Improving risk management in departmnet of defense government contracting

IMPROVING RISK MANAGEMENT IN DEPARTMNET OF DEFENSE GOVERNMENT CONTRACTING: ESTABLISHING A CYBER SECURITY GRANT PROGRAM

I. INTRODUCTION

In 2013, Target experienced a massive data breach[1]which left up to 70 million customer’s personal information vulnerable to hackers.[2]Information such as personal phone numbers, addresses, and credit card information was compromised after a phishing email allowed a bot access to company log in credentials.[3]Not only was the CEO of Target forced to resign after the incident[4]—a first for a major company suffering a data breach—but the company became the subject of multistate litigation stemming from its failure to protect customer data.[5]

Interestingly, the hackers did not gain access to Target's systems directly, but through a small vendor it contracted with for HVAC services, Fazio Mechanical Services Inc.[6]A third-party vendor, Fazio's only defense against malicious software was the free version of Malwarebytes Anti-Malware.[7]The free version does not scan for real-time threats and was not even licensed for corporate use.[8]Once Fazio's vendor credentials were obtained, hackers used malware to access billing and invoicing systems, and Target's own software spread the malware to virtually all of Target's Point of Sale systems.[9]

Target's vulnerability through a small, third party vendor which was not even involved in its billing systems is an illustrative example of how targets can be compromised through a small business. Criminals are increasingly using small businesses as a backdoor into larger organization, as their cybersecurity systems tend not to be as sophisticated.[10]Smaller businesses are less likely to have thorough cybersecurity systems in place, and are more likely to be unprepared for the costs of losses when a data breach occurs.[11]For small government contractors who deal with sensitive information crucial to national security, the stakes are even higher.

In 2011, a Chinese citizen who was living in Canada hacked into Lockheed Martin's networks and gained access to info about several military aircraft.[12]Given other recent breaches of government computer systems[13], the executive branch has recognized the importance of strict cybersecurity compliance as a cornerstone of national security. The Federal Modernization Security Act (FISMA) of 2002, which was amended in 2014, was passed by Congress in order to protect defined categories of information and information systems in order to provide a “ comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets” and to “ provide for development and maintenance of minimum controls required to protect Federal information and information systems.”[14]

Although small government contractors have limited resources, they are still subject to the same cybersecurity requirements that larger contractors with more resources must abide.[15]Recently, the Department of Defense has employed the Defense Federal Acquisition Regulation Supplement (DFARS), to institute uniform cybersecurity requirements for all covered DOD contractors and subcontractors, regardless of size.[16]

Additionally, the DOD has specified the inclusion of small businesses in its federal contracting process in order to support local economic development, offer opportunities to disadvantaged socio-economic groups, and gain access to new ideas that small businesses provide.[17]The DoD aimed to award at least 22 percent of small-business-eligible prime-contract spending to small businesses in fiscal year 2017.[18]

The impetus of the Small Business Act of 1953, was to establish the Small Business Administration, and to “ aid, counsel, assist and protect, insofar as is possible, the interests of small business concerns.”[19]Included in the SBA’s mandate was the assurance that it would give small businesses a “ fair proportion”; of government contracts and sales of surplus property.[20]In short, the DOD is required to ensure that a significant portion of its contracts are awarded each year to small businesses, all of whom must comply with the DFARS cybersecurity standards. This represents a significant challenge for both the government and small government contractors, as the percentage of federal contract dollars set aside for small businesses is likely to grow.[21]

“ One of the major impediments to changing how cybersecurity is addressed in Federal acquisitions is the differing priorities of cyber risk management and the Federal Acquisition System. The Acquisition Workforce is required to fulfill numerous, sometimes conflicting, policy goals through their work, and cybersecurity is but one of several competing priorities in any given acquisition.”[22]The government must attempt to allocate its target amount of contracts to small businesses while making sure to not compromise its cybersecurity goals at the same time. For small businesses, they must strategically allocate limited resources while remaining in step with the myriad and increasing security goals mandated by the government. The Director of the Kansas University Small Business Development Center, stated “ America’s small businesses have not made a dedicated effort to build cybersecurity into their P&Ls [Profits and Losses]. That lack of funding on the small business side has been noticed by hackers. Small businesses are the backdoor into big business. A Fortune 500 company or the U. S. Government can throw as many dollars as they want at the threat of a cybersecurity breach, but all it takes is one small business vendor to take down the whole thing.”[23]

