Bloomberg BNA

Federal Contracts Report™



*Cybersecurity*

# Contractors Caught in the Cyber Minefields: More Rules and Greater Confusion for Public Sector Cybersecurity

BY DAVID Z. BODENHEIMER & OLIVIA L. LYNCH

As if government contractors did not already have enough to worry about in cyberspace, every day brings new headlines about digital Pearl Harbors, terabyte losses of corporate intellectual property, and ever more litigation over compromised personal data. But now there's more—much more.

Agency by agency, more cyber rules are bursting out of solicitations and regulations, imposing expanded requirements for data breach notification, security audit access, personnel screening, and other information security obligations. For government contractors, this trend towards agency-specific cyber requirements has two key implications. First, contractors must shoulder the compliance burden of tracking and meeting an ever proliferating set of agency-level standards and clauses imposing different—perhaps even conflicting—requirements for each agency and solicitation. Second, each wave of new cyber requirements creates heightened risks that a contractor will miss a contractual duty, thus triggering negative past performance evaluations, various contractual breaches and penalties, and agency enforcement actions.

*David Z. Bodenheimer is a partner with Crowell & Moring's Government Contracts Group. David heads the Homeland Security practice and focuses his practice on cybersecurity, False Claims Act, government pricing, protests, and related litigation. Olivia Lynch is an associate in Crowell & Moring's Government Contracts Group. She represents government contractors in bid protests before the Government Accountability Office and the Court of Federal Claims, as well as in civil litigation and arbitration.*

This analysis addresses some examples of agency-specific cybersecurity requirements where contractors need to be on the lookout in four areas: (1) data breach notification; (2) security audit access; (3) personnel screening and management; and (4) risk allocation, liability, and penalties. While not a comprehensive list, it illustrates the compliance kaleidoscope now facing government contractors in dealing with cyber requirements.

**Security Breach Reporting.** For security breaches involving sensitive personal data, some duties to report have been around for a while. For example, 47 states now impose notification obligations when certain types of personal data, such as Social Security numbers, have been compromised. And the list continues to grow, such as the Securities and Exchange Commission's (SEC) Cybersecurity Disclosure Standard for publically traded companies experiencing material ''cyber incidents'' compromising the company's systems or data. *See* SEC, *CF Disclosure Guidance: Topic No. 2 – Cybersecurity* (Oct. 13, 2011).

For federal agencies and covered contractors, the Federal Information Security Management Act (FISMA) generally requires an incident response plan for ''security incident'' detection, reporting, and response. 44 U.S.C.A. § 3544(b)(7). But FISMA does not spell out the specifics—when, how, and to whom. Instead, these details must be found in agency-specific guidance.

*Defense Contractors*. For Fiscal Year 2013, the National Defense Authorization Act (NDAA) included a

 ISSN 0014-9063

new reporting requirement for ''cleared defense contractors'':

> (a) Procedures for Reporting Penetrations. The Secretary of Defense shall establish procedures that require each cleared defense contractor to report to a component of the Department of Defense designated by the Secretary for purposes of such procedures when a network or information system of such contractor that meets the criteria established pursuant to subsection; (b) is successfully penetrated.

Pub. L. No. 112-239, § 941(a). This provision only applies to defense contractors accessing or handling classified information, but the NDAA does not expressly limit these reporting duties to breaches of classified networks or data. When a ''cleared defense contractor'' suffers a successful ''penetration,'' that contractor must provide ''rapid reporting'' to an as-yet unspecified Department of Defense (DOD) component. *Id.*, § 941(c)(1). While not stating how ''rapid'' such reporting must be, the NDAA does specify the following data must be included in each report:

- ''A description of the technique or method used in such penetration.''

- ''A sample of the malicious software, if discovered and isolated by the contractor, involved in such penetration.''

- ''A summary of information created by or for the Department in connection with any Department program that has been potentially compromised due to such penetration.''

*VA Contractors*. In recent solicitations, the Department of Veterans Affairs (VA) has used a data breach notification clause requiring a contractor to *immediately* notify the Contracting Officer's Representative and the designated Information Security Officer and Privacy Officer of a ''security incident.'' In instances of criminal activity, the contractor must concurrently report to the appropriate law enforcement entity, including the VA Office of Inspector General and Security and Law Enforcement. A ''security incident'' is defined to mean an event that has, or could have, resulted in unauthorized access to, loss or damage to VA assets or sensitive information, or an action that breaches VA security procedures. These requirements for immediate notification for ''could have'' breach risks create standards that will trip up many contractors, as their forensics team struggles to find out who has breached what and how well after the breach occurred.

