THE GOVERNMENT CONTRACTOR®

THOMSON REUTERS

Information and Analysis on Legal Aspects of Procurement

Vol. 57, No. 35 **September 23, 2015**

Focus

¶ 283

FEATURE COMMENT: As OMB Catches Up To DOD On Cybersecurity With Proposed Guidance, DOD Forges Ahead With Interim Rule Enhancing Cyber Incident Reporting And Cloud Security Requirements

In recent weeks, the secretary of defense issued an interim rule requiring defense contractors to notify the Government regarding certain cyber incidents, and the Office of Management and Budget issued proposed guidance on cybersecurity protections in federal acquisitions.

For its part, the Department of Defense advanced Defense Federal Acquisition Regulation Supplement Case 2013-D018 from a proposed rule to an interim rule without public comment, citing the protection of covered defense information and the need to understand the full scope of cyber incidents involving defense contractors as a justification for bypassing standard rulemaking procedures. See 80 Fed. Reg. 51739 (Aug. 25, 2015). According to the secretary, recent high-profile breaches of systems containing federal information show the need to ensure that information security requirements are clearly and consistently addressed in Government contracts. Similarly, the proliferation of information technology and increased IT access associated with cloud computing have increased the threat to, and vulnerability of, DOD information.

The DFARS interim rule expands existing DOD requirements that cover the protection and reporting of incidents affecting controlled technical information. The OMB guidelines are intended to "take major steps toward implementing strengthened cybersecurity protections in federal acquisitions[,] thus mitigating the risks of potential incidents," and offer a preview of what defense *and* civilian IT contractors can expect to see in solicitations and Government orders in the near future. This FEATURE COMMENT analyzes the DFARS interim rule and the OMB proposed guidance.

Interim Rule on Network Penetration Reporting and Contracting for Cloud Services (DFARS Case 2013-D018)—On August 26, DOD issued an interim rule amending the DFARS to implement § 941 of the National Defense Authorization Act (NDAA) for Fiscal Year 2013, and § 1632 of NDAA 2015. Section 941 of NDAA 2013 requires cleared defense contractors to report information system and network penetrations, and allow DOD personnel access to the system or network to assess the impact of the penetration. Similarly, § 1632 of NDAA 2015 requires that a contractor designated as operationally critical to a DOD activity must report each penetration of its information system or network. The secretary of defense determined that urgent and compelling reasons justify issuing the interim rule without public comment. Additionally, this interim rule implements DOD policy on the purchase of cloud computing services. The rule is intended to streamline the reporting process for contractors and create a single reporting mechanism of cyber incidents involving unclassified information systems by DOD contractors.

The interim rule became effective upon publication on August 26. Comments on the interim rule must be submitted to DOD by October 26 to be considered in the formation of the final rule.

Network Penetration Reporting: The interim rule now requires contractors and subcontractors to report cyber penetration incidents that have an actual or potentially adverse effect on a covered contractor's information system or covered defense information residing therein, or on a contractor's ability to provide operationally critical support. To implement the requirements of § 941 of NDAA 2013 and § 1632 of NDAA 2015, the interim rule utilizes

DFARS subpt. 204.7, expanding existing clauses, and adding a new provision and clause. The interim rule also creates a new subpart, provision and clause covering contracting for cloud computing services, which will be discussed later in this FEATURE COMMENT.

The interim rule promulgated at DFARS 252.204-7012(c)(1)–(3) revises contractor reporting requirements when the contractor discovers a cyber incident affecting covered contractor information systems, or covered defense information residing therein, or compromises the contractor's ability to perform contract requirements under critical support activities. Upon discovery, the contractor will conduct a review of the incident, identifying the compromised computers, servers, specific data or user accounts. Additionally, the contractor's review will include analyzing the information systems on the contractor's network that may have been accessed by the cyber incident.

The contractor shall "rapidly report" cyber incidents to DOD via *http://dibnet.dod.mil*. The interim rule defines rapidly reporting as within 72 hours of the contractor's discovery of the cyber incident. The cyber incident report will be treated as information created for DOD and contain, at a minimum, the elements contained on the DOD report site. For reports under DFARS 252.204-7012, DOD requires at least twenty elements that identify the contractor, type of facility, points of contact, a description of what is known of the incident, information and systems involved, and whether the compromise was successful, failed or unknown.

