BRIEFING PAPERS® SECOND SERIES

PRACTICAL TIGHT-KNIT BRIEFINGS INCLUDING ACTION GUIDELINES ON GOVERNMENT CONTRACT TOPICS

GSA TECHNOLOGY ACQUISITIONS: How Cybersecurity Threats And Cloud Services Are Changing The Way The Government Buys Technology From Commercial Companies

*By Alexander W. Major, Franklin C. Turner, and Lillian M. Mezynski**

During the past few years, discussions in Washington, D.C. have intensified over the battle to modernize the Federal Government's information technology (IT) systems. In May 2016, Representative Jason Chaffetz—Chairman of the Committee on Oversight and Government Reform in the U.S. House of Representatives—boldly stated that American "[t]axpayers deserve a government that leverages technology to serve them, rather than one that deploys unsecured, decades-old technology that places their sensitive and personal information at risk."[1] Within six months of coming into office, President Trump issued an Executive Order calling on the Government to "transform and modernize [Government] information technology and how [the Government] uses and delivers digital services."[2] These sweeping proclamations sound an increasingly familiar tune, often whistled by those who work for Uncle Sam at the highest levels—*old technology wastes taxpayers dollars and leaves the Government more susceptible to cyberattacks*.[3] In fact, from 2006 through 2015, the number of reported security incidents in federal agencies increased by an astounding 1,303%.[4] Against this alarming backdrop, the Government has grown ever more reliant upon commercial companies to assist in modernizing its IT systems.

The key to that commercial reliance has been, and continues to be, the General Services Administration (GSA) Multiple Award Schedules Program. In the often complex world of Government procurements, Multiple Award Schedules are important tools that facilitate the Government's goals—codified in statutes and regulations—of conducting market research and promoting a preference for commercial items.[5] GSA Schedules are intended to streamline and simplify the procurement process while providing access to a wide range of commonly used commercial items through a large selection of qualified suppliers.[6] Of course,

*Alexander W. Major and Franklin C. Turner are partners and co-leaders of McCarter & English's Government Contracts & Export Controls Practice Group in Washington, D.C. Lillian Mezynski is an associate in the Government Contracts and Export Controls Practice Group in the firm's Boston office.

IN THIS ISSUE:

THOMSON REUTERS®

words like "streamline" and "simplify" are not only meant to attract Government purchasing professionals, but also commercial suppliers that may not otherwise conduct business with the Government. One such schedule, IT Schedule 70 (Schedule 70), is particularly adept at attracting purchasers and suppliers because it is intended to deliver "federal, state, and local customer agencies the tools and expertise needed to shorten procurement cycles, ensure compliance, and obtain the best value for innovative technology products, services, and solutions."[7] The schedule boasts that with over "7.5 million products and services from over 4,600 pre-vetted vendors" it is able to reduce Government "buying cycles by up to 50 percent over open market."[8] As of the date of this publication, Schedule 70 has successfully attracted commercial suppliers and is becoming "by far the most utilized GSA Schedule" in all of the Government.[9] For example, Schedule 70 sales totaled a whopping $14.6 billion in 2015 alone—*more than double the next most utilized vehicle*.[10]

The Government's focus on industry, however, presents a unique problem for contractors. In particular, contractors may quickly find themselves fencing away hackers and the threats they pose to Government and contractor IT systems with one hand, while simultaneously defending against threats of False Claims Act litigation and contract termination with the other hand.[11] This Briefing Paper addresses the increasingly complex battlefield that commercial companies must navigate when they participate in the Government's acquisition of IT products and services, especially in the face of cybersecurity threats and the constantly evolving IT market, while also providing risk mitigation strategies for participating in IT acquisitions.

"A Crisis Bigger Than Y2K"[12]

Maintaining the Government's aging IT systems is costly and risky.[13] Unlike the "Year 2000 (Y2K) problem," where the Government anticipated a crisis with a date certain in mind (*i.e.*, December 31, 1999), the Government currently faces a "ticking time bomb" that could go off at any time, as security concerns grow and efforts to secure the Government's antiquated IT systems become more difficult and more costly with each passing day.[14]

Modernizing Federal IT Systems

The Federal Information Technology Acquisition Reform Act (FITARA) of 2014 represented the first major overhaul of Federal Information Technology (IT) in the past 20 years and set forth the Government's objective of improving the Government's management of IT.[15] In the days before the passage of FITARA, some Senators acknowledged that "[w]e built an IT infrastructure that is bloated, inefficient, and actually makes it more difficult sometimes for the government to serve its citizens."[16] Meanwhile, others boldly held onto the idea of "better results for less money, or the same money."[17]

Soon after FITARA became law, the Government Accountability Office (GAO) issued a report elucidating the extravagant amount of money agencies spend annually to maintain legacy IT systems.[18] The GAO's 2015 High-Risk Series report found that "agencies spent over $80 billion annually on IT investments, but over 75 percent of the $80 billion went towards operations and maintenance of legacy IT," leaving less funding available for development.[19] As part of GAO's investigation, the Department of Defense (DOD) reported that its Strategic Automated Command and Control System—which coordinates the operational functions of the U.S. nuclear forces—is over 50 years old, runs on an IBM computer from the 1970s, and uses eight-inch floppy disks.[20] To put this in perspective, a single modern flash drive can hold the same amount of data as 3.2 million floppy disks.[21] During Committee hearings, members of

Editor: Valerie L. Gross

Briefing Papers® (ISSN 0007-0025) is published monthly, except January (two issues) and copyrighted by Thomson Reuters, 610 Opperman Drive, P.O. Box 64526, St. Paul, MN 55164-0526. Customer Service: (800) 328-4880. Periodical Postage paid at St. Paul, MN. POSTMASTER: Send address changes to Briefing Papers, 610 Opperman Drive, P.O. Box 64526, St. Paul, MN 55164-0526.

Congress recognized that "spending on legacy IT results in higher costs and security vulnerabilities where old software and operating systems are no longer supported by vendors. The Federal Government is years, *and in some cases decades,* behind the private sector."[22]

Funding For Modernization

Recognizing that the problem of modernization is perpetual, the House of Representatives recently passed the Modernizing Government Technology Act of 2017 (MGT Act).[23] The purpose of the MGT Act is "to build on FITARA and empower and hold accountable covered agency [chief information officers] to pursue IT modernization."[24] If it becomes law, the MGT Act would establish new budget accounts to fund efforts to modernize Government IT systems.[25] In congressional hearings, the need to modernize technology to be more cost effective and adequately protect information security was raised repeatedly.[26] Moreover, State Representatives acknowledged that budget cuts reduce the amount of funding agencies can devote to system upgrades, not to mention hiring and retaining staff needed to modernize and replace outdated information systems.[27]

The House of Representatives recognized that uncertainty in budgets for information systems and IT "handicap[s] our ability to modernize our legacy environments and our aging infrastructure and provide the services that taxpayers need."[28] A main purpose of the MGT Act, therefore, is to establish a dedicated modernization fund to help agencies replace their outdated information systems with "more modern, adaptive, and secure systems."[29] Importantly, the bill ensures that funding can continue by establishing a "revolving loan fund" that would be "self-sustaining because agencies that receive money for modernization projects would be required to repay it over time."[30]

Procuring Modern Information Technology

While funding for modernization is crucial, several barriers still exist in federal procurement, especially regarding the use of cloud computing. For example—as even the casual observer might quickly recognize—the Government has "ingrained cultures that are slow to change" (*i.e.*, the floppy disk) and the federal appropriations process does not lend itself to investing in risky, innovative, long-term procurements in IT systems.[31] The MGT Act is intended to be a crucial turning point, providing the Government with greater flexibility for the purposes of accessing and allocating critical IT-related funding.[32] Procurement officials, however, are likely to still face cautious contractors that wisely recognize the risks of increased targeting by hackers and that must remain alert to potential downstream liability to the Government in the event of a breach. In fact, the former head of the Office of Federal Procurement Policy and Defense Procurement and Acquisition Policy recently acknowledged that the Government needs to "decriminalize commerce."[33] The following sections of this BRIEFING PAPER, therefore, take a deeper dive into progress the Government has made in facilitating the procurement process for commercial suppliers that can offer assistance in taking the Government's IT systems out of "crisis" mode. Equally importantly, this PAPER also highlights the risks these commercial companies turned Government contractors will continue to face when conducting business with the Government.

