rule,[3] DoD now requires its entire supply chain to protect four kinds of ''covered defense information.''[4] To protect this information on contractor systems, DoD's Interim Rule adopts the new NIST SP 800-171 standard. DoD previously acted to obligate its key contractors to adopt systems and practices to detect and avoid counterfeit electronic parts.[5] By a Proposed Rule released for comment in September, DoD now proposes to extend supply chain security measures to its entire supply chain, inclusive of small businesses and sellers of Commercial Off The Shelf (COTS) products.[6]

■ The Office of Management and Budget (OMB) in August issued draft Acquisition Guidance to provide federal agencies with guidance on implementing strengthened cybersecurity protections in Federal acquisitions for products or services that generate, collect, maintain, disseminate, store, or provide access to Controlled Unclassified Information.[7] The draft guidance would direct agencies to ''continuously review contract activities'' to address, by contract requirements, four core functions – (1) use of security controls (NIST SP 800-171) for contractors' ''internal systems used to provide a product or service'' for the Government; (2) timely contractor reporting of ''all cyber incidents involving the loss of confidentiality, integrity, or availability of data''; (3) conduct of security assessments to ''confirm that contractors are maintaining their security posture'' (among other purposes); and (4) provision of continuous monitoring of information systems.

GSA has been relatively quiet on cyber or supply chain security during the same period. Yet, GSA is very much aware of the importance of using acquisition tools to improve cybersecurity and manage supply chain risk. On February 19, 2013, President Obama issued Executive Order 13636, Section 8(e) of which directed GSA, in coordination with DHS and DoD, to make recommendations ''on the feasibility, security benefits, and relative merits of incorporating security standards into acquisition planning and contract administration.'' GSA and DoD issued a Final Report, on November 19, 2013, in which a central recommendation

---

[1] *Controlled Unclassified Information*, (Proposed Rule), 80 Fed. Reg. 26501, May 8, 2015, available at http://www.gpo.gov/fdsys/pkg/FR-2015-05-08/pdf/2015-10260.pdf.

[2] *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*, NIST Special Publication (SP) 800-171, June 2015, available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171.pdf (14 PVLR 1190, 6/29/15).

[3] *Network Penetration Reporting and Contracting for Cloud Services*, (DFARS Case 2013– D018) (Interim Rule), 80 Fed. Reg. 51739, Aug. 26, 2015, available at http://www.gpo.gov/fdsys/pkg/FR-2015-08-26/pdf/2015-20870.pdf (14 PVLR 1599, 9/7/15). The new Interim Rule revises an earlier rule, *Safeguarding Unclassified Controlled Technical Information*, (DFARS Case 2011–D039) (Interim Rule) (UCTI Rule), Nov. 18, 2013, available at www.gpo.gov/fdsys/pkg/FR-2013-11-18/pdf/2013-27313.pdf. The 2015 Interim DFARS includes the category of information previously protected, Unclassified Controlled Technical Information (UCTI), as one of the four types of ''covered defense information.'' What was ''UCTI'' now is designated as ''controlled technical information,'' namely technical information with military or space application. DFARS 204.7301 (Definitions), at 80 Fed. Reg. 51742.

[4] The four information types include ''controlled technical information'', critical information (operations security), export-controlled information and ''[a]ny other information'' that requires safeguarding or dissemination controls pursuant to ''laws, regulations, and Governmentwide policies.'' The last category anticipates the final rule on Controlled Unclassified Information. DFARS 204.7301 (Definitions), at 80 Fed. Reg. 51742.

[5] *Detection and Avoidance of Counterfeit Electronic Parts*, (DFARS Case 2012–D055) (Final Rule), 79 Fed. Reg. 26092, May 6, 2014, available at http://www.gpo.gov/fdsys/pkg/FR-2014-05-06/pdf/2014-10326.pdf.

[6] *Detection and Avoidance of Counterfeit Electronic Parts—Further Implementation*, (DFARS Case 2014–D005) (Proposed Rule), 80 Fed. Reg. 56939, Sept. 21, 2015, available at http://www.gpo.gov/fdsys/pkg/FR-2015-09-21/pdf/2015-23516.pdf.

[7] *Improving Cybersecurity Protections in Federal Acquisitions*, (draft Guidance), Office of Management and Budget, Aug. 11, 2015, available at https://policy.cio.gov/(14 PVLR 1516, 8/17/15). The final Guidance is expected soon.