The interim rule modifies DFARS 204.73 to expand safeguarding and reporting requirements by requiring the protection of several classes of sensitive defense information, specifically, controlled technical information, export controlled information, critical information and other information determined to require protection by law, regulation or Government policy.

The policy stated in the prescription clause at DFARS 204.7302 was revised to require that contractors and subcontractors submit to DOD upon request reports identifying (1) a cyber incident; (2) malicious software, if detected and isolated; and (3) media (or access to covered contractor information systems and equipment). For submissions of contractor media and malicious software, contracting officers should refer to the instructions contained in DFARS Procedures, Guidance and Information 204-7303(a)(1)(iii).

In addition, *sub*contractors are now required to "rapidly" report cyber incidents directly to DOD at *http://dibnet.dod.mil* and to the prime contractor by providing the prime contractor with the DOD incident report number. Lower-tier subcontractors report to their next-higher tiers until the prime contractor receives a report.

The Government acknowledges that information disclosed by a contractor in accordance with these procedures may contain "contractor attributional/proprietary information that is not customarily shared outside the contractor's organization[,] and such disclosure or unauthorized use could cause competitive harm to the contractor." Consequently, pursuant to 204.7303(c), the Government shall protect against the unauthorized use or release of any information that includes contractor attributional/proprietary information.

It must be noted that the revised DOD policy promulgated at 204.7302(d) states that the reporting of a cyber incident by a contractor or subcontractor shall not be interpreted by the Government as evidence that the company has failed to provide adequate safeguards for covered defense information on its unclassified information systems, or has otherwise failed to meet the requirements contained in clause 252.204-7012. Once an incident is reported, the CO shall consult with the cognizant DOD chief information officer or cyber security office prior to assessing the contractor's compliance. The CO shall consider such cyber incidents in the context of an overall assessment of a contractor's compliance with the requirements and safeguards contained in 252.204-7012.

Additionally, DFARS clause 252.204-7012 is renamed "Safeguarding Covered Defense Information and Cyber Incident Reporting." The scope of this DFARS clause is expanded to cover the safeguarding of "covered defense information," and now requires contractors to report cyber incidents involving this new defined class of information. The modified DFARS clause also requires contractors to report cyber incidents that may affect their ability to provide operationally critical activities.

The interim rule also replaces the existing "Minimum Security Controls for Safeguarding" Table 1 contained in DFARS 252.204-7012, based on the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 with NIST SP 800-171. As stated in the SP and the interim rule's preamble, NIST SP 800-171 is a publication specifically tai-

lored for protecting sensitive information residing in contractor information systems. The rule also refines the requirements of Federal Information Processing Standard (FIPS)-200, and the controls from NIST SP 800-53. The DFARS transition to NIST SP 800-171 presents the minimum controls for contractor information systems in an easier to use format that significantly increases the protections afforded Government information residing on or moving through contractor information systems. NIST SP 800-171 was published in final form on June 19 and is available at *nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171.pdf*. As prescribed by 204-7304(c), this clause shall be included in all solicitations and contracts for FAR pt. 12 commercial-item acquisitions.

A new provision at DFARS 252.204-7008, "Compliance with Safeguarding Covered Defense Information Controls," is added. The purpose of this addition is to ensure that offerors are aware of the modified DFARS clause 252.204-7012 requirements that will be implemented for all covered defense information on all covered contractor information systems that support the performance of the awarded contract. According to the preamble, this new provision will allow for a process for the contractor to explain in writing (a) how alternative but equally effective security measures can compensate for the inability to satisfy a particular requirement, or (b) why a particular requirement is not applicable to the contracting activity, if the contractor deviates from any of the guidelines of NIST SP 800-171. As prescribed by 204-7304(a), this provision shall be included in all solicitations and contracts using FAR pt. 12 commercial-item acquisition procedures.