GSA Schedule 70 Overview

As one of over 30 different Schedules under the GSA MAS Program, Schedule 70 is the largest acquisition vehicle in the federal Government.[34] Schedule 70 covers commercial IT products and services, such as cybersecurity measures, cloud computing software and platforms, e-authentication hardware tokens, and equipment such as cables, desktop computers, and modems.[35] These items are available through the Schedule to all federal agencies as well as state, local, and tribal governments through cooperative purchasing for certain Special Item Numbers (SINs), which are identified in Table 1 below.[36] As of the date of the publication of this PAPER, the products and services available on Schedule 70 are classified into 31 SINs, some of which contain further discrete subcategories.[37]

The Government's commercial IT products and services needs range from the very basic, everyday hardware to advanced, specialized services. For example, many commercial suppliers take advantage of opportunities to lease, rent, and sell cables, modems, digital cameras, laptops and other forms of equipment to the Government. Meanwhile, other specialized suppliers focus on commercial satellite communications subscriptions, cyber hunt services, or penetration testing. The Government's various needs and reliance on commercial IT products and services continue to make Schedule 70 the most used Schedule in the Government.

In fiscal year 2016, federal, state, and local governments collectively purchased approximately $45 billion through GSA Schedule contracts, with about $14.7 billion in sales going through Schedule 70.[38] Needless to say, the Govern-

ment's eagerness and willingness to spend on IT lures many commercial IT suppliers into the realm of Schedule 70 like flies to honey. However, access to the ease that Schedule 70 offers to federal purchasers is not without significant risks that many commercial contractors may not be prepared to properly address. In addition to the normal list of compliance risks, country-of-origin requirements, audit rights, and recordkeeping requirements associated with contracting with the Government, the following sections of this PAPER briefly review some of the areas where commercial and Government sales can levy significant risks on Schedule contractors.

Table 1. Schedule 70 SINs[39]

SIN	Description
132-100	Ancillary Supplies and/or Services
132-40	Cloud Computing Services
132-41	Earth Observation Solutions
132-99	Introduction of New Information Technology Services and/or Products
	COMSATCOM SERVICES
132-54	Commercial Satellite Communications (COMSATCOM) Transponded Capacity*
132-55	Commercial Satellite Communications (COMSATCOM) Subscription Services*
	CYBER HUNT
132-45C	Cyber Hunt
	IDENTITY, CREDENTIAL AND ACCESS MANAGEMENT
132-60A	Electronic Credentials, Not Identity Proofed (Assurance Level 1 OMB M-04-04) Managed Service Offering
132-60B	Electronic Credentials, Identity Proofed (Assurance Level 2 OMB M-04-04) Managed Service Offering
132-60C	Digital Certificates, including ACES (Assurance Level 3 and 4 OMB M-04-04)
132-60D	E-Authentication Hardware Tokens
132-60E	Remote Identity and Access Managed Service Offering
132-60F	Identity and Access Management Professional Services
132-61	Public Key Infrastructure (PKI) Shared Service Providers (PKI SSP) Program
132-62	Homeland Security Presidential Directive 12 Product and Service Components
	INCIDENT RESPONSE
132-45B	Incident Response
	PENETRATION TESTING
132-45A	Penetration Testing
	PRODUCTS
132-3	Leasing of Products
132-4	Daily/Short Term Rental
132-8	Purchase of New Equipment (boards, cables, desktop computers, digital cameras, etc.)*
132–9	Purchase of Used or Refurbished Equipment
132-12	Maintenance of Equipment, Repair Services, and/or Repair/Spare Parts
	RISK AND VULNERABILITY ASSESSMENTS
132-45D	Risk and Vulnerability Assessments
	SERVICES
132-56	Health Information Technology Services
132-50	Training Courses
132-51	Information Technology Professional Services (automated news, data, and other information services, desktop management, IT backup and security services, programming services, etc.)
132-52	Electronic Commerce and Subscription Services (e-mail services, internet access services, etc.)
132-53	Wireless Services
	SOFTWARE
132-32	Term Software License (Macintosh, Office Suites, Virus Detect, etc.)*
132-33	Perpetual Software License*
132-34	Maintenance of Software as a Service*
**TDR Applies*	

Commercial Sales Practice And The "Price Reductions" Clause

The MAS Program provides agencies with competitive, market-based pricing. Orders placed under the MAS Program will be found to meet federal competition requirements as long as they result in the lowest overall cost alternative for the Government's needs.[40] In order to ensure that Schedule orders meet MAS Program competition requirements, the Government historically used the Commercial Sales Practice (CSP) disclosures and "Price Reductions" clause (PRC) requirements to "secure the vendor's most favored pricing and maintain this position for the life of the contract."[41] Under this regime, the Government generally relied on "vertical" pricing models to establish reasonableness by comparing the contractor's prices with those offered to their other customers.[42]

In general terms, the PRC is a condition negotiated by the GSA before a company is granted a Schedule contract. It is intended to address "[a]ny change in the Contractor's commercial pricing or discount arrangement applicable" to the contractor's Basis of Award customer or category customers that "disturbs" the Government's price/discount relationship to the chosen customer or category of customers.[43] The key to the PRC working as intended, of course, is for commercial companies to identify the customer or category of customers upon which the price/discount relationship is established.[44] Equally, if not more importantly, it is beholden on the GSA to "[s]tate clearly in the award document the price/discount relationship between the Government and the identified commercial customer (or category of customers) on which the award is predicated."[45]

With the relationship negotiated and established, the clause identifies three events that can trigger its protections and mandate a price reduction be given to the Schedule purchaser. This will occur if the supplier/contractor:

> (i) Revises the commercial catalog, pricelist, schedule, or other document upon which contract award was predicated to reduce prices;
>
> (ii) Grants more favorable discounts or terms and conditions than those contained in the commercial catalog, pricelist, schedule, or other documents upon which contract award was predicated; or
>
> (iii) Grants special discounts to the customer (or category of customers) that formed the basis of award, and the change disturbs the price/discount relationship of the Government to the customer (or category of customers) that was the basis of award.[46]

In the presence of these events, the contractor is required to "offer the price reduction to the eligible ordering activity with the same effective date, and for the same time period, as extended to the commercial customer (or category of customers)" that the contractor identified as its Basis of Award.[47] There are, of course, exceptions to the PRC and sales that do not trigger the activation of the clause, such as sales outside the Basis of Award, sales to federal agencies, and sales of products that are not on schedule.[48] Commercial companies contemplating moving into the Schedule 70 arena, however, need to ensure that they have adequate sales discipline to ensure that the sales' staff pricing and discipline fall within the confines of the PRC. In light of how quickly IT products, services, and competition change, the PRC can pose a significant burden on contractors and may severely limit the sales flexibility upon which many software companies rely to conduct business.