Although several government entities have implemented programs to assist small businesses which contract with the DOD by focusing on outreach and education efforts[24], they have fallen short. These attempts typically centered more on creating broad initiatives and policy advice than concrete solutions. These programs are no doubt helpful, but they have not targeted the underlying issue which small government contractors face when attempting to comply with cybersecurity mandates—allocation of limited financial resources. This note argues that congress should pass legislation giving the Small Business Administration the authority to establish a federally funded grant program for cyber security in which eligible small business defense contractors will be directly provided with funds which can be used for internal cyber security improvements. Congress should give the SBA authority to make cybersecurity grants to assist small businesses with Department of Defense contracts in order to meet their DFARS and NIST 800-171 SP cybersecurity requirements. This will help the DOD achieve its cybersecurity objectives, which include expanding cyber cooperation with the private sector, and securing DOD information on non-DOD owned networks.[25]Putting the power of compliance in the hands of individual businesses who are most equipped to know where to allocate their resources would help alleviate inefficiency and the funding of duplicate resources.

Part II of this note lays out a brief overview of the DOD’s current cybersecurity mandates, providing a look at the origins of the DFARS cybersecurity initiatives and the Department of Commerce’s National Institute of Standards and Technology, and their increasing emphasis on standardization among all contractors. It will also take a look at two recent cases in which cybersecurity was used as an evaluation criteria by agencies. Part III will analyze ongoing efforts to ameliorate the unique difficulties faced by small federal contractors. It will then argue that establishing a cyber security grant program for eligible small government contractors who are subject to DFARS requirements would assist individual contractors in completing the three main tasks of DFARS 252. 294-7012 and the NIST SP 800-171—figuring out what information is covered, implementing cyber incidence reporting requirements, and developing a security system and plan of action.

II. Background: The Current Cybersecurity Regime

The Department of Defense protects sensitive information held by contractors through rules known as the " Federal Acquisition Regulation" (FAR), and the " Defense Federal Acquisition Regulation Supplement" (DFARS) which provides DOD specific acquisition regulations for the procurement process[26]. In 2016 the DFARS supplement published a final ruling [27] , which was clarified by the DOD's Frequently Asked Questions (Network Penetration Reporting and Contracting for Cloud Services FAQ).   As of Dec. 31 st , 2017, all Department of Defense (DoD) contractors that store, process, or transmit covered defense information (CDI) are subject to DFAR 252. 204-7012.[28]This clause requires that all contractors implement the security requirements in the NIST SP 800-171 standards for cybersecurity.[29]

Cybersecurity regulations which govern government contracts require increasing levels of compliance across multiple categories in order for firms to remain competitive in the bidding process, placing placed major emphasis on requiring government contractors to adhere to stringent cybersecurity rules. The DOD also issued feedback on how a small business could approach meeting the requirements of NIST SP 800-171. It stated that most requirements could be met by instituting policy/process changes or by adjusting the configuration of existing IT systems. [30]

While the FAR rules create a baseline of protection,[31]the final DFARS rule applies to all contractors and subcontractors which safeguard “ covered defense information” (CDI) residing in or transiting through “ covered contractor information systems”[32]. Previously, this rule only applied to “ cleared” and “ operationally critical” contractors. The following highlights additional important changes to the final DFARS ruling.

Coverage

The final DFARS rule expands coverage.[33]Unless a solicitation or contract is for the acquisition of COTS items[34], the clause must be required in all subcontracts for any “ operationally critical support”[35]provided, or if performance of the contract will require “ covered defense information.”[36]The old clause only applied to “ cleared” and “ operationally critical” contractors as specified in the 2013 and 2015 National Defense Authorization Act (NDAA).