A new clause at 252.204-7009, "Limitation on the Use and Disclosure of Third-Party Reported Cyber Incident Information," is added to protect information submitted to DOD in response to a cyber incident. This clause sets forth the new definitions (discussed below) applicable to network penetration reporting, and establishes restrictions on any information that the contractor receives or creates in the performance of the contract. The restrictions mandate that a contractor (1) access and use the reported information only for the purpose of furnishing advice to the Government; (2) protect the information from further unauthorized release or disclosure; (3) ensure that its employees are subject to use and nondisclosure obligations consistent with this clause before they have access to the information; and (4) recognize that the third party who reported the information is a third-party beneficiary of the nondisclosure agreement between the Government and the contractor. A breach of these restrictions may subject the contractor to criminal, civil, administrative and contractual actions in law or in equity, for penalties, damages or other remedies found appropriate by the Government. In addition, a contractor may be liable for civil actions for damages and other remedies by the third party who reported the incident as a "third-party beneficiary" of this clause. The substance of this clause will be flowed down in all subcontracts related to safeguarding covered defense information and cyber incident reporting, including subcontracts for commercial items.

Definitions: The interim rule revises a number of clauses to create new definitions or amend existing definitions in DFARS 202.101 and 204.7301.

"Contractor attributional/proprietary information" means information that identifies the contractor, directly or indirectly, by the grouping of information that can be traced back to the contractor (e.g., program description, facility locations), as well as personally identifiable information, trade secrets, commercial or financial information, or other commercially sensitive information that is not customarily shared outside of the company.

"Controlled technical information" means technical information with military or space application that is subject to controls on access, use, reproduction, modification, performance, display, release, disclosure or dissemination. Controlled technical information would meet the criteria, if disseminated, for distribution statements B through F using the criteria set forth in DOD Instruction 5230.24, Distribution Statements on Technical Documents. The phrase does not include information that is lawfully publicly available without restrictions.

"Covered contractor information system" means an information system that is owned, or operated by or for, a contractor, and that processes, stores or transmits covered defense information.

"Covered defense information" means unclassified information that—

(1) Is—

(a) Provided to the contractor by or on behalf of DOD in connection with the performance of the contract; or

(b) Collected, developed, received, transmitted, used or stored by or on behalf of the contractor in support of the performance of the contract; *and*

(2) Falls in any of the following categories:
(a) Controlled technical information.
(b) Critical information (operations security). Specific facts identified through the operations security process about friendly intentions, capabilities and activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment (part of operations security process).
(c) Export control. Unclassified information concerning certain items, commodities, technology, software or other information whose export could reasonably be expected to adversely affect the U.S. national security and nonproliferation objectives. To include dual-use items; items identified in export administration regulations, international traffic in arms regulations, and munitions list; license applications; and sensitive nuclear technology information.
(d) Any other information, marked or otherwise identified in the contract, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations and Government-wide policies (e.g., privacy, proprietary business information). Information system means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of information.

"Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of information.

"Operationally critical support" means supplies or services designated by the Government as critical for airlift, sealift, intermodal transportation services or logistical support that are essential to the mobilization, deployment or sustainment of the Armed Forces in a contingency operation.

"Rapid(ly) report(ing)" means within 72 hours of discovery of a cyber incident.

In addition, the interim rule adds or relocates the following definitions to FAR 202.101.

"Compromise" means disclosure of information to unauthorized persons, or a violation of the security policy of a system, in which unauthorized intentional or unintentional disclosure, modification, destruction or loss of an object, or the copying of information to unauthorized media, may have occurred.

"Cyber incident" means action taken through the use of computer networks that results in a compromise or an actual or potentially adverse effect on an information system or the information residing therein.

"Media," as used in pts. 204 and 239, means physical devices or writing surfaces, including, but not limited to, magnetic tapes, optical disks, magnetic disks, large-scale integration memory chips and printouts onto which covered defense information is recorded, stored or printed within a covered contractor information system.

Small Businesses: Neither the interim rule nor DFARS 252.204-7012 contains a small business exception.

Flowdown: Contractors shall include the substance of 252.204-7009 and 252-204-7012 in all subcontracts including subcontracts for commercial items.

Commercial-Item Acquisitions: As mentioned above, the interim rule modifies pt. 212, "Acquisition of Commercial Item," to make 252.204-7008, 252.204-7009 and 252.204-7012 applicable to acquisitions of commercial items as prescribed.