Transactional Data Reporting Rule

On June 23, 2016, the GSA issued a final rule to implement "the most significant change to the Schedules program in the past two decades."[49] In response to feedback that the CSP and PRC requirements were some of the most burdensome requirements of the GSA Schedule program, the GSA implemented the Transactional Data Reporting (TDR) Rule to replace these requirements.[50] The TDR Rule aimed to provide "a more dynamic market driven pricing model," in which contractors submit prices paid by the Government and the Government uses this data to "ensure a vendor's offered price is competitive relative to other vendors."[51] Under the TDR Rule, contractors submit 11 transactional data elements to the GSA on a monthly basis in exchange for the elimination of CSP disclosures and PRC requirements.[52] As opposed to the "vertical" model, the TDR Rule allows the Government to take a "horizontal" approach by comparing the contractor's prices with other contractors.[53]

As noted in Table 1, the current TDR Pilot Program applies to 6 of the 31 Schedule 70 SINs.[54] In general, the TDR Program applies to hardware and software procurements, while most services remain subject to CSP and PRC requirements.[55] To expand the TDR program, the TDR requirements will apply to an entire GSA Schedule 70 contract if the contract involves *at least* one SIN that is covered under the TDR Pilot Program.[56] If a contractor only offers non-TDR SIN(s), however, such as the newly added SINs for cybersecurity services, the contract remains subject to CSP and PRC requirements.[57]

Highly Adaptive Cybersecurity Services (HACS)

Relatively new to the GSA schedule are four new SINs specifically targeted to the Government's cybersecurity needs: Penetration Testing under SIN 132-45A, Incident Response under SIN 132-45B, Cyber Hunt under SIN 132-45C, and Risk and Vulnerability Assessment (RVA) under SIN 132-45D (collectively, "Highly Adaptive Cybersecurity Services" or "HACS"). In response to failed IT projects demonstrating the Government's lag behind industry, the Government has turned to Schedule 70 to help to streamline and standardize procurements, providing agencies with a way to develop and implement standard best practices and bridge the gap to industry.[58] While the Government's addition of HACS SINs was meant to improve how agencies acquire cybersecurity services, the process of competing for and obtaining HACS SINs is somewhat unique for those wishing to win a Schedule.

Oral Evaluations

A unique element of the HACS SINs—which is not typical for other Schedule 70 offerings—is an oral technical evaluation. This factor is meant to evaluate contractors wishing to offer HACS to Government Schedule 70 purchasers based on the vendor's knowledge of the proposed services.[59] Prospective contractors are invited to an interview, either in person or virtually, which is held at the unclassified level.[60] At the interview, contractors are given a set of questions and a scenario per SIN and allowed 40 minutes to respond to each SIN-related round of questions and scenarios, with a total evaluation session expected to take up to three hours depending on the number of SINs proposed.[61] The Technical Evaluation Board (TEB) judges the vendor's answers and determines an overall "acceptable" or "unacceptable" rating under the oral technical evaluation factor.[62] Contractors that fail the oral evaluation have one opportunity to provide clarifications regarding the oral interview within 24 hours of the TEB's notice to provide clarifications.[63] If rejected, contractors are ineligible to resubmit proposals for the SIN for which they were rejected for a period of six months following the date of rejection.[64]

Notably, contractors are not permitted to "record or transmit any of the oral evaluation process" and, therefore, may be prohibited from removing their notes from the evaluation room.[65] Contracting Officers (COs) are vested with broad discretion over the creation of the record of the oral presentation and they may use various methods to record the presentation, including videotaping, Government notes, or copies of the offeror's briefing slides.[66]

Transactional Data Reporting Rule Exclusion

When introducing the new TDR Rule, the GSA noted that the CSP and PRC requirements were introduced in the 1980s to help the GSA and customer agencies "maintain advantageous pricing from original equipment manufacturers," which held the majority of MAS contracts.[67] However, the GSA found that "changes in what the Government buys and shifts in the federal marketplace have eroded the effectiveness of these tools over time."[68] Therefore, the TDR Rule would fulfill the Government's purpose of ensuring it obtained fair and reasonable pricing, while balancing the burden on contractors. The newest market for commercial IT services on Schedule 70, however, is generally exempt from the new TDR Rule. Thus, procurements for HACS SINs are rife with requirements CSP and PRC and obligations.[69] The Government will therefore require pure HACS contractors to monitor pricing and provide the Government with all mandatory price reductions over the life of the contract.[70]

Cloud Computing Products & Services

In addition to increasing its focus on the acquisition of cybersecurity services and products, the Government has also embarked upon an IT modernization initiative focused on the use of cloud computing. In 2011, the Government implemented a Federal Cloud Computing Strategy, recognizing cloud computing's potential to solve major inefficiencies in the Government's IT environment, such as low asset utilization, fragmented demand for resources, duplicative systems, difficult to manage systems, and long lead times, and instituted a "Cloud First policy."[71] Like commercial industry, for the Government, cloud computing's appeal is found in its ability "to be scalable and elastic" and does not require the users to "determine their exact computing resource requirements upfront," similar to a utility service.[72] For contractors, cloud computing's appeal, again, lies in its expanding opportunities for awards.

Cloud Computing On Schedule 70

The Government is finding cloud computing to be a fast, cost efficient, and flexible solution for aging IT systems.[73] Purchasing services through a cloud provider "enables [Government] agencies to avoid paying for all the assets (*e.g.,* hardware, software, networks) that would typically be needed to provide such services [in-house]."[74] Moreover,

commercial spending on cloud computing is projected to increase from $67 billion in 2015 to an astounding $162 billion in 2020 worldwide.[75] As commercial sales increase, opportunities for the Government to fulfill its "Cloud First policy" by switching to cloud services have also expanded.[76] In fact, over the past two consecutive fiscal years, the Government has awarded more than $2 billion in cloud contracts.[77] Meanwhile, the SIN for cloud computing under Schedule 70, SIN 132-40, is gaining popularity with agencies that are being pushed to procure commercial cloud computing services "first" and with contractors looking to take advantage of MAS contracts. Recent contract awards for cloud services on Schedule 70 alone more than doubled from $666 million in 2016 to $1.6 billion mid-way through fiscal year 2017.[78]

In April 2015, SIN 132-40 was introduced to Schedule 70 in order to simplify the Government's acquisition of commercial cloud services.[79] While SIN 132-40 was a significant step towards standardizing cloud service procurements, these acquisitions are often laden with Service Level Agreements (SLAs) that are typically comprised of standard *commercial* terms and conditions that often vary dramatically between and amongst suppliers. For example, while the Government is required to address "reliability" as a key service element in SLAs, suppliers use different terms to define reliability, using various terms such as "uptime," "resilience," and "availability."[80] The lack of an industry standard SLA for cloud computing services can cause Government customers to evaluate suppliers' proposed SLAs differently and, often, to reject them out of hand. Moreover, cloud services are not yet measured with the "precision with which we categorize units of measurement in electricity, light, or fuels," and, as a result, procurement officials have a difficult time requesting cloud services with a "high degree of predictability [like other utilities], and cannot achieve maximum cost-effectiveness in cloud computing service application."[81]

Challenges In The Cloud

(1) *Service Level Agreements*. SIN 132-40 for cloud computing services is similar to the HACS SINs, in that they are all exempt from the TDR Rule.[82] SIN 132-40, however, is not subject to the oral technical evaluation requirement.[83] Instead, Government agencies ensure cloud services are performed "effectively, efficiently, and securely," by negotiating SLAs in the resulting contract.[84] SLAs define the level of service and performance, roles and responsibilities, how performance will be measured, and enforcement mechanisms used to ensure performance levels are achieved.[85] As mentioned above, the current cloud computing market does not have "defined and applied standardized units of measurements that can be specified in Service-Level Agreements," so such agreements tend to "vary widely."[86] During negotiations, contractors must carefully review SLA terms provided by the Government to ensure the terms closely align to their specific services being provided.