Incidence reporting :

In addition, the new DFARS requires a contractor to report any cyber “ incidents” within 72 hours of discovery.[37]Some public comments complained that reporting within 72 hours was too burdensome because it was highly likely that they have all the information required by the clause within 72 hours. But the DOD has issued clarification that contractors should report “ whatever information is available to the DIBNet portal[38]within 72 hours of discovery. When more information becomes available, the contractor/subcontractor should submit a follow-on report with the added information.”[39]

Sharing of malware

When malicious Malware is discovered, it should be submitted to the DoD Cyber Crime Center “ in accordance with instructions provided by DC3 or the Contracting Officer. Do not send the malicious software to the Contracting Officer.”[40]Previously, contractors were required to “ submit the malicious software in accordance with instructions provided by the Contracting Officer”.[41]

Contractor network access

The DoD’s is now allowed access to contractor information and systems in the event of a cyber incident.[42]Although this has been criticized as allowing the government to have too much access to contractor information, the DoD has stated in commentary to the rule that access is limited to “ determining if DoD information was successfully exfiltrated… and, if so, what information was exfiltrated.”[43]

Subcontractor Reporting Obligations

When a subcontractor provides operationally critical support, or the execution of the contract involves covered defense information, they must report the cyber incident to the DOD.[44]Additionally, the subcontractor must notify the prime when requesting a divergence from the NIST SP 800-171 security control requirements.[45]

Cloud service providers

Cloud Service Providers that are being operated on behalf of the government, and those that are not, receive different treatments. Cloud Service Providers which operate on behalf of the government must comply with the Cloud Computing Security Requirements Guide (SRG), also known as the FedRAMP+[46]rules. Otherwise, Cloud Service Providers must meet the FedRAMP Moderate baseline[47]requirements and comply with the Final Rule's " cyber incident reporting, malicious software, media preservation and protection, access to additional information and equipment necessary for forensic analysis, and cyber incident damage assessment".[48]

Most covered contractor information systems are not operated on behalf of the government and must abide by the security requirements in NIST SP 800-171, " Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations".[49]The National Institute of Standards and Technology (NIST) is charged with " developing information security standards and guidelines, including minimum requirements for federal information systems".[50]NIST developed this publication to further its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014.[51]The requirements contractors adhere to in the NIST SP 800-171 are complex and expansive.

As an example of the technical complexity contractors must grapple with, NIST SP 800-171 details 14 different " Families" of requirements for protecting the confidentiality of information: Access Control; Awareness and Training; Audit and Accountability; Configuration Management; Identification and Authentication; Incident Response; Maintenance; Media Protection; Personnel Security; Physical Protection; Risk Assessment; Security Assessment; System and Communications Protection; and System and Information Integrity.[52]Each of these requirements need to be “ applied to the nonfederal organization’s internal systems processing, storing, or transmitting CUI”.[53]

The measures needed to implement the requirements of the NIST SP 800-171 can be quite burdensome and may require continuous monitoring efforts.[54]Compliance is demonstrated through having a robust system security plan alongside a plan of action describing how any non-compliant practices can be rectified.[55]Any contractors new to the arena may acquire significant upfront costs that make it all but impracticable to thoroughly comply with all the guidelines set forth in the NIST publication. This is important for small businesses, which may find it challenging to comply with so many requirements, especially if their previous contracts with the DOD were limited. Some contractors may even decide that compliance is too costly and are willing to risk non-compliance.