  PVLR ISSN 1538-3423

was to institute baseline cybersecurity requirements ''as a condition of contract award for appropriate acquisitions.''[8]

Two years after the 8(e) Final Report, however, GSA has yet to act to impose ''baseline'' cybersecurity requirements and has not addressed risks of counterfeit electronics in its Schedule Contracts.[9] Through the MAS program that GSA administers, federal agencies purchase billions of dollars annually of IT hardware, software and services. A tension is present, however, because *agencies*, not GSA, fund the Task or Delivery Orders under those Contracts. Agencies decide how to employ equipment or utilize services, and determine what federal information to share with MAS contractors. GSA acts as both a market facilitator and a source gatekeeper. For GSA to also act as cyber or supply chain security regulator is a demanding proposition.

In the IT area, GSA's purchasing domain embraces an enormous variety of services and supplies to serve many different purposes of varying purchasers. An established basis to address cyber or supply chain **risk** is to consider threat, vulnerability and consequence.[10] A risk-based strategy, applied to the immense breadth of supplies and services acquired through GSA MAS vehicles, requires discrimination among various Federal Supply Schedules and even the Special Item Numbers (SINs) within these schedules. As a basic example, both cyber and supply chain risk differ substantially between Information Technology (Schedule 70) and Office Solutions (Schedule 75). Even within a single Schedule, such as Information Technology Schedule 70, the need for and benefit of cyber and supply chain security measures will vary according to many factors. These may include the motivation and capability of potential adversaries (the threat), the nature of equipment or service procured and its susceptibility to corruption or even subversion (vulnerability) and the impact of system or service failure upon agency mission or function (consequence). These complexities preclude ''monolithic'' solutions to improve security in GSA MAS purchases, but they do not justify complacency or deny the importance and urgency of using acquisition measures to better protect information, information systems and purchased electronic equipment.

GSA's Multiple Award Schedule (MAS) Programs

Under the MAS Programs, GSA enters into governmentwide contracts with commercial firms to provide over 11 million distinct commercial supplies and services. Agencies place Orders directly with MAS contractors. For information and communications technology needs, GSA has distinct regimes. Eligible buyers (federal agencies and other authorized buyers, such as state, local and tribal governments) can acquire many forms of information technology through Schedule 70 (Information Technology Equipment, Software and Services) of the Federal Supply Schedule (FSS). More than 5,000 companies offer IT supplies and services through Schedule 70 of the FSS. Schedule 70 is by far the largest of all the FSS categories, accounting for more than $14 billion in sales in fiscal 2014.[11] Under Schedule 70, there are SINs to buy (for example) Cloud IT Services, Computer and Networking Hardware, Cyber Security, Data Center and Storage, Software and Applications, Systems Life Cycles Integration, Telecommunications, Wireless, and Mobility Telepresence. Annual sales for all Schedule 70 SINs amount to a significant percentage of the federal IT budget.[12] The Department of Defense is among the largest purchasers of IT supplies and services from Schedule 70.

GSA also manages several Governmentwide Acquisition Contracts (GWACS), including ALLIANT, 8(a) STARS (for small businesses) and VETS (for service-disabled veteran-owned small businesses). GWACS are purpose-focused, pre-competed contracts, generally involving a small number of selected contractors.[13] Reflecting increased demand for many different forms of IT services, GSA recently released a 300-page second draft for the ''ALLIANT 2'' Request for Proposal, anticipating a $50 billion, 5-year contract, with a 5-year option. This GWAC will offer agencies opportunities to purchase for ''every conceivable aspect of IT services.''[14]

---

[8] *Improving Cybersecurity and Resilience through Acquisition*, Final Report of the Department of Defense and the General Services Administration, Feb. 2013, available at https://www.wbdg.org/pdfs/DoD-GSA_Cyber_Acquisition.pdf.

[9] GSA, along with DoD and NASA, issued a proposed rule in June 2014 that would expand reporting obligations for nonconforming parts for all federal contracts involving supplies. *Expanded Reporting of Nonconforming Items*, (FAR Case 2013-002) June 10, 2014, available at http://www.gpo.gov/fdsys/pkg/FR-2014-06-10/pdf/2014-13336.pdf. The final rule on this FAR case has not been promulgated.

[10] *Resilient Military Systems and the Advanced Cyber Threat,* Task Force Report of the Department of Defense Science Board, Jan. 2013, at 6, available at http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf.

[11] *FEDSched, GSA Schedule Sales Fiscal Year 2014*, available at http://gsa.federalschedules.com/resources/gsa-schedule-sales-2014/.