(2) *FedRAMP*. The Federal Information Security Management Act of 2002 (FISMA) established standard IT security requirements for federal systems.[87] In furtherance of FISMA, the GSA created the Federal Risk and Authorization Management Program (FedRAMP) to ensure contractors providing cloud services to the Government were compliant with FISMA requirements.[88] Importantly for contractors, FedRAMP provides a standardized—and arduous—program for receiving a FedRAMP-compliant designation that is applicable Government-wide.[89] While standardization and streamlining is generally welcomed by industry, contractors should still approach FedRAMP with ample time and preparation.[90] According to a recent Coalfire report, the time for a CSP to reach FedRAMP status and be provided to Government purchasers as FedRAMP compliant has shrunk dramatically over the last few years with an average time now hovering around eight months.[91] The duration of the process will, however, depend on a company's advance preparation in conjunction with the breadth of the authorization it wishes to pursue with the Government.[92] Of course, the cost to obtain FedRAMP authorization can also be a substantial hurdle for some companies and will vary. It has been estimated by Coalfire to range from $350,000 to $865,000 for a Software-as-a-Service solution[93] to upwards of $2.25 million for a mid-range CSP.[94]

(3) *Building in Trust and Termination*. Along with ensuring that cloud service providers meet both technical and security requirements, agencies have also been instructed to specifically plan for contract termination and contractor transition.[95] Toward this end, agencies are required to consider "cessation of service, extraction of data, format(s) for the extracted data, sending the data to a new provider, and restarting key services on the new provider's platform."[96] Inarguably, these are smart steps for the Government to take. However, contractors should prepare themselves for these conversations as they may be points of contention during negotiation.

Government And Industry Concerns

As mentioned above, GSA Schedule 70 is currently the

largest Schedule within the MAS Program. As a result, both Government and industry have felt the burdens of oversight surrounding Schedule 70. For example, the Government has received internal criticism regarding compliance with the MAS Program.[97] In addition, Schedule 70 contractors have often become entangled in the crossfires of major fraud allegations resulting in billions of dollars in fines and tense political controversies. Over time, several major contractors have come and gone from Schedule 70, raising eyebrows throughout Government and industry.

2016 Office Of Inspector General Audit Of Schedule 70 Contracts

In September 2016, the GSA Office of Inspector General (IG) conducted an audit of Schedule 70 price evaluations and contemporaneous contract negotiations to determine whether contract and option awards under the Schedule complied with federal regulations and policies.[98] The resulting report reminded agencies that price negotiation is a key tool for ensuring the Government obtains the best price possible under Schedule contracts.[99] The IG then rebuked Schedule 70 contracting personnel for not consistently conducting negotiations or maintaining proper award documentation.[100] In response to a draft report of the audit, the GSA Office of IT Schedule Programs acknowledged the errors discovered during the audit, while also noting the continuous efforts contracting staff make to adjust to the "ever-changing IT market conditions."[101]

Government personnel faced with procuring commercial IT products and services are faced with a range of issues. In fact, just a few months after the IG's audit, a hearing before the House of Representatives Committee on Oversight and Government Reform highlighted the fact that Government personnel have been faced with finding old parts for legacy systems, which contain either obsolete parts or components that are more than 50 years old.[102] In stark contrast, agencies are also faced with purchasing modern electronics, such as smart phones, with ever-changing operating systems.[103]

The issues facing the GSA and the Government writ large provide commercial companies with significant opportunity. But it is important for commercial companies to realize that the Government may, in its zeal to purchase, attempt to cut corners in the contracting process. While this may sound like good news for a commercial company that just wants to make the sale, it is imperative that any company wishing to sell to the Government not only follow the rules themselves, but make sure the Government is following the same rules.

Oracle Departs The Schedule

In 2016, Oracle removed all products, including those sold through resellers, from the GSA Schedule 70.[104] Although Oracle did not release an official statement, the reasons for departure appeared to be to avoid the hassle of contracting with the Government through its "simplified" means and that the relatively small percentage of Government sales was not worth the severe risks Oracle faced, like those posed by the False Claims Act.[105] For example, in 2011 Oracle settled a lawsuit with the GSA based on Department of Justice allegations that the company failed to meet its contractual requirements to provide the GSA with current, accurate, and complete CSP information, including the discounts the company offered to other customers, and alleged, therefore, that Oracle failed to comply with the PRC requirements.[106] Similarly, in 2015, IT companies VMWare and Carahsoft paid a $75.5 million fine to resolve allegations of misrepresenting CSP information that led to alleged overcharging of the Government on VMWare software and services under the GSA Schedule.[107] Oracle's departure may reflect its, and even industry's, concerns surrounding the potential for severe liability under the False Claims Act for attempting to abide by the often confusing and undefined rules and regulations governing selling through the GSA.

Kaspersky Kicked From The Schedule

Concerns that one GSA Schedule 70 holder may be "susceptible to manipulation by the Russian government, and that its products could be used as a tool for espionage, sabotage, or other nefarious activities against the United States" caused the Government to remove the cyber security firm, Kaspersky Lab, from Schedule 70 in July 2017.[108] In the weeks prior to the removal, Kaspersky drew attention in Washington, D.C. when allegations were raised that Kaspersky maintained ties to Russian intelligence.[109] Kaspersky Lab is a global company, headquartered in Russia, with a U.S. Subsidiary, Kaspersky Lab North America.[110]

In the midst of investigations and questions surrounding Russia's involvement in the 2016 U.S. Presidential election, U.S. officials became concerned that Russian intelligence services "could try to exploit Kaspersky Lab's anti-virus software to steal and manipulate users' files, read private emails or attack critical infrastructure in the U.S."[111] While many references to "concerns" regarding Kaspersky's products and potential ties to Russia's main intelligence agency have been made, Kaspersky denies ties to any government and claims to be in the middle of a "geopolitical fight" between Russia and the United States.[112]

Notably, the Government's actions come when neither Kaspersky Lab nor Kaspersky Government Security Solutions has been formally excluded "from receiving certain federal contracts, subcontracts, and financial and non-financial assistance and benefits" through the System for Award Management (SAM).[113] That is to say, Kaspersky has not been suspended or debarred. However, the use of Kaspersky by Government agencies remains highly restricted and, effectively, banned. The Senate's proposed National Defense Authorization Act for Fiscal Year 2018 expressly calls for the DOD to stop using Kaspersky Lab's products on DOD systems.[114] And, if the Government's actions against Kaspersky with the GSA and the DOD were not clear enough, on September 13, 2017, the Department of Homeland Security issued a Binding Operational Directive (BOD) directing Federal Executive Branch departments and agencies "to identify any use or presence of Kaspersky products on their information systems in the next 30 days, to develop detailed plans to remove and discontinue present and future use of the products in the next 60 days, and at 90 days from the date of this directive, unless directed otherwise by DHS based on new information, to begin to implement the agency plans to discontinue use and remove the products from information systems."[115]

The message out of what is happening with Kaspersky is something that should come as no surprise to many international companies selling to the United States—contractors are susceptible to political whims. Why, exactly, Kaspersky was targeted and what the Government actually knows about the company will probably never be known outside of the intelligence community, but the allegations have a broader effect than simply stopping federal sales. Recently, taking apparent cue from the Government's actions, Best Buy pulled Kaspersky products from the products it is selling.[116] And while the issues surrounding Kaspersky are current, they are far from new or exclusive to the United States. Technology companies from all over the world, and the employees they hire, often find themselves in close proximity to—and initially trained by—their home country's intelligence and national security infrastructure. As such, and be it right or wrong, it is likely that in the future they too can come under suspicion because of those relationships and find themselves, like Kaspersky, "*software non grata*" in the United States.[117]

Guidelines

Despite the seemingly heavy-handed nature of the warnings in this BRIEFING PAPER, the U.S. Government remains a reliant and voracious consumer of commercial IT products. Companies just need to be careful and recognize that the customer with which they are dealing is a multi-headed hydra, with some heads friendly, and others decidedly not. These *Guidelines* are intended to help you navigate the many risks relating to GSA technology acquisitions. They are not, however, a substitute for professional representation in any specific situation.