However, noncompliance is not an option for government contractors looking to mitigate their risks and avoid potential negative outcomes from bid protestors. DFARS 252. 204-7008 provides that “[b]y submission of this offer, the Offeror represents that it will implement the security requirements specified by [NIST SP 800-171] . . . that are in effect at the time the solicitation is issued or as authorized by the contracting officer not later than December 31, 2017."[56]

However, there is some relief for contractors who feel they cannot meet the full burden of the NIST up-front. In some cases, contractors are permitted to ask for deviances from the requirements after they have been awarded the contract if they believe they can offer an " equally effective security measure in its place".[57]Contractors can begin this process by submitting a written request to the Contracting Officer which will then be considered by the DOD Chief Information Officer.[58]Contractors can also request a pre-award adjudication[59]if they feel a security requirement is not consistent with the requirements of the contract, or they have " an alternative, but equally effective security measure that may be implemented in its place".[60]

B. Cybersecurity as an Evaluation Criteria: *Syneren* and *IP Keys Tech*

Revision 1 of the NIST SP 800-171 states that agencies have the right to inspect any system security plans (SSP) and plan of actions and milestones (POAM) from government contractors.[61]Additionally, these SSP and POAM may be used by agencies to as evaluation criteria in awarding contracts which require the processing, storing, or transmission of Covered Defense Information (CDI).[62]The DOD can determine " whether it is an acceptable or unacceptable risk to process, store, or transmit" CDI on any individual's system.[63]Two recent cases help illustrate how cybersecurity has been used as an evaluation criteria for contractors.

Syneren Tech Corp.

On Feb. 10, 2016, The Department of the Navy issued an RFP asking contractors to provide support to the Sea Warriors Program[64]for the " design, development, implementation and sustainment of IT systems and software supporting enterprise business services, personnel and pay, position management, recruiting and accessions, workforce development, and distance support." The solicitation was an indefinite-delivery, indefinite-quantity (IDIQ) contract and had the following five evaluation factors:

"(1) software development experience; (2) first sample task (net recruiting placement and alignment (NetRPA)[65]development/modernization); (3) second sample task (Department of Defense (DOD) IT portfolio repository/database management system sustainment); (4) cost; and (5) past performance."[66]

Because the contract had work that was to be performed at a government site in New Orleans, Louisiana, and involved Department of Defense and Department of the Navy information, the winning contractor had to comply with both DOD and Navy cybersecurity requirements.[67]Among them was the requirement that some of the software in use by the contractor meet certain accreditation standards.[68]In addition, it was the bidder's responsibility to clearly show its ability to satisfy these requirements.[69]

The proposal received 20 offers, including Syneren's.[70]Unfortunately, the software it proposed to use for the second evaluation factor, the Net Recruiting Placement and Alignment

(NetRPA), was not accredited for use by the Navy.[71]Additionally, Syneren offered no explanation of how it planned to become accredited.[72]Syneren's proposal was ultimately rejected and it subsequently filed a protest of the Navy’s decision.[73]Syneren protested that the Navy should not have evaluated its proposal as unacceptable for its use of an unaccredited software.[74]In reference to its rejection, Syneren asserted that “ There was no requirement for Syneren to address the accreditation process prior to award or to explain in its proposal how it would attain accreditation.”[75]The GAO ultimately rejected this argument and sided with the Navy.[76]The decision explained “ because performance will occur in a government facility and involve DOD and Navy data, the solicitation provided that the contractor’s system must comply with multiple cybersecurity requirements… more importantly, that Syneren’s proposal failed to address in any meaningful way how compliance would be achieved”.[77]The Navy concluded that “ Syneren’s proposal failed to reflect an adequate understanding of both the time and costs associated with Syneren’s successful contract performance, specifically including compliance with the solicitation’s cybersecurity requirements.”[78]In short, Syneren was on notice of the Navy’s cybersecurity requirements, and the Navy did not believe the Syneren fully understood what steps it needed to take to perform the work in the solicitation in order to remain complaint within the agency’s cybersecurity requirements.[79]It is likely that agencies will increasingly look to incorporate cybersecurity[80]into their bidding process, and that those who fail to do so may be disqualified if they cannot meet the applicable qualifications.

IPKeys Tech.