Contracting for Cloud Computing: The interim rule implements DOD policies and procedures for use when the Government contracts for cloud computing services. The DOD CIO on Dec. 15, 2014 issued a memo, "Updated Guidance on the Acquisition and Use of Commercial Cloud Computing Services," intended to clarify DOD guidance for acquiring commercial cloud services. This guidance was followed by the DOD CIO's issuance in January 2015 of "Cloud Computing Security Requirements Guide (SRG), Version 1." This interim rule implements the DOD policies and procedures set forth in those guides to ensure uniform application when acquiring cloud services with the intended goals of increasing cyber security across DOD and mitigating the risks of compromised information when using cloud services.

The interim rule adds a new subpart, provision and clause related to cloud computing. DFARS subpt. 239.76 is added to implement policy for the acquisition of cloud computing services. The new provision at 252.239.7009, "Representation of Use of Cloud Computing," is added to allow an offeror to represent its intention to utilize cloud computing services in performance of the contract, or alternatively, to state that it will not be so utilizing.

The new clause at 252.239-7010, "Cloud Computing Services," adds standard contract language for the acquisition of cloud computing services including the access, security and reporting requirements.

Additionally, these new clauses and provisions are added to the list of solicitation provisions and contract clauses for the acquisition of commercial items at 212.301(f).

From a policy perspective, DOD will generally acquire cloud computing services using commercial terms and conditions consistent with federal law. Common examples of commercial terms and conditions are end-user license agreements and terms of service. The CO shall award a contract for cloud computing services only if the contractor or subcontractor (regardless of tier) has provisional authorization from the Defense Information Systems Agency at a level appropriate to the requirement in accordance with the then-current DOD CIO's SRG. When contracting for cloud services, the CO shall ensure that the purchasing request states (a) the Government data and data descriptions; (b) data ownership, licensing, delivery and disposition instructions specific to the relevant Government data; (c) appropriate limitations and requirements on contractor and third-party access, use and disclosure of the Government data; (d) appropriate requirements to inspect and audit the contractor's activities applicable to the type of Government data; (e) appropriate requirements for system-wide search and access capabilities supporting inspections, audits, investigations, litigation, eDiscovery and records management needs corresponding with the agency's record retention schedules; and (f) a requirement that the contractor coordinate with CO-designated officials who are responsible for responding to spillage in connection with the cloud computing services provided.

DFARS 202.101 and 204.7301 include definitions created by the interim rule. In addition, the interim rule moves the definition of "cyber incident" from subpt. 204.73 to 202.1. The terms "compromise" and "media" are also added to 202.101.

"Authorizing official," as described in DOD Instruction 8510.01, "Risk Management Framework (RMF) for DOD Information Technology (IT)," means the senior federal official or executive with the authority to assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image or reputation), organizational assets, individuals, other organizations and the nation.

"Cloud computing" means a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service-provider interaction. This includes other commercial terms, such as on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service. It also includes commercial offerings for software-as-a-service, infrastructure-as-a-service and platform-as-a-service.

"Government data" is any information, document, media or machine-readable material, regardless of physical form or characteristics, that is created or obtained by the Government in the course of official Government business.

"Government-related data" is any information, document, media or machine-readable material, regardless of physical form or characteristics, that is created or obtained by a contractor through the storage, processing or communication of Government data. This does not include a contractor's business records, e.g., financial or legal records, or data such as operating procedures, software coding or algorithms that are not uniquely applied to the Government data.

"Media" are defined above.

"Spillage" is a security incident that results in the transfer of classified or controlled unclassified information (CUI) on an information system not accredited or authorized for the appropriate security level.

The interim rule creates a new clause at 252.239-7010, which is to be used in solicitations and contracts, including those for FAR pt. 12 commercial items, when procuring IT services. Principally, this new clause sets forth cloud computing security requirements applicable when using cloud computing to provide IT services in the performance of a contract.