1. *If applicable, carefully identify and explain your commercial sales practices to the GSA CO negotiating your contract.* Make sure there are no open questions or issues in the mind of the GSA CO as to how pricing and discounting is accomplished. Avoid "company speak" and "program vernacular." Clearly identify, in written communication to the CO, what elements of your proposal constitute a price, a discount, a rebate, a sales incentive, etc. There is no need for a contractor to change the way it sells to commercial companies as long as it clearly identified how it is being done in its CSP.

2. *Choose your Basis of Award customer wisely.* Be wary of attempts or efforts to identify your Basis of Award as "all commercial customers," as such an identification would trigger PRC obligations with *every* commercial sale. This, in turn, would either severely hamstring your company's sales flexibility or would significantly increase your risk of violating the PRC and resulting in possible, and significant, False Claims Act liability.

3. If already on Schedule 70, refamiliarize yourself with the submitted Commercial Sales Practice and the negotiated Price Reduction Clause. If proposing only HACS SINs, you will need to be prepared for the CSP and PRC requirements. If proposing HACS SINs along with TDR Rule SINS, you will need to be prepared for the TDR requirements.

4. *Become familiar with the HACS SINs.* Carefully investigate the depth and breadth of requirements for each SIN. When preparing for the oral technical evaluation, inquire as to how the TEB intends to record the oral presentation, request that the evaluation be videotaped to preserve the record, and mark your information as proprietary, especially if briefing slides or presentation notes will be incorporated into the Government's contract file.

5. *Look to the clouds*. Commercial and governmental entities are both pushing towards cloud services. If participating in the market, important processes include FedRAMP certification and negotiating SLAs. Contractors should

prepare for SLA negotiations, which will most likely involve topics such as cessation of service, extraction of data, formats for the extracted data, sending the data to a new provider, and restarting key services on the new provider's platform.

6. *Remain cognizant of "ever-changing IT market conditions."* The Government is looking to the future of IT systems, and you should too. Attend industry day presentations relating to your company's lines of business, monitor Government websites for releases of potentially relevant business opportunities, and stay abreast of technology developments that affect your business.

7. *Decide if the GSA Schedule Program is right for you.* Carefully investigate the benefits of selling commercial products and services to the Government. Like Oracle, some may determine the risk is not worth the benefit. International companies should also examine the likelihood that their home-nation relationships may work against their commercial efforts.

8. *Follow IT budgets*. Monitor the progression of the MGT Act and strategize as to how your company might be able to take advantage of the Government's increasing investments in IT.

ENDNOTES:

[1]Federal Agencies' Reliance on Outdated and Unsupported Information Technology: A Ticking Time Bomb: Hearing Before the H. Comm. on Oversight & Gov't Reform, 114th Cong. 3 (May 25, 2016).

[2]Exec. Order No. 13794, "Establishment of the American Technology Council," 82 Fed. Reg. 20811 (Apr. 28, 2017); see 59 GC ¶ 140.

[3]Jessica A. Gunzel, "Tackling the Cyber Threat: The Impact of the DOD's 'Network Penetration Reporting and Contracting for Cloud Services' Rule on DOD Contractor Cybersecurity," 46 Pub. Cont. L.J. 687, 693 (Spring 2017).

[4]Jessica A. Gunzel, "Tackling the Cyber Threat: The Impact of the DOD's 'Network Penetration Reporting and Contracting for Cloud Services' Rule on DOD Contractor Cybersecurity," 46 Pub. Cont. L.J. 687, 693 (Spring 2017).

[5]See 41 U.S.C.A. § 3307 (requiring agencies to acquire commercial items to the maximum extent practicable to fulfill agency needs); FAR pt.12 (implementing the Government's preference for the acquisition of commercial items); FAR pt. 8 (encouraging use of commercial sources and GSA Schedules when agencies are unable to satisfy requirements for supplies and services from the mandatory sources, such as inventories of the requiring agency, excess from other agencies, Federal Prison Industries, Inc., AbilityOne, and wholesale supply sources).

[6]Federal Acquisition Institute, Using Multiple Award Schedules, Advanced Version Student Guide, Version 7.0, https://www.gsa.gov/portal/getMediaData?mediaId=220983 (last visited Aug. 2, 2017).

[7]GSA IT Schedule 70 description, https://www.gsa.gov/portal/content/104506 (last visited Aug. 2, 2017).

[8]GSA IT Schedule 70 description, https://www.gsa.gov/portal/content/104506 (last visited Aug. 2, 2017).

[9]Nat'l Contract Mgmt. Ass'n, Annual Review of Government Contracting, 2016 Edition, 41, http://www.ncmahq.org/docs/default-source/default-document-library/pdfs/exec16-book-annual-review-of-government-contracting_lowres.

[10]Nat'l Contract Mgmt. Ass'n, Annual Review of Government Contracting, 2016 Edition, 41, http://www.ncmahq.org/docs/default-source/default-document-library/pdfs/exec16-book-annual-review-of-government-contracting_lowres.

[11]Jessica A. Gunzel, "Tackling the Cyber Threat: The Impact of the DOD's 'Network Penetration Reporting and Contracting for Cloud Services' Rule on DOD Contractor Cybersecurity," 46 Pub. Cont. L.J. 687, 694 (Spring 2017) ("Government contractors play a key role in [the Government's] interconnected networks, making them a prime target for hackers looking for a backdoor into the nation's largest government agencies.").

[12]Federal Agencies' Reliance on Outdated and Unsupported Information Technology: A Ticking Time Bomb: Hearing Before the H. Comm. on Oversight & Gov't Reform, 114th Cong. 2 (May 25, 2016).

[13]Jason Miller, "The State of Federal Technology: 'A Crisis Bigger Than Y2k,' " Federal News Radio, Nov. 18, 2015, https://federalnewsradio.com/omb/2015/11/state-federal-technology-crisis-bigger-y2k/ (last visited July 18, 2017).

[14]Jason Miller, "The State of Federal Technology: 'A Crisis Bigger Than Y2k,' " Federal News Radio, Nov. 18, 2015, https://federalnewsradio.com/omb/2015/11/state-federal-technology-crisis-bigger-y2k/ (last visited July 18, 2017).

[15]See National Defense Authorization Act for Fiscal Year 2015, Pub. L. No. 113-291, §§ 831–837, 128 Stat. 3292, 3438 (2014); see also Management and Oversight of Federal Information Technology, Management.cio.gov, https://management.cio.gov (last visited July 18, 2017).

[16]Innovating With Less: Examining Efforts To Reform Information Technology Spending: Hearing Before the Subcomm. on Fed. Fin. Mgmt., Gov't Info., Fed. Servs. & Int'l Sec. of the S. Comm on Homeland Sec. & Govtl. Affairs, 112th Cong. 37 (May 24, 2012).