Another decision by the GAO highlights the use of cybersecurity as a technical evaluation factor. IPKeys Technologies, LLC, a small business, challenged the Defense Information Systems Agency's (DISA) evaluation of By Light Professional IT Services, Inc.'s

cybersecurity solution.[81]By Light, also a small business, submitted a proposal which was higher-priced than that of IPKeys.[82]The RFP was for " engineering, transition, implementation, sustainment, and cybersecurity monitoring support services for DISA's Global Video Service (GVS)."[83]

The request only considered two evaluation factors, "(1) technical/management approach; and (2) cost", with the technical/management approach to be more important than the cost, and cost to be evaluated for completeness, reasonableness, and realism.[84]As to the technical/management approach factor, it was to be evaluated by four equally weighted factors.[85]

---

[1]https://www. usatoday. com/story/money/2017/05/23/target-pay-185m-2013-data-breach-affected-consumers/102063932/

[2]https://www. usatoday. com/story/money/business/2014/01/10/target-customers-data-breach/4404467/

[3] *See* Natalie Gagliordi, *The Target breach, twoyears later,* ZDNET (Nov. 27, 2015),

http://www. zdnet. conarticle/the-target-breach-two-years-later.

[4]Id.

[5]The settlement requires Target to improve sata security, pay a monetary penalty, and provide credit monitoring for impacted consumers.

Agreement With 47 States And D. C. Represents Largest Multistate Data Breach Settlement To Date.

See A. G. Schneiderman Announces $18. 5 Million Multi-State Settlement With Target Corporation Over 2013 Data Breach, https://ag. ny. gov/press-release/ag-schneiderman-announces-185-million-multi-state-settlement-target-corporation-over

[6]Target's Heating and Refrigeration Company Gave Hackers the Key to Customer Data, Lily Hay Newman Feb 6, 2014.

https://slate. com/technology/2014/02/the-target-hackers-got-credentials-from-hvac-and-refrigeration-company-fazio-mechanical-services. html

[7] *See* Brian Krebs, *Email Attack on Vendor Set Up Breach at Target,* Krebs On Security (Feb. 14, 2014), http://krebsonsecuritycor/2014/02/email-attack-on-vendor-set-up-breach-at-target.

[8]Id.

[9] *See* N. Eric Weiss and Rena S. Miller, The Target and Other Financial Data Breaches: Frequently Asked Questions, Congressional Research Service (Feb. 4, 2015), https://www. fas. org/sgp/crs/misc/R43496. pdf. at 4.

[10]PwC, *Managing cyber risks in an interconnected world: Key findings from The Global State of Information Security Survey 2015* , 8 (Sept. 30, 2014) (stating " Small firms often consider themselves too insignificant to attract threat actors—a dangerous misperception. It's also important to note that sophisticated adversaries often target small and medium-size companies as a means to gain a foothold on the interconnected business ecosystems of larger organizations with which they partner. This dangerous reality is compounded by the fact that big companies often make little effort to monitor the security of their partners, suppliers, and supply chains.

"), *available at* https://www. pwc. com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015. pdf.

[11]The average cost due to damage or theft of IT assets and infrastructure increased from $879, 582 to $1, 027, 053. The average cost due to disruption to normal operations increased from $955, 429 to $1, 207, 965. Ponemon Institute, *The State of Cybersecurity in Small and Medium Businesses 2017* (2017) at 2, *available at* https://keepersecurity. com/2017-State-Cybersecurity-Small-Medium-Businesses-SMB. html.

[12]https://news. vice. com/en_us/article/kz9xgn/man-who-sold-f-35-secrets-to-china-pleads-guilty

[13]Julie Hirschfeld Davis, " Hacking of Government Computers Exposed 21. 5 Million People," N. Y. Times, July 9, 2015.

[14]See E-Government Act of 2002. Pub. L. No. 107-347, § 301, 116 Stat. 2899, 2946 (2002).

[15]New DFARS Regulation = New Standard for Cybersecurity? American Institute of Aeronautics and Astronautics. https://www. aiaa. org/januaryprotocol/

[16]Id. The DFARS Rule previously applied to only “ cleared” and “ operationally critical” contractors as specified in the 2013 and 2015 National Defense Authorization Act (NDAA).

[17]Contracting Guide. https://www. sba. gov/federal-contracting/contracting-guide

[18]Department of the Navy Office of Small Business Programs. DOD FY17 Small Business Goals. http://donosbp. navylive. dodlive. mil/2017/05/25/dod-fy17-small-business-goals/

[19]About the SBA. https://www. sba. gov/about-sba/what-we-do/history

[20]Id.