[12] GovWin (from Deltek), *GSA Schedule 70 Analysis*, Feb. 20, 2013, available at http://iq.govwin.com/corp/downloads/Deltek-Proactive-Schedule-70-2013.pdf.

[13] Several other federal agencies have their own IT GWACS, open to all federal agencies. These include, for example, NASA's SEWP (Solutions for Enterprise-Wide Procurement), the National Institutes of Health's CIO-SP (CIO—Solutions and Partners), and the Army's ITES-2S. Several federal agencies have IT GWACS with limited access, such as SeaPort-e (Navy), EAGLE and EAGLE II (DHS). GSA receives an ''Industrial Funding Fee'' (IFF) as a percentage of sales made from under the GSA Schedule Contract. These fees help support GSA. As GSA contemplates cyber and supply chain security measures in its Schedule Contracts, it likely appreciates that burdensome obligations will affect FSS pricing and could drive federal agencies to use other available GWACS vehicles.

[14] *Special Notice 2nd draft Request For Proposal (DRFP)15 October 2015*, Federal Business Opportunities (FBO), available at http://src.bna.com/bxm. To illustrate its breadth, among the forms of IT services that are encompassed within the ALLIANT 2 draft RFP are Big Data; Cloud Computing; Context-aware Computing; Critical Infrastructure Protection and Information Assurance; Cyber Security; Digital Trust and Identity Integration and Management; Enterprise Resource Planning; Integration Services; Internet of Things; IT Services for Healthcare; Mobile-Centric Application Development, Operations and Management; Network Operations, Infrastructure, and Service Oriented Architecture; Outsourcing IT Services; Software Development; Voice and Voice Over Internet Protocol (VOIP); Web Analytics; Web Services and Web Hosting.

GWACS and the FSS operate at two levels. The Schedule *Contract* is distinct from the *Task* or *Delivery-Order*. GSA awards Contracts (for example, an Indefinite Delivery Indefinite Quantity (IDIQ)) to companies selected through competition. At the level of the Schedule Contract, GSA requires fulfillment of various regulatory obligations, terms and conditions, as well as requirements for the scope of performance or specification of supplies. In each case, however, the awarded contracts enable agencies (and others eligible) to award Task Or Delivery Orders. Orders are funded and represent binding commitments from the seller to provide the supplies and services. Pursuant to Federal Acquisition Regulation (FAR) 8.404(b)(1), the contracting officer, when placing an Order or establishing a BPA, ''is responsible for applying the regulatory and statutory requirements applicable to the agency for which the order is placed or the BPA is established.'' A master Schedule contract may contain both mandatory provisions, applicable to all orders, and optional provisions that agencies can elect to include when seeking bids for Task and Delivery Orders.

This ''bifurcation'' between the contracting vehicle and the Task or Delivery Order may explain why GSA has been slow to impose security obligations across the billions of federal dollars spent annually for IT through GSA vehicles. Simply put, it is hard to know what to include at the Schedule Contract level that might be, at once, either too little or too much security for the particular Order. Yet, there is an important national interest to protect IT equipment and services purchased through all MAS vehicles against cyber and supply chain risk. Therefore, with due regard for the difficulty, GSA can and should set baseline requirements to operate at the level of master Schedule Contracts. These might be tailored to the particulars of the scope of individual Schedule Contracts and more narrowly for Special Item Numbers (SINs). GSA should also develop and secure industry's views on standard contract clauses that purchasing agencies can utilize at the order level where more than the baseline measures are needed.

Current GSA Cybersecurity and Supply Chain Practices

The General Services Administration Acquisition Manual (GSAM) contains the General Services Acquisition Regulations (GSAR) and nonregulatory agency acquisition guidance. Today, the GSAM contains few cybersecurity or supply chain security requirements. GSAR 552.23970 (Information Technology Security Plan and Security Authorization) and GSAR 552.239-71 (Security Requirements for Unclassified Information Technology Resources) operate upon the Task or Delivery Order rather than at the Contract level. Their focus is upon IT security ''for all systems connected *to a GSA network* or operated by the Contractor *for GSA*, regardless of location.'' (Emphasis added.) In other words, they apply to GSA contractors who operate ''federal information systems,'' as defined by statute and NIST.[15] But the controls would not extend to protect information or systems, even if purchased from a MAS contractor, if used for *other* federal agencies or on *nonfederal* (contractor) information systems. Even as to GSA systems, there is an emphasis upon an IT Security Plan – as distinct from specific cyber controls and enhancements, as have been stated by NIST for federal information systems through SP 800-53.