The new DFARS clause requires contractors using cloud services in the performance of a contract to implement and maintain administrative, technical and physical safeguards and controls with the requisite security level and services in accordance with the DOD CIO's then-current SRG version. The contractor is now required to maintain *within the U.S. or outlying areas* all Government data not physically located on DOD premises. This means all cloud computing servers must be physically located in the

U.S. or its outlying areas. Outlying areas as defined in FAR 2.101 include U.S. possessions and territories. Any other location requires the CO's written notice in accordance with DFARS 239.7602(a).

Moreover, the contractor shall not access, use or disclose Government data unless specifically authorized by the contract or task or delivery order. If so authorized, then the access, use or disclosure shall be limited to that specified in the contract or task or delivery order. The limitations on access, use and disclosure survive termination or expiration of the contract. If the contracted activities support the Government, the contractor shall only use the data to manage the operational environment supporting the Government data unless expressly authorized by the CO.

If a cyber incident related to cloud computing services occurs, the contractor will report the incident to DOD via *dibnet.dod.mil*. While this is the same DOD reporting portal as required under DFARS 252.204-7012, there is a separate section for reporting cyber incidents by contractors who provide cloud services. When the cyber incident involves malicious software, the contractor or subcontractor shall provide the malicious software to the Government. Additionally, the contractor or subcontractor will preserve and protect images of all known affected information systems, including all relevant monitoring/packet capture data, for not less than 90 days.

Once an incident is reported, the interim rule requires contractors to allow DOD access to the information or equipment to perform forensic analysis. If DOD elects to conduct a damage assessment, the 252.239-7010(f) media preservation and protection requirements summarized above apply.

The interim rule promulgates records management and contractor facility access requirements. The contractor will provide the CO all Government data and Government-related data, and must dispose of the data as stated in the contract. Such disposition will be confirmed to the CO in accordance with the contract closeout procedures. If a contractor receives a third-party request to access Government data, the contractor will promptly notify the CO and cooperate with the CO to take *all measures* to protect said data. Third-party requests include warrants, subpoenas and other seizure orders from federal agencies or courts.

The contractor will also provide the Government or its authorized representative access to all Government data, access to the contractor personnel involved in performance of the contract, and physical access to the contractor's facilities containing Government data, for the purposes of inspections, audits, investigations and similar activities authorized by federal law.

Flowdown: The contractor will include the substance of 252.239-7010 in all subcontracts that involve or might involve cloud services, including subcontracts for commercial items.

How the Interim Rule Affects Contractors—The interim rule requires contractors and subcontractors to report cyber incidents that result in an actual or potential adverse effect on a covered contractor's information system or covered defense information residing in a contractor's information system. Subcontractors are now required to report cyber incidents to their prime contractor or next-higher tier, but also directly to DOD. In addition, the interim rule implements existing DOD policies and procedures for the procurement and use of cloud services. The interim rule applies to all solicitations and contracts, including those for commercial items. As discussed above, comments on the interim rule are due October 26.

The OMB Proposed Guidance for Improving Cybersecurity—On August 11, OMB issued a cybersecurity "proposed guidance" document titled, "Improving Cybersecurity Protections in Federal Acquisitions." The stated goal of the guidance is "to take major steps toward implementing strengthened cybersecurity protections in federal acquisitions and therefore mitigating the risk of potential incidents in the future." The guidance focuses primarily on contractors that store or manage Government information in non-federal systems, and, as one commenter has noted, largely brings the requirements applicable to all federal agencies in line with DOD regulations that have been in place for a few years. Wolff et al., "What the OMB Cybersecurity Proposal Does and Doesn't Do," Law360 (Aug. 19, 2015). The guidance, if and when it is finalized, will not be binding on federal contractors, but it will direct agencies to promulgate acquisition rules consistent with the guidance.

The guidance directs agencies to require contractors to conform to NIST SP 800-53 when they operate a system on behalf of the Government. SP 800-53 lists 51 specific security controls for federal information systems and organizations. It is a dense set of standards for achieving "adequate security" that is adaptable to different organizations and has been revised a number of times. Contractors that do not operate

federal systems, but need access to CUI in performing a contract, should be required to conform to NIST SP 800-171. NIST SP 800-171 is less burdensome than 800-53 and requires only 14 security controls, some or all of which apply if agencies are relying on contractors to protect CUI.