[21]In 2017, U. S. Rep Sam Graves, Head of the House Small Business Committee called for the Federal government to award 25 percent of its prime contract work to small businesses, 2 percent more than the current goal of 23 percent. *Graves Wants to Increase the Percentage of Federal Contracts Awarded to Small Business* . Nov. 1 2017. Joshua Sophy. https://smallbiztrends. com/2014/03/graves-more-government-contracts-for-small-businesses. html

[22](Improving Cybersecurity and Resilience through Acquisition: Final Report of GSA and DOD). https://www. gsa. gov/cdnstatic/IMPROVING_CYBERSECURITY_AND_RESILIENCE_THROUGH_ACQUISITION. pdf

[23]Government Contractor Cybersecurity: Q&A with the Director of the Kansas SBDC Cybersecurity Center

Oct. 25, 2017. Matthe Moriarty. Interview with Brian S. Dennis. http://smallgovcon. com/uncategorized/government-contractor-cybersecurity-qa-with-the-director-of-the-kansas-sbdc-cybersecurity-center/

[24]https://www. gao. gov/assets/680/672725. pdf. GAO Highlights. Opportunities Exist for DOD to Share Cybersecurity Resources with Small Businesses. Sept. 2015. Selected Examples of Cybersecurity Resources GAO Identified as Available to Defense Small Businesses include Cybersecurity E-Learning Courses, which are “ Online courses related to cybersecurity topics such as risk management and phishing—that is, social engineering that uses authentic looking, but fake, e-mails to request information from users or direct them to a fake website that requests information.”

[25]The 2018 Department of Defense (DoD) Cyber Strategy articulates how the Department will implement the priorities of the National Defense Strategy in and through cyberspace. 2018 DoD Cyber Strategy and Cyber Posture Review *Sharpening our Competitive Edge in Cyberspace* . https://media. defense. gov/2018/Sep/18/2002041659/-1/-1/1/Factsheet_for_Strategy_and_CPR_FINAL. pdf

[26]DFARS 252. 201. 101 https://www. acq. osd. mil/dpap/dars/dfars/html/current/201_1. htm

[27]81 FR 72986.

[28]252. 204-7012(b)(ii)(a).

[29]NIST is the National Institute of Standards and Technology. NIST Special Publication 800-171 “ Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations” (available via the internet at http://dx. doi. org/10. 6028/NIST. SP. 800-171) must go into effect at the time the solicitation is issued or as authorized by the Contracting Officer.

[30]https://www. acq. osd. mil/dpap/pdi/docs/FAQs_Network_Penetration_Reporting_and_Contracting_for_Cloud_Services_(01-27-2017). pdf at p. 13

[31]81 Fed. Reg. 30, 439 (May 16, 2016).

[32]Covered contractor information systems are any unclassified information systems owned, or operated by or for, a contractor and that process, store, or transmit covered defense information. DFARS 252. 204-7012(a). Contractors must provide “ adequate security” on any contractor information systems which are covered. This means that protective measurements must be taken that are proportionate to the likelihood of risk that the information will be compromised. There are two types of covered information systems, and each require compliance with different security requirements: those that

are part of an IT system operated on behalf of the government, and those which are not operated on behalf of the government.

[33]DFARS 204. 7301, 252. 204-7012(a).

[34]DFARS 204. 7304(c)

[35]Operationally critical support means " supplies or services designated by the government as critical for airlift, sealift, intermodal transportation services, or logistical support that is essential to mobilization, deployment, or sustainment of the Armed Forces in a contingency operation". DFARS 252. 204-7012(a)

[36]DFARS 252. 204-7012(m) " Covered defense information" is " unclassified controlled technical information or other information, as described in the Controlled Unclassified Information (CUI) Registry at http://www. archives. gov/cui/registry/c ategory-list. html, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Governmentwide policies, and is (1) Marked or otherwise identified in the contract, task or- der, or delivery order and provided to the contractor by or on behalf of DOD in support of the performance of the contract; or (2) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract." DFARS 252. 204-7012(a).