Especially after the breach of OPM personnel records, some federal agencies, in a ''rush to regulate,'' on occasion have sought to protect federal interests by collecting every at-hand cyber requirement and thrusting them upon contractors by solicitation requirement or contract term. Resort to such ''blunderbuss'' thinking is a mistake – however well intended.

Examples have been seen where federal agencies impose on commercial providers a veritable ''laundry list'' of security requirements that were intended only for *federal* information systems and (in certain cases) literally cannot be satisfied by a commercial contractor. When federal agencies reach into a ''grab bag'' of conceivable requirements, they may impose on contractors several or even many arduous obligations that were created exclusively for federal information systems and not for contractors who operate their own IT systems to perform federal contracts.[16] Excessive demands derived from inapposite sources may have no relationship to the actual cyber risk or sensitivity of hardware purchased off Schedule 70 (for example) from commercial sources and may contribute nothing to protection – but will be very costly to perform and could create high compliance risks to contractors willing to sign up.

Recently, as noted, GSA released the second draft of the RFP for ALLIANT 2. It includes a Special Provision, at H.6, that makes contractors subject to ''all ordering activity IT security standards . . . and government wide laws or regulation applicable to the protection of government wide information security.'' Special Provision H.7 lists twenty-two (22) separate government policies or requirements, including GSAM provisions 552.239-70 and 552.239-71, which are to apply ''to all users of sensitive data and information technology (IT) resources, including contractors, subcontractors, lessors, suppliers and manufacturers.'' Indisputably, this is an expensive approach – but it is insufficiently informative as well as indiscriminate. No contractor bidding to ALLIANT 2 can guess in advance what may comprise ''all ordering activity IT security standards'' any more than they can predict or presume what (if any) agency ''sensitive data and information'' will be conveyed in the performance of a Task Order. Similarly, examples can be identified where GSA has sought to impose FISMA standards on private contractors – a meaningless effort, since FISMA does not apply to the nonfederal community.

Considering so many examples of damage done through cyber attacks on both federal and nonfederal

[15] NIST SP 800-171 defines a *federal information system* as a system that is used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency. An information system that does not meet such criteria is a *nonfederal information system*. *See alsoMinimum Security Requirements for Federal Information and Information Systems*, FIPS Publication 200, March 2006, at 7, citing 40 U.S.C. § 11331, available at http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf.

[16] One example would be the proposition that a contractor, because it uses some form of CUI, must obtain an ''authorization to operate'' (or ATO) before it can use its IT system to perform a federal contract.

  PVLR ISSN 1538-3423

systems, and the well-documented hazards of counterfeit electronics, GSA can be expected to address cyber and supply chain requirements in Schedule Contracts and by adding new provisions to the GSAM. Yet, GSA also has to guard against going too far. Both to obtain the desired results and to set goals that contractors actually can and will achieve (and not merely promise), GSA initiatives to improve cyber and supply chain security in MAS contracting must be risk-based and discriminating. New approaches should go through notice and comment rulemaking, so that the views of industry are considered. Because industry may not be ready for new measures, care is necessary to provide for transition, reasonable means of implementation, and access to resources and support for contractors, especially small business.

Schedule contractors faced with such excessive demands must be wary. Cyberattacks can, do and will happen, irrespective of and despite best practices. If government information is compromised after a cyber attack, GSA Schedule contractors who sign up to provide information security can expect review or even investigation of their cyber practices. Should a Schedule contractor sign up to obligations it knows it has not met or cannot meet, it risks potentially severe contractual sanctions should the Government conclude it failed to perform to the stated requirements. Liability could extend to assertions, under the False Claims Act, that contractors misled the Government by express or implied certification of conformance with federal cyber standards.[17] GSA should not make its Schedule IT contracts traps for the unwary – cyber obligations, such as those to protect CUI, must be reasonable and feasible and allow for transition and resolution of implementation issues. GSA should disclaim any intent to make its contractors ''guarantors'' of information security, because that is an unobtainable goal. At the same time, Schedule contractors can expect GSA to issue new rules to add cyber security to their obligations – and should take prudent measures now in anticipation of these requirements.[18]

[17] False claims may be divided into factually false claims and legally false claims. A factually false claim would include billing for services or goods that were in fact not provided. A legally false claim includes billing for services or goods that were provided, but some other requirement was not satisfied. Legally false claims may arise from a contractor's certification to the Government. This certification may be express or implied. A contractor, for example, may expressly certify that it will meet all federal IT security requirements. This is an express certification. If the contractor fails to meet this certification even though performance has been satisfactory in all other areas, the claim will be legally false. An implied certification occurs when the contractor does not directly certify compliance with the requirement, but compliance with that requirement was expected as part of performance and a condition for payment — or sometimes simply tied to the Government's decision to pay.

