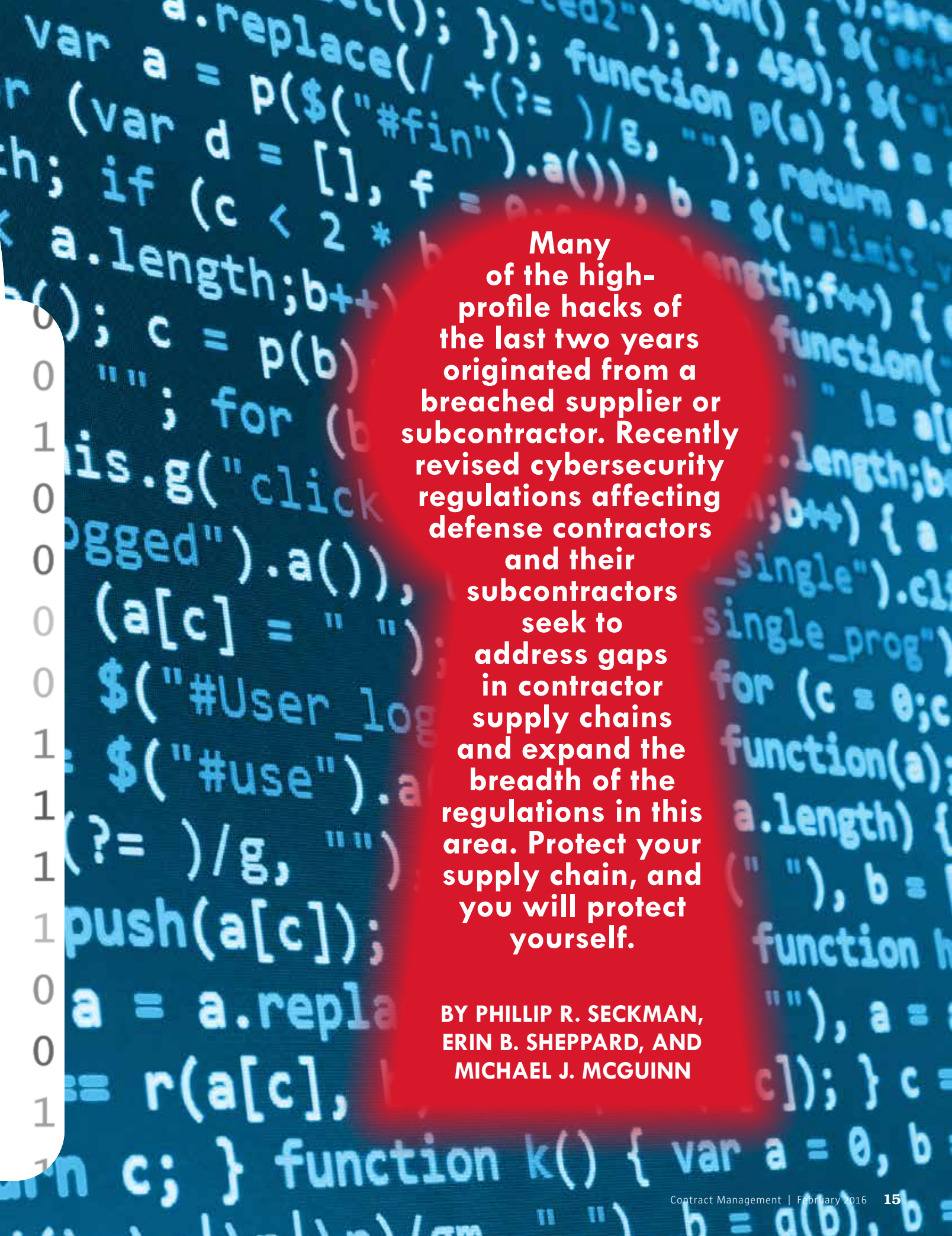
CYBERSECURITY AND YOUR SUPPLY CHAIN: WHAT YOU DON'T KNOW MAY HURT YOU



Many of the high-profile hacks of the last two years originated from a breached supplier or subcontractor. Recently revised cybersecurity regulations affecting defense contractors and their subcontractors seek to address gaps in contractor supply chains and expand the breadth of the regulations in this area. Protect your supply chain, and you will protect yourself.

BY PHILLIP R. SECKMAN, ERIN B. SHEPPARD, AND MICHAEL J. MCGUINN

Target, Home Depot, AT&T, Goodwill, Lowe's, AutoNation, the U.S. Office of Management and Budget—cyber breaches involving these major U.S. organizations have been headline news over the past two years.

Although each hack differed in its method and scope, the common thread among them is where they reportedly started—with the companies' suppliers and subcontractors. Subcontractors lacking basic safeguarding and reporting controls are increasingly considered the path of least resistance in cyberattacks, and these entities are frequently targeted by "black hat" hackers, both for the information they possess and the access they can provide.

Securing the supply chain is a particularly vexing problem in the government contracts market, where high stakes and huge costs are intertwined with supply chain hyper-specialization, directed teaming agreements, and small business goals. There is a growing recognition that adequate cybersecurity for government contracts requires prime contractors to take significant steps to provide not just for their own cybersecurity, but also for that of their subcontractors.