*OPM Contractors*. Similarly, Office of Personnel Management (OPM) solicitations have required that all security incidents involving OPM information or information systems must be reported ''immediately upon discovery of the incident'' to the OPM Situation Room and the Contracting Officer. Furthermore, all incidents ''must be reported, even if it is believed the breach is limited, small, or insignificant''; the OPM IT security experts will determine which breaches need ''additional focus and attention.'' Such notification requirements not only impose substantial compliance burdens on contractors, but could affect OPM's ability to focus its resources upon the most serious breaches.

**Security Audit Access.** Many years ago, Congress gave federal agencies broad audit access to contractors' financial data for certain types of contracts. Increasingly, agencies are now requiring contractors to open their corporate networks and systems to security audits and reviews to assess the soundness of information security controls. Like financial audits, these expansive demands for security audit access raise serious questions for government contractors.

*Defense Contractors*. In the 2013 NDAA, Congress granted DOD access to the networks of ''cleared defense contractors.'' Specifically, Section 941 requires DOD procedures that ''include mechanisms for Department of Defense personnel to, upon request, obtain access to equipment or information of a cleared defense contractor necessary to conduct forensic analysis in addition to any analysis conducted by such contractor.'' Pub. L. No. 112-239, § 941(c)(2)(A) (2013). However, this provision does place certain limits upon DOD's access to the defense contractor's networks and information systems. First, DOD may only obtain access ''to determine whether information created by or for the Department in connection with any Department program was successfully exfiltrated from a network or information system of such contractor and, if so, what information was exfiltrated.'' *Id.*, § 941(c)(2)(B). Second, the NDAA requires that DOD ''provide for the reasonable protection of trade secrets, commercial or financial information, and information that can be used to identify a specific person.'' *Id.*,§ 941(c)(2)(C). Ultimately, the extent of protection for covered contractors will depend upon both the procedures that DOD actually issues and how DOD handles such access on a case-by-case basis.

*GSA Contracts*. Based upon a FISMA audit, the General Services Administration (GSA) Inspector General recommended that GSA strengthen security requirements in contracts for information technology. As a result, GSA expanded its audit rights to obtain access to contractors' and subcontractors' facilities, installations, operations, documentation, databases, IT systems and devices, and personnel used in performance of the contract:

> Access shall be provided to the extent required, *in GSA's judgment*, to conduct an inspection, evaluation, investigation or audit, including vulnerability testing to safeguard against threats and hazards to the integrity, availability and confidentiality of GSA data or to the function of information technology systems operated on behalf of GSA, and to preserve evidence of computer crime. This information shall be available to GSA upon request.

GSAM 552.239-71(k) (emphasis added). In short, GSA has reserved virtually unfettered discretion to prowl through a contractor's networks, systems, and databases.

*Other Agencies*. Such audit provisions also appear in other agencies' solicitations, such as the Department of Health and Human Services (HHS) and Department of Commerce (DOC). And with the rising importance of continuous monitoring, agencies have begun requiring that they be provided what could be interpreted as continuous access to a contractor's systems and infrastructure, such as in this OPM clause, ''Contractor System Oversight/Compliance'':

> The Contractor shall support the OPM in its efforts to assess and monitor the contactor systems and infrastructure. The contractor shall provide logical and physical access to the contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases upon request. The contractor will be expected to perform automated scans and continuous monitoring activities

  FCR ISSN 0014-9063

> which may include, but not limited to, authenticated and unauthenticated scans of networks, operating systems, applications, and databases and provide the results of the scans to OPM or *allow OPM personnel to run the scans directly*.

These types of very broad audit and inspection rights will likely cause friction between agencies and contractors over the scope of security audits. They raise questions as to how contractors can protect their sensitive, proprietary, or privileged information while complying with these clauses.

**Personnel Screening and Management.** Agencies have greatly expanded their oversight and control of the contractor workforces that develop, operate, or maintain government information systems, or that have access to government information.

As part of their information security programs, agencies often require personnel screening as a condition for access to IT systems and data. Examples of the types of highly personal data that agencies have required from contractor personnel include:

- Standard Form 85P ''Questionnaire for Public Trust Positions (requiring personal information such as drug use, police records, and financial data);
- FD-258 ''Applicant Fingerprint Chart'' (fingerprint biometric data); and
- Fair Credit Reporting Act (FCRA) Authorization Form (credit checks and financial information).

Such screening requirements not only limit the contractor's applicant pool for doing the job, but increase the volume of high-risk data contractors must maintain and protect.