[18] Some in GSA may favor asking for greater contractor commitment to cyber controls as a ''market differentiator'' that should encourage adoption by contractors. This presumes, incorrectly, positive contractor reaction to the absence of stated requirements, established controls or standards, or means to realize competitive benefit in the selection process. Cyber security measures come at a cost. Bidders who adopt more controls could be non-competitive for Task or Delivery Order requirements that do not include corresponding requirements.

How GSA Can Protect Controlled Unclassified Information

GSA MAS vehicles, such as Schedule 70, are used by agencies and other eligible purchases to procure many forms of IT supplies and services. The absence of any generally applicable cybersecurity requirement from Schedule Contracts is a noteworthy omission that should be corrected. Cyber measures can be applied at the Schedule Contract level to protect CUI in performing an IT supply or service through any GSA vehicle. GSA should be able to identify those Schedule Contracts and particular SINs where performance of Task or Delivery Orders will involve communication, use or storage of CUI. Additional controls and enhancements can be added to the GSAM, included in master Schedule Contracts and applied, where necessary, at the Order level.

At the Schedule Contract level, GSA should align its cyber requirements to NIST SP 800-171, which NIST intends to be the new norm for commercial companies who host, transmit or use any form of federal controlled unclassified information. DoD has taken this approach with its recently revised Interim DFARS, deliberately developed to apply NIST SP 800-171 cyber controls to protect unclassified but sensitive DoD information in private company hands. Individual Contracting Officers and Requiring Activities do not have to decide independently how to protect the four categories of ''covered defense information'' subject to this rule. GSA should be able to identify those GWACS (e.g., ALLIANT) and Schedule Contracts where a contractor will be entrusted with a form of Controlled Unclassified Information, similar to the approach taken by DoD. (This could leverage what DoD has learned since it first promulgated the UCTI Rule in 2013.) Implementation of CUI controls at the Schedule Contract level should simplify the challenge and reduce the need to develop order-specific controls.[19] Using SP 800-171 as the common basis of controls across MAS contracts should promote another important federal objective, namely consistency in the cyber requirements imposed upon industry across agencies.

NARA's announced intentions include development and promulgation of a single FAR regulation to apply CUI safeguarding measures across all agency contracts.[20] The urgency of responding to cyber and supply

[19] Another pending GWACS initiative is the Veterans Technology Services 2 (VETS 2) solicitation, available at http://src.bna.com/bDb. VETS 2 will be restricted to SDVOSB prime contractors. The draft RVP includes, at Attachment J-3, an example of a ''laundry list'' of federal information assurance requirements. It includes both NIST SP 800-53a and SP 800-171. While these have similar purposes, the nature of the requirements they impose upon commercial sources is *fundamentally* different.

[20] As explained by NARA, the single FAR clause ''will apply the requirements of the proposed rule to the contractor environment and further promote standardization to benefit a substantial number of businesses, including small entities that may be struggling to meet the current range and type of contract clauses. In the process of this three-part plan (rule, NIST publication, standard FAR clause), businesses will not only receive streamlined and uniform requirements for any unclassified information security needs, but will have information systems requirements tailored to contractor systems, allowing the businesses to help develop the requirements and to be in com-

chain threats suggests that GSA should not wait until NARA's effort is complete.[21] GSA has the tools it needs to act now and it can subsequently adjust the FAR rule when completed by NARA.

GSA should distinguish between controls it imposes on GWACS Contracts and those it selects for Federal Supply Schedule Contracts. When ALLIANT or similar GWACS are used to make contractors responsible for operation of a federal information system, controls beyond SP 800-171 may be necessary. Companies qualified to bid and win an ALLIANT award are more likely capable of implementing more rigorous controls. For IT Schedule 70, in contrast, imposition of unnecessary requirements will drive costs, drive away credible and competitive suppliers, and frustrate federal access to the commercial marketplace.

GSA also should augment the GSAM to establish further cyber-specific contract terms. The new terms should be developed with stakeholder input and then made available to contracting officers. Schedule contractors should be informed of what cyber contractual terms GSA may employ to address specific cybersecurity objectives. New master Schedule Contracts can include additional cyber terms and inform bidders which will be imposed on all orders and which can be selected by agencies.