[17]Innovating With Less: Examining Efforts To Reform Information Technology Spending: Hearing Before the Subcomm. on Fed. Fin. Mgmt., Gov't Info., Fed. Servs. & Int'l Sec. of the S. Comm on Homeland Sec. & Govtl. Affairs, 112th Cong. 8 (May 24, 2012).

[18]GAO, GAO-15-290, 2015 GAO High Risk Series: An Update (2015).

[19]H. Comm. on Oversight & Gov't Reform, Modern-

izing Government Technology Act of 2017, H.R. Rep. No. 115-129, at 2 (May 17, 2017) (agencies reported over 550 unsupported systems or software applications; for example, some agencies reported still using Windows 3.1, which was last supported by Microsoft in 2001).

[20]H. Comm. on Oversight & Gov't Reform, Modernizing Government Technology Act of 2017, H.R. Rep. No. 115-129, at 5 (May 17, 2017).

[21]H. Comm. on Oversight & Gov't Reform, Modernizing Government Technology Act of 2017, H.R. Rep. No. 115-129, at 5 (May 17, 2017).

[22]Federal Agencies' Reliance on Outdated and Unsupported Information Technology: A Ticking Time Bomb: Hearing Before the H. Comm. on Oversight & Gov't Reform, 114th Cong. 1 (May 25, 2016) (emphasis added).

[23]Modernizing Government Technology Act of 2017, H.R. 2227, 115th Cong. (2017).

[24]H. Comm. on Oversight & Gov't Reform, Modernizing Government Technology Act of 2017, H.R. Rep. No. 115-129, at 10 (May 17, 2017).

[25]H. Comm. on Oversight & Gov't Reform, Modernizing Government Technology Act of 2017, H.R. Rep. No. 115-129, at 1–2 (May 17, 2017).

[26]Federal Agencies' Reliance on Outdated and Unsupported Information Technology: A Ticking Time Bomb: Hearing Before the H. Comm. on Oversight & Gov't Reform, 114th Cong. 1 (May 25, 2016).

[27]Federal Agencies' Reliance on Outdated and Unsupported Information Technology: A Ticking Time Bomb: Hearing Before the H. Comm. on Oversight & Gov't Reform, 114th Cong. 4 (May 25, 2016).

[28]Federal Agencies' Reliance on Outdated and Unsupported Information Technology: A Ticking Time Bomb: Hearing Before the H. Comm. on Oversight & Gov't Reform, 114th Cong. 87 (May 25, 2016).

[29]Federal Agencies' Reliance on Outdated and Unsupported Information Technology: A Ticking Time Bomb: Hearing Before the H. Comm. on Oversight & Gov't Reform, 114th Cong. 5 (May 25, 2016).

[30]Federal Agencies' Reliance on Outdated and Unsupported Information Technology: A Ticking Time Bomb: Hearing Before the H. Comm. on Oversight & Gov't Reform, 114th Cong. 5 (May 25, 2016).

[31]Darrell M. West & Joshua Bleiberg, Analyzing the Federal Government's Use of the Cloud, Brookings, Feb. 9, 2015, https://www.brookings.edu/blog/techtank/2015/02/09/analyzing-the-federal-governments-use-of-the-cloud/ (last visited July 18, 2017); Jason Miller, "The State of Federal Technology: 'A Crisis Bigger Than Y2k,' " Federal News Radio, Nov. 18, 2015, https://federalnewsradio.com/omb/2015/11/state-federal-technology-crisis-bigger-y2k/ (last visited July 18, 2017).

[32]Adam Mazmanian & Troy K. Schneider, "$500M IT Modernization Bill Passes House," FCW, May 17, 2017, https://fcw.com/articles/2017/05/17/mgt-act-passes-house.aspx (last visited July 18, 2017).

[33]Witnesses Call for IT Acquisition Reform, FITARA Implementation, 59 GC ¶ 89 (Apr. 5, 2017) (noting risk is especially large for small companies that fear "minor, unintentional mistakes may result in criminal charges, hefty finds, and damaged reputations").

[34]See GSA, Office of Inspector General, Office of Audits, Audit of Price Evaluations and Negotiations for Schedule 70 Contracts, Report No. A150022/Q/T/P16005, at 1 (Sept. 28, 2016); see also GSA eLibrary, Schedule List, https://www.gsaelibrary.gsa.gov/ElibMain/scheduleList.do (last visited July 18, 2017).

[35]See GSA IT Schedule 70, https://www.gsa.gov/portal/content/104506 (last visited July 18, 2017).

[36]See GSA IT Schedule 70, https://www.gsa.gov/portal/content/104506 (last visited July 18, 2017).

[37]See GSA eLibrary, Schedule Summary, Schedule 70: General Purpose Commercial Information Technology Equipment, Software, and Services, https://www.gsaelibrary.gsa.gov/ElibMain/scheduleSummary.do?scheduleNumber=70 (last visited July 18, 2017) (for example, SIN 132-40 "Cloud Computer Services" defines four subcategories: Infrastructure as a Service (Iaas), Software as a Service (SaaS), Email as a Service (EaaS), and Platform as a Service (PaaS)).

[38]GSA Schedule Sales Fiscal Year 2016, Federal Schedules, Inc., http://gsa.federalschedules.com/resources/gsa-schedule-sales-2016/ (last visited Aug. 30, 2017).

[39]General Purpose Commercial Information Technology Equipment, Software and Services, Solicitation No. FCIS-JB-980001-B, Refresh No. 43 (June 15, 2017).

[40]GSA, Office of Inspector General, Office of Audits, Audit of Price Evaluations and Negotiations for Schedule 70 Contracts, Report No. A150022/Q/T/P16005, at 1 (Sept. 28, 2016).

[41]Final Rule, Transactional Data Reporting, 81 Fed. Reg. 41104 (June 23, 2016).

[42]81 Fed. Reg. at 41108.

[43]GSAM (GSAR) 552.238-75, Price Reductions (May 2004).

[44]GSAM (GSAR) 552.238-75, Price Reductions (May 2004).

[45]GSAM (GSAR) 538.271(c) (May 2004).

[46]GSAM (GSAR) 552.238-75(c)(1), Price Reductions (JUL 2016) [48 C.F.R. § 552.238-75(c)(1)].

[47]GSAM (GSAR) 552.238-75(c)(2), Price Reductions (JUL 2016) [48 C.F.R. § 552.238-75(c)(2)].

[48]See, e.g., GSAM (GSAR) 552.238-75(d), Price Reductions (JUL 2016) [48 C.F.R. § 552.238-75(d)].

[49]81 Fed. Reg. 41104.

[50]81 Fed. Reg. 41104.

[51]81 Fed. Reg. 41104.

[52]81 Fed. Reg. 41104 (noting only Federal Supply Schedule (FSS) contracts managed by the Department of Veterans Affairs are exempt from the TDR Rule).

[53]81 Fed. Reg. at 41108.

[54]General Purpose Commercial Information Technology Equipment, Software and Services, Solicitation No. FCIS-JB-980001-B, Refresh No. 43 (June 15, 2017).

[55]General Purpose Commercial Information Technology Equipment, Software and Services, Solicitation No. FCIS-JB-980001-B, Refresh No. 43 (June 15, 2017).

[56]General Purpose Commercial Information Technology Equipment, Software and Services, Solicitation No. FCIS-JB-980001-B, Refresh No. 43 (June 15, 2017).

[57]General Purpose Commercial Information Technology Equipment, Software and Services, Solicitation No. FCIS-JB-980001-B, Refresh No. 43 (June 15, 2017).