*HHS Contractors*. Agencies can place contractors in the dicey position of proposing the most qualified people, but without knowing whether their personnel have a reasonable chance of being cleared in a screening. The Department of Health and Human Services' (HHS) regulations on Personal Identity Verification require screening based on the sensitivity level of a position, in the event that the position requires contractor personnel to have routine physical access to an HHS-controlled facility, logical access to an HHS-controlled information system, access to sensitive HHS data or information, or any combination of these types of access. HHSAR 304.13. Given that ''[i]nvestigations are expensive and may delay performance'', HHS has shifted the risk to the contractor to make an initial determination as to the likelihood of its personnel being cleared:

> Accordingly, if position sensitivity levels are specified in paragraph (c), the Offeror shall ensure that the employees it proposes for work under this contract have a reasonable chance for approval.

HHSAR 304.13. But HHS does not necessarily have to include the sensitivity levels of positions in a solicitation, instead stating such sensitivity levels are ''To Be Determined at the Time of Award.'' As a result of these personnel security rules, a contractor may be delayed or even unable to perform if its personnel subsequently fail the agency's ''TBD'' security standards.

*DHS Contractors*. When a contract requires contractor personnel to have individual access to agency IT resources, some agencies have constrained contractors' staffing choices based on the nationality of the personnel. For example, Department of Homeland Security (DHS) regulations require that all contractor personnel that will have access to DHS IT resources—regardless of the classification of the information—must be U.S. citizens:

> Non-U.S. citizens shall not be authorized to access or assist in the development, operation, management or maintenance of Department IT systems under the contract, unless a waiver has been granted by the Head of the Component or designee, with the concurrence of both the Department's Chief Security Officer (CSO) and the Chief Information Officer (CIO) or their designees.

HSAR 3052.204-71(k). To obtain a waiver, there must be a compelling reason for using a specific non-U.S. citizen rather than a U.S. citizen, and the waiver must be in the best interest of the government, which is a rather subjective test.[1]

*Commerce Contractors*. Once contractor personnel pass the initial hurdle for access to government IT systems or data, agencies may still retain the right to revoke that access. Some solicitation provisions appear to confer agencies with open-ended discretion to disqualify personnel or revoke their access rights. For example, in a DOC solicitation for Enterprise System Support Services, the following clause put contractor personnel in jeopardy of having system access revoked for a whole spectrum of conduct ranging from falsification on documents submitted to DOC to ''infamous . . . or notoriously disgraceful conduct'':

> Notification of Disqualifying Information. If the Office of Security receives disqualifying information on a contract employee, the COR will be notified. The COR, in coordination with the contracting officer, will immediately remove the contract employee from duty requiring access to Departmental facilities or IT systems. Contract employees may be barred from working on the premises of a facility for any of the following:
>
> * * *
>
> (3) Improper conduct once performing on the contract, including criminal, infamous, dishonest, immoral, or notoriously disgraceful conduct or other conduct prejudicial to the Government regardless of whether the conduct directly related to the contract.
>
> (4) Any behavior judged to pose a potential threat to Departmental information systems, personnel, property, or other assets.

How does a contractor train its employees to avoid ''infamous . . . or notoriously disgraceful conduct''?

*USPS Contractors*. In another example from a United States Postal Service (USPS) solicitation for a Federal Cloud Credential Exchange, the USPS provision on the security clearance process allows denial or revocation of a personal clearance ''based on appraisal of circumstances surrounding serious incidents involving the employee or applicant related to'' such incidents as:

- ''Dismissal from prior employment for cause.''
- ''Habitual use of intoxicating beverages to excess.''

[1] A prior version of this provision only allowed individuals that were legal permanent residents of the United States, or citizens of Ireland, Israel, the Republic of the Philippines, or any nation on the Allied Nations List maintained by the Department of State to receive waivers. This earlier provision was used in solicitations as recently as 2012, including for the Remote Video Surveillance System Upgrade.

■ ''Any legal other disqualification which makes the applicant unfit for the Postal Service, this would include but not be limited to bankruptcy and credit history.''

**Risk Allocation, Liability, and Penalties.** Increasingly, federal agencies have reallocated huge risks for security breaches to contractors through indemnification and penalty provisions. Given that government systems and databases often contain high-value sensitive data targeted by a wide spectrum of hackers, contractors may be shouldering potentially catastrophic risks through these indemnification and penalty provisions that have become much more common in agency regulations and solicitations.

**Indemnification Provisions.** Some agencies have included broad indemnity provisions, effectively shifting indefinite and potentially ruinous liability to contractors. For example, a Department of Interior solicitation for cloud services included the following provision by which the contractor agrees to indemnify the government for damages sustained arising from any fault, negligence, or wrongful act by the contractor or any of its agents:

> The Contractor shall hold and save the Government, its officers, agents and employees, harmless from liability of any nature or kind, including costs and expenses to which they may be subject, for or on account of any or all suits or damages of any character whatsoever resulting from injuries or damages sustained by any person or persons or property by virtue of performance of this contract, arising or resulting in whole or in part from the fault, negligence, wrongful act or wrong mission of the Contractor, or any subcontractor, or their employees, agents, etc.