Another strategy to consider is suggested by GSA's recent initiative to explore a new Special Item Number (SIN) on Schedule 70 specifically for Cybersecurity and Information Assurance (CyberIA) supplies and services.[22] Behind this initiative is the proposition that GSA should concentrate and apply special qualification requirements for high sensitivity cybersecurity services that agencies might purchase off Schedule 70–Information Assurance, Virus Detection, Intrusion Detection and Prevention, Network Management, Situational Awareness and Incident Response, Secure Web Hosting, Backup and Security Services and Communications Security. Advocates believe a CyberIA SIN will concentrate and differentiate cybersecurity offerings. This strategy might be extended to other new cyber-specific SINS under Schedule 70. For these cybersecurity-specific SINs, GSA could establish appropriate cyber and supply chain standards and manage a qualification process. Where applicable, GSA could require submission of system security or supply chain risk management plans and disclosure of information that could be relevant to supply chain risk assessment. If able to select from cybersecurity-specific SINs, agencies would have more informed choices when they need high-assurance supplies or services, and companies would price these supplies and services to reflect the costs of the security enhancements. At the same time, commercial sources of IT technology can continue to offer supplies and services under existing Schedule 70 SINs where the cyber measures are unnecessary. Because this will be a sensitive subject to the community of GSA Schedule suppliers, GSA should consider a public meeting or other means to seek input from all stakeholders on these initiatives.

For appropriate GWACs and SINs that call upon contractors to handle CUI, GSA could invoke (and include in the GSAM) obligations for prospective suppliers to conduct a cyber self-assessment. For illustration, commercial suppliers on FSS Schedule 70, SIN 132-51 (Information Technology Professional Services) could be tasked to employ the NIST Framework for Improving Critical Infrastructure Cybersecurity, released in February 2014.[23] The Framework Core comprises five functions – Identify, Protect, Detect, Respond and Recover – that are broadly applicable to many technologies and systems vulnerable to cyber threats. While some parts of industry would object, the diversity and persistence of cyber threats may justify a Schedule Contract requirement that companies who would provide ICT to the federal government, at least where CUI is involved, should complete a self-assessment guided by the Framework (or commercial equivalent) and prepare a basic system security plan.[24]

How GSA Can Protect Supply Chain Security

Supply chain security includes assurance of the authenticity of electronic systems and detection and avoidance of counterfeit equipment. For ICT purchases, this objective also can be addressed at the GWACS or Schedule Contract level.

Measures that improve assurance of authentic supplies and reduce the risk of counterfeits or nonconforming material are important to fulfill mission objectives of every federal agency and to reduce cyber vulnerability that can be present across product and system lifecycle. Increasing attention is being paid to cyber-physical threats, for example the exploitation of active electronic components or embedded firmware to degrade or deny intended system functionality. Cyber-physical vulnerabilities increase as the ''Internet of Things'' (IOT) proliferates connected devices that are software-enabled or controlled. Threats to the IOT might exploit cyber-physical vulnerabilities to result in physical harm to individuals, failure of critical government systems or compromise to facilities infrastructure. Over time, manufacturers and providers of connected, active devices, in many areas of federal application, will need to address and respond to IOT vulnerabilities. Further, there is a distinct national interest in assuring that

pliance with Federal uniform standards with less difficulty than currently.'' 80 Fed. Reg. 26503.

[21] The OMB draft Acquisition Guidance also anticipates that the Federal Acquisition Regulatory Council will amend the FAR to provide for inclusion of contract clauses that address, as appropriate, guidance that includes application of NIST SP 800171 security controls to protect CUI.

[22] *Request for Information (RFI)-GSA Proposed to Add a CyberIA Special Item Number (SIN) on IT Schedule 70*, Solicitation Number: MAS_S70_CyberIA_FCIS-JB-980001-B, Aug. 12, 2015, available at http://src.bna.com/bxn.

[23] *Framework for Improving Critical Infrastructure Security*, NIST SP 800-37 v. 1.0., Feb. 12, 2014, *available at* http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf. The Framework document was developed by NIST to guide private concerns on how to view cybersecurity risk and the processes in place to manage that risk. The Framework is relevant to many commercial sources of ICT, without imposing specific control regimes.

[24] For contracting vehicles such as ALLIANT that look to a smaller number of companies to sell IT services and solutions to federal agencies, GSA should also consider use of requirements at the master Contract level to mandate use of the risk management framework of NIST SP 800-37, intended for federal information systems. *Guide for Applying the Risk Management Framework to Federal Information Systems*, Rev. 1, Feb. 2010, *available at* http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf.