[58]GAO, GAO-14-671T, Information Technology: Reform Initiatives Can Help Improve Efficiency and Effectiveness 3 (June 10, 2014) (noting "despite spending hundreds of billions on IT since 2000, the federal government has experienced failed IT projects and has achieved little of the productivity improvements that private industry has realized from IT").

[59]General Purpose Commercial Information Technology Equipment, Software and Services, Solicitation No. FCIS-JB-980001-B, Refresh No. 43, at xliii (June 15, 2017).

[60]General Purpose Commercial Information Technology Equipment, Software and Services, Solicitation No. FCIS-JB-980001-B, Refresh No. 43, at xliii (June 15, 2017).

[61]General Purpose Commercial Information Technology Equipment, Software and Services, Solicitation No. FCIS-JB-980001-B, Refresh No. 43, at xliii (June 15, 2017).

[62]General Purpose Commercial Information Technology Equipment, Software and Services, Solicitation No. FCIS-JB-980001-B, Refresh No. 43, at xliii (June 15, 2017).

[63]General Purpose Commercial Information Technology Equipment, Software and Services, Solicitation No. FCIS-JB-980001-B, Refresh No. 43, at xliii (June 15, 2017).

[64]General Purpose Commercial Information Technology Equipment, Software and Services, Solicitation No. FCIS-JB-980001-B, Refresh No. 43, at xliii (June 15, 2017).

[65]General Purpose Commercial Information Technology Equipment, Software and Services, Solicitation No. FCIS-JB-980001-B, Refresh No. 43, at xliii (June 15, 2017).

[66]See FAR 15.102(e).

[67]81 Fed. Reg. at 41105.

[68]81 Fed. Reg. at 41105.

[69]General Purpose Commercial Information Technology Equipment, Software and Services, Solicitation No. FCIS-JB-980001-B, Refresh No. 43, at 19, 21, 23, 25–26 (June 15, 2017) (noting new HACS SINs are not subject to TDR Rule, however, when proposing HACS SINs along with SINs to which the TDR Rule applies, the TDR Rule will apply to all SINs being offered).

[70]See GSAR 552.238-75 (JUL 2016) [48 C.F.R. § 552.238-75].

[71]Vivek Kundra, U.S. Chief Information Officer, Federal Cloud Computing Strategy (Feb. 8, 2011).

[72]Vivek Kundra, U.S. Chief Information Officer, Federal Cloud Computing Strategy 6 (Feb. 8, 2011).

[73]Vivek Kundra, U.S. Chief Information Officer, Federal Cloud Computing Strategy 6 (Feb. 8, 2011) (finding "NASA Nebula, through a community cloud, gives researchers access to IT services relatively inexpensively in minutes").

[74]GAO, GAO-16-325, Cloud Computing: Agencies Need To Incorporate Key Practices To Ensure Effective Performance 1 (Apr. 7, 2016).

[75]Louis Columbus, "Roundup of Cloud Computing Forecasts, 2017," Forbes, Apr. 2017, https://www.forbes.com/sites/louiscolumbus/2017/04/29/roundup-of-cloud-computing-forecasts-2017/#5d020e9431e8 (last visited July 18, 2017).

[76]Department of Commerce, Int'l Trade Admin., 2016 Top Markets Report: Cloud Computing (Apr. 2016) (noting that by 2020, "no-cloud" policies may be as rare as "no-internet" policies are today).

[77]Alexander Rossino, "Federal Cloud Contracting in Fiscal Year 2016," GovWin, Deltek, Feb. 14, 2017, https://iq.govwin.com/neo/marketAnalysis/view/1869?researchTypeId=1 (last visited Aug. 2, 2017).

[78]Alexander Rossino, "Federal Agency Cloud Procurement Trends," GovWin, Deltek, Apr. 19, 2017, https://iq.govwin.com/neo/marketAnalysis/view/2051?researchTypeId=1 (last visited Aug. 1, 2017) (noting that while contract awards increased, actual spending on awarded contracts decreased from fiscal year 2014 to fiscal year 2016, yet, factors accounting for the drop-off are unclear; meanwhile, data seem to confirm that agency use of GSA Schedule 70 is increasing in 2017).

[79]Mary Davie, "Schedule 70 Cloud Special Item Number (SIN), the Cloud One-Stop Shop," GSA Great Government Through Technology, May 18, 2015, https://gsablogs.gsa.gov/technology/2015/05/18/schedule-70-cloud-special-item-number-sin-the-cloud-one-stop-shop/ (last visited Aug. 2, 2017).

[80]NIST Special Publication 500-293, U.S. Government Cloud Computing Technology Roadmap Volume I: High-Priority Requirements To Further USG Agency Cloud Computing Adoption 7 (Oct. 2014).

[81]NIST Special Publication 500-293, U.S. Government Cloud Computing Technology Roadmap Volume I: High-Priority Requirements To Further USG Agency Cloud Computing Adoption 15 (Oct. 2014).

[82]General Purpose Commercial Information Technology Equipment, Software and Services, Solicitation No. FCIS-JB-980001-B, Refresh No. 43, at 16 (June 15, 2017) (unless SIN 132-40 is offered with other SINs to which TDR Rule applies).

[83]General Purpose Commercial Information Technology Equipment, Software and Services, Solicitation No. FCIS-JB-980001-B, Refresh No. 43, at 16 (June 15, 2017) (unless SIN 132-40 is offered with other SINs to which TDR Rule applies).

[84]GAO, GAO-16-325, Cloud Computing: Agencies Need To Incorporate Key Practices To Ensure Effective Performance 12 (Apr. 7, 2016).

[85]GAO, GAO-16-325, Cloud Computing: Agencies

Need To Incorporate Key Practices To Ensure Effective Performance 12 (Apr. 7, 2016).

[86]NIST Special Publication 500-293, U.S. Government Cloud Computing Technology Roadmap Volume I: High-Priority Requirements To Further USG Agency Cloud Computing Adoption, at 7, 15 (Oct. 2014).

[87]44 U.S.C.A. §§ 3541–3549.

[88]GSA, White Paper: Best Practices for Effective Cloud Computing Services Procurement Within the Federal Government 6 (Jan. 2016).

[89]GSA FedRAMP, https://www.fedramp.gov (last visited July 18, 2017).

[90]GSA FedRAMP, FedRAMP Security Assessment Framework, Version 2.1, at 9–19 (Dec. 4, 2015) (contractors document controls and details of implementation in various FEDRAMP forms and templates (e.g., developing a System Security Plan)).

[91]Coalfire, Securing Your Cloud Solutions: Research and Analysis on Meeting FedRAMP / Government Standards 16, https://www.coalfire.com/Resources/FedRAMP-Market-Report/Asset-Delivery (last visited Aug. 2, 2017).

[92]Coalfire, Securing Your Cloud Solutions: Research and Analysis on Meeting FedRAMP / Government Standards 16, https://www.coalfire.com/Resources/FedRAMP-Market-Report/Asset-Delivery (last visited Aug. 2, 2017). The timelines can be affected by whether a CSP chooses to be authorized by the Joint Authorization Board (JAB), which provides Government-wide access, or by a specific agency

[93]Coalfire, Securing Your Cloud Solutions: Research and Analysis on Meeting FedRAMP / Government Standards 20, https://www.coalfire.com/Resources/FedRAMP-Market-Report/Asset-Delivery (last visited Aug. 2, 2017).

[94]Matt Goodrich, "How Much Does It Cost To Go Through FedRAMP?," https://www.fedramp.gov/how-much-does-it-cost-to-go-through-fedramp/ (last visited Aug 2, 2017)

[95]GSA, White Paper: Best Practices for Effective Cloud Computing Services Procurement Within the Federal Government 8 (Jan. 2016).