In the USPS solicitation for the Federal Cloud Credential Exchange, a similar indemnification provision shifts all liability to the contractor for damages resulting in whole or in part from negligent acts or omissions of the contractors or any of its agents:

> The supplier must save harmless and indemnify the Postal Service and its officers, agents, representatives, and employees from all claims, losses, damage, actions, causes of action, expenses, and/or liability resulting from, brought for, or on account of any personal injury or occurring, or attributable to any work performed under or related to this contract, resulting in whole or in part from negligent acts or omissions of the supplier, any subcontractor, or any employee, agent, or representative of the supplier or any subcontractor.

By pushing full liability to the contractor for ''all'' losses or damages that result ''in part'' from a contractor's negligent act or omission, the contractor may have indemnified the government not only for the contractor's own negligence, but also for any contributory negligence of the government. With respect to cyber attacks on government IT systems or data, contractors need to ask whether such one-sided allocations of liability may expose them to bet-the-company risks from a massive cyber breach.

**Liquidated Damages and Penalty Provisions.** For certain breaches involving personally identifiable information, agencies have used liquidated damages and penalty provisions to define the contractor's liability on a per-record basis in the event of a breach.

The VA has a liquidated damages provision for breaches of ''sensitive personal information,'' which includes ''any information about an individual that can reasonably be used to identify that individual that is maintained by VA.'' VA Handbook 6500.6 ¶ 6(24); *id.*, Appendix C ¶ 7. In response to a May 2006 breach of personal data of 26.5 million individuals caused by the VA, Congress passed legislation relating to the VA's information security program, requiring the VA to include a liquidated damages provision in contracts ''for the performance of any Department function that requires access to sensitive personal information.'' 38 U.S.C. § 5725(a). As a result, the VA developed a provision that allocates liability to the contractor on a per affected individual basis. Recent VA solicitations implementing this regulation have set this amount at $37.50 per affected individual:

> [T]he contractor shall be responsible for paying to the VA liquidated damages in the amount of $*37.50* per affected individual to cover the cost of providing credit protection services to affected individuals consisting of the following:
>
> (1) Notification;
>
> (2) One year of credit monitoring services consisting of automatic daily monitoring of at least 3 relevant credit bureau reports;
>
> (3) Data breach analysis;
>
> (4) Fraud resolution services, including writing dispute letters, initiating fraud alerts and credit freezes, to assist affected individuals to bring matters to resolution;
>
> (5) One year of identity theft insurance with $20,000.00 coverage at $0 deductible; and
>
> (6) Necessary legal expenses the subjects may incur to repair falsified or damaged credit records, histories, or financial affairs.

The VA determines the amount of money a contractor will owe per affected individual based on an independent risk analysis performed by a non-Department entity or the VA Office of Inspector General. VA Handbook 6500.6, Appendix C ¶ 7. This risk analysis determines the level of risk associated with a data breach for the potential misuse of any sensitive personal information involved in the data breach. *Id.*, ¶ 7(b).

HHS has also included a provision that explicitly pushes liability to the contractor for remediating the effects of breach of individual's personal data. In a solicitation for the Online Respirator Medical Questionnaire, HHS included the following provision:

> In the event of a breach, the contractor shall be liable for $500 per effected user. The contractor shall be liable for the Government's costs to notify and/or remediate the breach of private personal data with FOH customers. Based on the nature of the breach, the Government shall define a remediation plan, and the contract shall support the defined actions. In addition to restitution for the labor efforts to coordinate the notifications, this remediation shall include the cost of providing credit protection to all effected people.

The solicitation provides no basis for how HHS determined that $500 per effected user was an appropriate amount. For breaches involving millions of individual records (like the VA or TRICARE breaches), such a clause could expose a contractor to billions of dollars of liability – and effectively put the company out of business.

**Conclusion.** Agency-specific regulations and solicitation provisions governing cybersecurity have significantly raised the stakes for government contractors that must not only deal with the expanding compliance burdens of coping with differing agency-by-agency security

  FCR ISSN 0014-9063

rules, but also the escalating contractual and enforcement risks arising from these agency requirements for cybersecurity. Until either Congress or the FAR Council provide greater uniformity and consistency to the acquisition regulations governing information security, contractors must exercise great caution to assure contractual compliance – while avoiding the assumption of bet-the-company risks – arising from the thicket of agency-specific regulations and provisions imposing tougher security requirements.