   ISSN 1538-3423

certain ICT hardware, when used for critical systems or applications, is not obtained from sources that may present national security risks. When IT hardware is used in trusted systems and installed in a network environment, cyber-physical vulnerability at one link could be exploited to attack sensitive equipment or compromise sensitive information.

GSA has done little so far to protect against these ''cyber-physical threats.'' Because federal agencies (including DoD) purchase billions of dollars of ICT through GSA Schedules, especially Schedule 70, GSA should give priority to finding measures that will improve protection of federal MAS purchasers against these threats. It should also be possible for GSA to identify categories of hardware purchased on Schedule Contracts and SINs that have comparatively greater vulnerability to supply chain risk or receipt of counterfeit or nonconforming electronic components. Here too, GSA should be able to employ some of the regulatory methods DoD already has employed. GSA also might consider creation of specific SINs for ''higher assurance'' equipment and systems. Again, GSA needs to be discriminating in security strategies and in the selection and application of control measures. Threats and objectives that drive DoD's programs may have similarities to GSA's concerns, but there will be important differences that could lead GSA to measures that are less demanding than those of DoD.

GSA is not insensitive to supply chain risk. On December 12, 2014, GSA issued a RFI for Business Due Diligence for Acquisitions.[25] The objective of this initiative is to establish confidence in contractors and the goods and services they provide to the government. This includes, among other things, ensuring that goods provided to the Government are authentic and have not been altered or subject to tampering, and that service providers have appropriate programs to detect insider threats. The approach selected relies upon collection of large quantities of information about contractors and subcontractors and their performance of supply orders. It envisions application of data analytics measure contractors along a set of risk indicators, e.g., financial condition, reported quality problems, legal proceedings, mergers and acquisitions, and foreign ownership. These purposes are commendable. GSA should be cautious with a data analytics approach, however, and not allow algorithms to make ''automatic'' decisions to exclude sources of particular equipment.[26] GSA's Schedule 70, especially, reaches and relies upon a global supply chain. The uses of equipment purchased through Schedule 70 vary enormously. Thus, it appears neither prudent nor necessary to impose ''bright line'' rules excluding sources on the basis of country of ownership or operation. Also, analytic methods can depend upon algorithms which can be ''gamed'' by criminals or adversaries seeking to avoid alert triggers.

There is immediate value in government policies that express preference for ''trusted suppliers,'' i.e., original component, equipment and device manufacturers and their authorized distributors.[27] Experts have long concluded that purchasing exclusively from original and authorized sources mitigates a significant portion of risk in ICT purchasing. GSA may wish to adopt similar rules for IT hardware and support, expecting its MAS vendors to rely upon trusted suppliers where possible.[28]

At the GWACS or Schedule Contract level, for certain types of complex ICT acquisitions, where high-sensitivity utilization reasonably can be expected, GSA prudently could seek information from its suppliers and other open sources to better inform selection decisions of potential supply chain risks, and to suggest confidence-building or risk-mitigation measures. If it were to create a Schedule Contract or specific SINs for ''higher assurance'' ICT equipment, GSA could limit eligibility to suppliers who can assert and can demonstrate that they meet selected industry standards for quality systems (e.g., ISO 9001, SAE AS913), counterfeit avoidance (e.g., SAE AS553), avoidance of maliciously encoded parts (e.g., ISO/IEC 20243), or equivalent. Also available for selection decisions would be information derived from open sources (e.g., ERAI, PPIRS, GIDEP) as to reported quality or performance problems, or the ability to apply advanced test and inspection methods (e.g., SAE AS6171). Other measures are available beyond preferences for ''trusted suppliers.'' Additional controls, however, may be in the domain of ordering agencies. In addition to an enlarged inventory of developed, reasonable GSAM terms, GSA should provide examples of actions agencies should take to affect vendors and achieve system security goals (use-cases) and other guidance for ordering agencies where it is appropriate to impose higher-level cyber or supply chain security requirements. This guidance should be made available to the contractor community.

Actions for Contractors

For several years, DoD contractors, at all levels of the defense supply chain, have been dealing with mandated

[25] *Business Due Diligence for Acquisitions involving Government Information or Information Systems*, Solicitation number: BIZDUEDIL-RFI-001, Dec. 12, 2014, available at http://src.bna.com/bxo.