[96]GSA, White Paper: Best Practices for Effective Cloud Computing Services Procurement Within the Federal Government 8 (Jan. 2016).

[97]GSA, Office of Inspector General, Office of Audits, Audit of Price Evaluations and Negotiations for Schedule 70 Contracts, Report No. A150022/Q/T/P16005 (Sept. 28, 2016).

[98]GSA, Office of Inspector General, Office of Audits, Audit of Price Evaluations and Negotiations for Schedule 70 Contracts, Report No. A150022/Q/T/P16005, at 3 (Sept. 28, 2016).

[99]GSA, Office of Inspector General, Office of Audits, Audit of Price Evaluations and Negotiations for Schedule 70 Contracts, Report No. A150022/Q/T/P16005, at 4 (Sept. 28, 2016).

[100]GSA, Office of Inspector General, Office of Audits, Audit of Price Evaluations and Negotiations for Schedule 70 Contracts, Report No. A150022/Q/T/P16005, at 4, 6 (Sept. 28, 2016).

[101]GSA, Office of Inspector General, Office of Audits, Audit of Price Evaluations and Negotiations for Schedule 70 Contracts, Report No. A150022/Q/T/P16005, app. B-2 (Sept. 28, 2016).

[102]Federal Agencies' Reliance on Outdated and Unsupported Information Technology: A Ticking Time Bomb: Hearing Before the H. Comm. on Oversight & Gov't Reform, 114th Cong. 7 (May 25, 2016).

[103]Apple, Apple Security Updates, https://support.apple.com/en-us/HT201222 (last visited July 18, 2017) (noting 150 updates have been released for various Apple products from January 2015 through May 2017).

[104]Jason Miller, "Oracle To Leave GSA Schedule: A Signal of Broader Change," Federal News Radio, Sept. 16, 2016, https://federalnewsradio.com/reporters-notebook-jason-miller/2016/09/oracle-leave-gsa-schedule-signal-broader-change/ (last visited July 18, 2017); see also Matthew Weigelt, "GSA's Oracle Cancellation Still a Mystery," FCW, Apr. 23, 2012, https://fcw.com/articles/2012/04/23/reaction-gsa-oracle-cancellation.aspx (last visited July 18, 2017) (noting turmoil between GSA and Oracle regarding the GSA Schedule 70 goes back several years).

[105]Jason Miller, "Oracle To Leave GSA Schedule: A Signal of Broader Change," Federal News Radio, Sept. 16, 2016, https://federalnewsradio.com/reporters-notebook-jason-miller/2016/09/oracle-leave-gsa-schedule-signal-broader-change/ (last visited July 18, 2017).

[106]U.S. Dep't of Justice, Office of Public Affairs, Oracle Agrees To Pay U.S. $199.5 Million To Resolve False Claims Act Lawsuit (Oct. 6, 2011), https://www.justice.gov/opa/pr/oracle-agrees-pay-us-1995-million-resolve-false-claims-act-lawsuit (last visited July 18, 2017).

[107]U.S. Dep't of Justice, Office of Public Affairs, VMWare and Carahsoft Agree To Pay $75.5 Million To Settle Claims that They Concealed Commercial Pricing and Overcharged the Government (June 30, 2015), https://www.justice.gov/opa/pr/vmware-and-carahsoft-agree-pay-755-million-settle-claims-they-concealed-commercial-pricing (last visited July 18, 2017).

[108]Morgan Chalfant, "Trump Admin Removes Russian Cyber Firm from Approved List," The Hill, July 12, 2017, http://thehill.com/policy/cybersecurity/341665-trump-admin-removes-russian-cyber-firm-from-approved-list (last visited July 18, 2017); Dustin Volz, "Exclusive: Congress Asks U.S. Agencies for Kaspersky Lab Cyber Documents," Reuters, July 28, 2017, https://www.reuters.com/article/us-usa-kasperskylab-probe-idUSKBN1AD2H0 (last visited Aug. 2, 2017).

[109]Morgan Chalfant, "Trump Admin Removes Russian Cyber Firm from Approved List," The Hill, July 12, 2017, http://thehill.com/policy/cybersecurity/341665-trump-admin-removes-russian-cyber-firm-from-approved-list (last visited July 18, 2017); Dustin Volz, "Exclusive: Congress Asks U.S. Agencies for Kaspersky Lab Cyber Documents," Reuters, July 28, 2017, https://www.reuters.com/article/us-u

sa-kasperskylab-probe-idUSKBN1AD2H0 (last visited Aug. 2, 2017); see also Jordan Robertson & Michael Riley, "Kaspersky Lab Has Been Working With Russian Intelligence," Bloomberg Businessweek, July 11, 2017, https://www.bloomberg.com/news/articles/2017-07-11/kaspersky-lab-has-been-working-with-russian-intelligence (last visited July 18, 2017).

[110]Joe Uchill, "Overnight Cybersecurity: Trump Jr.'s Email Bombshell / Five Questions Raised by Emails / Committees Jockey To Question Trump Jr. / Officials Weigh Government Ban on Russian Security Software," The Hill, July 11, 2017, http://thehill.com/policy/cybersecurity/overnights/341518-overnight-cybersecurity-trump-jr-email-bombshell-trump-sr-to (last visited July 18, 2017).

[111]Mike Levine, "Trump Administration Pulls Russian Cyber Firm From Government-Approved List," ABC News, July 12, 2017, http://abcnews.go.com/US/trump-administration-pulls-russian-cyber-firm-government-approved/story?id=48578556 (last visited July 18, 2017).

[112]Sergei Karpukhin, "Kaspersky Lab Says It Has Become Pawn in U.S.-Russia Geopolitical Game," Reuters, July 11, 2017, http://www.reuters.com/article/us-usa-kasperskylab-russia-statement-idUSKBN19X0PG (last visited July 18, 2017).

[113]System for Award Management, SAM.gov.

[114]S. 1519, § 160B, 115th Cong. (2017); see Mike Levine, "Trump Administration Pulls Russian Cyber Firm From Government-Approved List," ABC News, July 12, 2017, http://abcnews.go.com/US/trump-administration-pulls-russian-cyber-firm-government-approved/story?id=48578556 (last visited July 18, 2017) (reporting Senator Shaheen has taken legislative steps to bar the U.S. military from using Kaspersky Lab products); Ramona Adams, Senate Panel's 2018 NDAA Would Reorganize DOD CIO Office, Ban Russian Anti-Virus Software, July 3, 2017, http://www.executivegov.com/2017/07/senates-2018-ndaa-would-ban-foreign-anti-virus-software-reorganize-dod-cio-role/ (last visited Aug. 2, 2017).

[115]DHS Statement on the Issuance of Binding Operational Directive 17-01 (Sept. 13, 2017), https://www.dhs.gov/news/2017/09/13/dhs-statement-issuance-binding-operational-directive-17-01 (last visited Sept. 19, 2017).

[116]"Confusion Hits Consumer Market Over US Ban of Kaspersky," CNBC, Sept. 14, 2017, https://www.cnbc.com/2017/09/14/confusion-hits-consumer-market-over-us-ban-of-kaspersky.html (last visited Sept. 19, 2017).

[117]Philip Chertoff, "Why The US Government Shouldn't Ban Kaspersky Security Software," Wired Opinion, https://www.wired.com/story/why-the-us-government-shouldnt-ban-kaspersky-security-software/ (last visited Sept. 19, 2017).

NOTES:

BRIEFING PAPERS