[37]DFARS 204. 7300. " Cyber incident" means actions taken through the use of computer networks that result in a compromise or an actual or

potentially adverse effect on an information system and/or the information residing therein. 252. 204-7012(a).

[38]The DIBNet portal is the DoD’s only reporting mechanism for DoD contractor reporting of cyber incidents on unclassified information systems.

[39] *Network Penetration Reporting and Contracting for Cloud Services (DFARS Case 2013-D018) Frequently Asked Questions (FAQs).* Jan 27, 2017. Available at: https://www. acq. osd. mil/dpap/pdi/docs/FAQs_Network_Penetration_Reporting_and_Contracting_for_Cloud_Services_(01-27-2017). pdf.

[40]DFARS 252. 204-7012(d).

[41]Id.

[42]DFARS 252. 204-7012(f).

[43]81 Fed. Reg. 72991.

[44]DFARS 252. 204-7012(m)(1).

[45] *See* DFARS 252. 204-7012(m)(2).

[46]In describing FedRAMP+, in addition to the FedRAMP requirements, the DOD adds “ specific security controls and requirements necessary to meet and assure DoD’s critical mission requirements.” *See* DEPARTMENT OF DEFENSE (DoD) CLOUD COMPUTING SECURITY REQUIREMENTS GUIDE (SRG), Version 1, Release 1 at 8, Jan. 12, 2015. *Available at* https://iase. disa. mil/cloud_security/documents/u-cloud_computing_srg_v1r1_final. pdf.

[47] *See Id* . Explaining the background of FedRAMP: “ FedRAMP is a “ Federal Government program focused on enabling secure cloud computing for the Federal Government. FedRAMP is mandated for use by all Federal Agencies by the Office of Management and Budget (OMB)… FedRAMP provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud services by incorporating the Federal Government RMF processes. FedRAMP uses a “ do once, use many times” framework that intends to reduce cost, time, and staff required for security assessments and process monitoring reports.”

[48] *See* DFARS 252. 204-7012(b)(2)(ii)(D).

[49]DFARS 252. 204-7012(b)(2)(i).

[50]https://csrc. nist. gov/CSRC/media/Publications/sp/800-171/rev-1/archive/2016-12-20/documents/sp800-171r1-20161220. pdf.

[51] *See* NIST SP 800-171, Rev. 1, “ Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations,” at i (Dec. 2016), available at http://nvlpubs. nist. gov/nistpubs/SpecialPublications/NIST. SP. 800-171r1. pdf.

[52]Id. at 8

[53]https://csrc. nist. gov/CSRC/media/Publications/sp/800-171/rev-1/archive/2016-12-20/documents/sp800-171r1-20161220. pdf p. 21

[54]NIST p. 11

[55]http://dodprocurementt oolbox. com/cms/sites/default/files/resources/2017-09/USA 002829-17-DPAP. pdf.

[56]ADD CITE

[57] *See* DFARS 252. 204-7012(b)(2)(ii)(B).

[58] *Id* .

[59] *See* DFARS 252. 204-7008.

[60]DFARS 252. 204-7012(b)(2)(ii)(B).

[61] *See* NIST SP 800-171 Rev. 1 (https://nvlpubs. nist. gov/nistpubs/SpecialPublications/NIST. SP. 800-171r1. pdf)

[62]Id.

[63]Id.

[64]The Navy's Sea Warrior Program " provides information technology (IT) business systems to recruit, train, pay, promote, move, retire, and support Navy personnel. As such, PMW 240 is the single IT acquisition agent for non-tactical business operations providing full life cycle management to support Navy human resource management, criminal justice, Fleet support, afloat business applications, Navy and Department of Defense (DoD) portfolio management, Department of Navy (DON) administration, and joint aviation

aircraft scheduling.” (https://www. public. navy. mil/spawar/PEOEIS/Documents/SWP/FS_PMW240. pdf)

[65]the solicitation states that “[t]he NetRPA application is the Navy’s primary market research tool utilized for making decisions concerning the placement of personnel, the setting of recruiting goals, and the alignment of Zone, Station, and Zone Improvement Program (ZIP) Codes at the Navy Recruiting Districts.” Agency Report, exh. 4, Performance Work Statement for NetRPA, at 3.