The guidance also directs agencies to require that contractors report any cyber incidents affecting their internal systems, but only if those incidents involve or affect CUI. A "cyber incident" is action taken through the use of computer networks that results in a compromise or an actually or potentially adverse effect on an information system and/or the information residing therein. The guidance offers a list of specific provisions that contracts should contain.

- Language to indicate that a cyber incident that is properly reported by the contractor shall not, by itself, be interpreted as evidence that the contractor has failed to provide adequate information safeguards for CUI.
- The definition of what constitutes a cyber incident.
- The required timeline for first reporting to the agency.
- The types of information required in a cyber incident report, including company and point of contact information, contract information and the type of information compromised.
- The contractor shall send only one report to each agency contact identified in the contracts, not a report for each contract with that agency. The report may contain information required by other agencies, so one report may satisfy the requirements of multiple agencies.
- Specific Government remedies if a contractor fails to report according to the agreed-upon contractual language.

Next, the guidance prescribes guidelines for assessing contractors that are operating Government systems. The guidance acknowledges that many, if not most, contractors already undergo independent security assessments that provide the same assurances that Government monitoring would provide. The guidance directs that this should be taken into account as agencies develop their cybersecurity rules for contractors to avoid any unnecessary redundancy. The guidance provides a list of contractor system assessment guidelines:

- Agencies should first use FIPS-19910 to assess the impact level of the data that are to reside in the contractor's information system, in order to determine what types of controls should be applied, followed by determining whether it is appropriate to obtain an independent security assessment;
- agencies may accept independent third-party verification of security assessment results, or contractor or Government assessment evidence based on their risk assessment;
- the assessment of privacy controls must be performed by the senior agency official for privacy; and
- after performance under the contract has begun, agencies shall ensure that they have access for security reviews on a periodic and event-driven basis for the life of the contract.

The guidance goes on to recommend that agencies insist on broad rights to examine contractors' IT systems and physical facilities. The guidance further directs that agencies should insist on contract terms that require contractors to certify that they have "sanitized" (i.e., destroyed) any sensitive Government information before completing contract closeout procedures.

After the assessment process and award, the guidance directs agencies to put "information security continuous monitoring" provisions in their contracts. Agencies should insist that a contractor's system meet the requirements laid out in an earlier OMB cybersecurity memorandum, OMB Memorandum M-14-03, or, alternatively, they should carry out continuous monitoring themselves. Finally, the guidance directs the General Services Administration to create a business information shared service to function as a sort of "clearinghouse" for contractor cyber-threat information that would allow agencies to stay better informed regarding emerging cyber threats and cybersecurity best practices, as well as know which contractors have faced cybersecurity problems in the past.

How the Proposed Guidance Affects Contractors—The guidance raises several concerns. First, the guidance states that after contract performance has begun, agencies shall ensure they have a right to access contractor systems for security reviews on a periodic and event-driven basis for the life of the contract. This level of unfettered access to contractor facilities is virtually unheard of in commercial IT contexts, and may prevent federal agencies from enjoying the benefits of commercial offerings at com-

mercial prices as IT vendors refuse to adhere to such intrusive Government oversight.

In addition, the guidance indicates that agencies should reserve to themselves the right to assess contractors' continual security monitoring capabilities and to elect whether to conduct monitoring themselves. Again, this is far more extensive than the set of monitoring rights cloud vendors generally extend to commercial customers. Ultimately, these sorts of security measures may lead IT vendors simply to avoid any Government business if they cannot profitably operate "Government-only" data hosting facilities. "Co-tenant" cloud facilities achieve the greatest cost savings for customers, and many contractors already adhere to the Federal Risk and Authorization Management Program requirement for dedicated Government connections to co-tenant cloud facilities. It remains to be seen whether, and to what extent, industry can persuade OMB to "dial back" these requirements, and, if not, whether IT vendors can live with pervasive Government assessment and monitoring of their networks.

✦

This Feature Comment was written for The Government Contractor by* Dean P. Vanek *and* Steven D. Tibbets*. Mr. Vanek is a principal of the Chicago-based law firm GCL Group, Chartered. Mr. Tibbets serves as Counsel at CA Technologies, primarily supporting the company's public-sector business.