[26] Data-driven analytics, for illustration, can establish a correlation between a data point (manufacture of a system or assembly in China, for example) and generation of risk indicators (red flags) that might disqualify a device or its suppliers. In certain cases, public source data can reliably inform purchasers and operators of comparatively greater supply chain risk. However, open source data is not always reliable and information could be collected that is subject to mitigation or where an affected contractor should be informed and afforded opportunity to respond.

[27] The proposed DFARS improving measures to avoid counterfeit parts, *supra* n.6, retains as government policy for DoD suppliers that they should obtain electronic parts from original manufacturers, authorized dealers or suppliers who obtain such parts exclusively from the original sources. If other sources must be used, additional measures such as testing are expected. DFARS 246.870-2, DFARS 252.246-70XX. Experience gained by DoD will be relevant but the challenge faced by GSA may differ materially. DoD has obligations to sustain fielded equipment that create exposure to counterfeits because needed electronic parts no longer are in production or available from authorized sources. GSA has less of a problem with parts obsolescence but it must address what is likely to be a much larger universe of equipment to buy and support as well as many more sources and distribution channels.

[28] Not all distribution arrangements, however, produce the same level of assurance. The breadth of the global supply chain accessed through GSA schedules and the diversity of supplies and services acquired by schedule purchases suggest that GSA could identify certain areas of supply where it should require disclosure of the sales relationship between original sources and their distributors.

cyber and supply chain security contracting measures. Civilian agency contractors should expect to follow suit. The size and importance of GSA MAS vehicles and the value of ICT purchased through these vehicles make it highly likely that cyber and supply chain security requirements will come to the GSA environment, and soon. The transition will not be without difficulties and costs, but these are necessary to protect multiple national interests against threats of new character but high impact to agency functions. Compromise of protected information also can have adverse consequences affecting individuals if their private personal information is lost, as made all too evident by the OPM breach.

There is no single script to how responsible companies should prepare for new requirements, but several steps are recommended. To start, a company might conduct a self-analysis, guided by the NIST Framework (or equivalent), to identify vulnerabilities and risk. Government contractors should ascertain whether they access and use CUI and whether their products are exposed to supply chain risk. Companies then might examine present controls and practices and compare these to emerging government requirements and existing standards and best practices. A company then could prepare a ''fit/gap'' analysis to document where its practices are sufficient and where improvements are needed. This effort would support documentation of an information system and supply chain security plan. Such a plan likely will reveal where compliance is assured and where new controls or procedures could be needed. When companies are faced with new cyber and supply chain solicitation requirements, they will benefit from having this documentation prepared. Over the course of contract performance, companies should keep records to document its implementation of planned security improvements and to show continuous self-assessment as new threats emerge. Taking these actions may become the ''minimum'' to qualify for future GSA IT procurements, and certainly represent prudent measures to mitigate liability risk should a cyber event occur in the performance of a MAS Task or Delivery Order.

Conclusion

Federal agencies rely upon GSA purchasing vehicles for huge amounts of IT supplies and services that are crucial to agency missions and which involve many forms of sensitive information, including records subject to privacy controls. It is therefore necessary and timely for GSA to extend and improve cyber and supply chain protection to its MAS vehicles. At the contract level, GSA should provide a baseline of protection against cybersecurity threats to physical systems and to protect federal information that contractors host, transmit or use on behalf of agency customers. GSA must balance the value of these measures against many potentially dysfunctional consequences, not the least of which are added cost and complexity or foreclosure of access to innovation of commercial sources. GSA should seek to inform and align its measures by reference to current initiatives of NARA, NIST and DoD. Contractors naturally seek consistency in rules applied to them. The federal government should promote convergent rather than divergent agency approaches to common security problems.

While consistency is an important objective, agencies should retain the ability to impose additional measures in Task and Delivery Orders when justified. Whenever an agency places an order under a MAS contract to satisfy an ICT requirement, it will know whether and what CUI is or may be provided and the impact to its mission should there be a compromise of information security. Agency-specific considerations should figure into risk-adjusted determination of whether additional safeguards are justified and what added costs are worth paying. Creation of Schedule Contracts and SINs that concentrate supplies and services where cyber and supply chain risks are greatest would focus the capabilities of the commercial supply base where responsive measures are needed and agencies will pay the attendant costs. Agencies can use other Schedules and SINs without these enhancements where they determine the cyber or supply chain risk does not justify the costs of more secure solutions. Similarly, successful contractor adoption of improved security measures on GSA MAS purchases would be facilitated by development of new provisions for the GSAM through a process that solicits and considers contractor positions on risk, benefit, effectiveness, cost, transition, implementation, oversight, administration and enforcement.

  PVLR ISSN 1538-3423