[66]The solicitation provided that factors 1 through 4 were listed in descending order of importance; that factors 1 through 3 would be rated under an adjectival rating system of good, acceptable, marginal and unacceptable; and that factor 5 (past performance) would be evaluated on a pass/fail basis. FRP 140-47.

[67] See RFP at 32-35

[68] See RFP at 32-35. For an explanation of these requirements, *see* Agency Report , exh. 8, Declaration of Agency’s Information Technology Specialist, Aug. 31, 2017, at 1. “[r]igorous cybersecurity requirements are applied to DOD and Department of the Navy (DON) systems . . . because of their potential impact on national security,” adding that “[c]ybersecurity requirements are heightened when . . . personally identifiable information (PII) data is present, particularly for members of the armed forces.”

[69]The RFP stated that proposals should include “ information in sufficient detail so that the government evaluators are able to meaningfully evaluate

the Offeror’s proposal without discussions” and must demonstrate that the offeror “ has valid and practical solutions for all requirements.” RFP at 115. Finally, offerors were warned that the agency “ may judge a proposal to be unacceptable” if it failed to “ clearly reveal the Offeror’s proposed approach.” Id.

[70]See GAO decision B-41508, B-415058. 2, Nov. 16, 2017 at 2. (https://www. gao. gov/assets/690/688945. pdf)

[71] *See* Protest at 7-11. A Technical evaluation team referred to Syneren’s proposal to use its software as “ not accredited” and stated that Syneren’s proposal did not include any specific plans to achieve accreditation.

[72] *Id.*

[73] *See* GAO decision at 4.

[74] *See* Protester’s Comments on AR, Sept. 11, 2017, at 4.

[75] *Id.* at 4

[76] *Id.* at 4.

[77]GAO Decision at 4.

[78]Id.

[79]Id. at 5 In reviewing Syneren’s protest, the GAO stated: “ On this record, we find no basis to question the reasonableness of the agency’s determination that Syneren’s proposal failed to adequately address how it

would successfully comply with the solicitation's cybersecurity requirements and, accordingly, that its proposal was unacceptable. ”

[80] *See* 83 FR 9, January 12, 2018. “ GSA is proposing to update the General Services Administration Acquisition Regulation (GSAR) to update existing GSA cybersecurity requirements that did not previously go through the rulemaking process and integrate these updated requirements within the GSAR. This rule will require contracting officers to incorporate applicable GSA cybersecurity requirements within the statement of work to ensure compliance with Federal cybersecurity requirements and implement best practices for preventing cyber incidents.” *See also* , Executive Order 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, May 11, 2017.

[81] *See* , GAO Decision B-414890, B-414890. 2: Oct 4, 2017 at 1-2. (https://www. gao. gov/assets/690/687812. pdf). The RFP was issued as a small business set-aside under “ DISA's GSM-ETI multiple-award IDIQ contract…on a best-value basis of a cost-plus-fixed-fee task order for a base year and up to two 1-year option periods and one 5-month option period.”

[82] *See* , GAO Decision B-414890, B-414890. 2 at 2.

[83]Id at 2. DISA's Global Video Service offers “ on-demand, high-quality assured video conference capabilities for users to interact visually within the Sensitive but Unclassified IP Router Network (NIPRNet) and the Secret IP Router Network (SIPRNet). GVS is built to support conference rooms across the Department of Defense (DOD) with high definition video and offers a desktop video solution, allowing face-to-face meetings from the desktop.”

See Global Video Services Fact Sheet available at: https://disa.

mil/Enterprise-Services/Video/~/media/Files/DISA/Fact-Sheets/GVS. pdf

[84] *Id* at 2.

[85] *Id.* at 2.