On August 26, 2015, the Department of Defense (DOD) continued its efforts to address contractor cybersecurity by updating a contract clause in the *Defense Federal Acquisition Regulation Supplement* (*DFARS*), "Safeguarding Covered Defense Information and Cyber Incident Reporting" (i.e., DFARS 252.204-7012).[1] This clause—issued via an interim rule and updating a prior clause that had dealt with DOD contractors handling "unclassified controlled technical information" (UCTI)—imposes mandatory security controls and reporting obligations on DOD contractors handling "covered defense information." On December 30, 2015, DOD revised these requirements via another interim rule that affords contractors until December 31, 2017, to fully implement the required security controls.[2]

The updated *DFARS* covered defense information clause is sweeping in its scope. The clause applies to every DOD contract, prime and sub, large and small, and regardless of procurement value, that will involve covered defense information. It requires prime contractors to flow the clause down to any subcontractor throughout the supply chain that is providing operationally critical services or any subcontractor whose subcontract performance will require access to covered information systems. Other than mandating standard flow-down language, however, the updated interim clause remains, frustratingly, silent on how prime contractors should provide for their supply chain's cybersecurity.

In our experience, primes have been struggling with the question of how best to ensure their own compliance with the stringent requirements of the updated *DFARS* clause while also taking steps to provide for the cybersecurity of their supply chain. DOD's August 26, 2015, interim rule will obligate contractors and subcontractors that had begun work to comply with the prior UCTI clause to reassess their compliance under the updated clause, while the December 30, 2015, interim rule will provide more time to accomplish full compliance.

This article provides three steps for contractors to follow to best enhance subcontractor compliance under the updated *DFARS* covered defense information clause. Although targeted at the covered defense information clause, these steps will be helpful for any government contractor subject to cybersecurity obligations that is considering how best to manage supply chain compliance.

Step 1: Read Your Contract(s)

The golden rule of government contracts is to *read* your contract(s). This is the fundamental first step to identify, assess, and control contractual requirements and responsibilities. Unfortunately, this step is often given limited attention, to the contractor's peril.

Contractors that invest the time to review and understand their potential contractual obligations prior to submitting a proposal or, at a minimum, immediately upon contract award, will better understand their compliance obligations. In particular, contractors should check "Section I" of their prime contracts or their relevant appendix/exhibit of subcontracts to determine if DFARS 252.204-7012 is included. Likewise, contractors should also review their contracts to determine whether they include other, similar agency-specific security obligations. Typically, such additional clauses will appear in "Section H."

Reading each prime contract and consulting with project teams can result in a proper assessment of the scope of information the contractor may receive that is or may be marked, and which would constitute "covered defense information" under the updated *DFARS* clause. Additionally, given the August and December interim rules, contractors must assess whether their prime contracts contain the prior UCTI version of the clause or the updated *DFARS* clause so as to appropriately flow down the applicable clause and other information security clauses.

More important, the prime contractor should consider other additional subcontract terms that may be necessary to protect the company from further liability. Additional clauses to consider, although not mandatory under the *Federal Acquisition Regulation* (*FAR*) and *DFARS*, include the following.

REQUIREMENT FOR SUBCONTRACTORS TO REPORT ANY INCIDENT AFFECTING THEIR SUBCONTRACT-RELATED DATA, WITHOUT EXCEPTION

Flowing down such an expanded reporting obligation effectively eliminates any reporting discretion the subcontractor may have had. It leaves the determination of whether the information at issue constitutes "covered defense information" or UCTI up to the prime contractor. Such an expanded reporting obligation would have to be included in the subcontract separately and drafted in a manner that is complementary to the updated *DFARS* clause. This is the case because the December 2015 interim rule also clarified that the updated *DFARS* clause is to be flowed down to subcontractors with very limited adjustments.

SHORTENED SUBCONTRACTOR REPORTING TIMEFRAME

The new interim rule requires subcontractors to report incidents directly to DOD and then provide the prime contractor with the incident report number as soon as practicable. Prime contractors seeking to comply with similar reporting provisions may nevertheless wish to shorten subcontractor reporting timelines to ensure the prime can meet the rapid reporting requirements of such clauses. The predecessor UCTI rule, for example, required prime contractors to report on behalf of subcontractors. Again, while the December 2015 interim rule clarifies that contractors must flow down the clause without alteration, this does not preclude prime contractors from requesting additional reporting to the prime contractor in addition to the direct reporting obligations under the 252.204-7012 clause, provided a prime contractor's adjustments do not create conflicts or ambiguity.

ENHANCED INDEMNITY CLAUSE

Prime contractors may wish to specifically indemnify themselves from liability stemming from a subcontractor's failure to implement required security controls, thereby shifting the risk of noncompliance

with flow-downs squarely on to the subcontractor. Primes might look to analogous clauses (e.g., defective pricing indemnities) as a framework for crafting the indemnity.

Subcontractors, on the other hand, would be well advised to limit such clauses so they only trigger the subcontractor's obligation to indemnify based on the prime's receipt and payment of a claim from the government. Subcontractors should also seek to ensure they are included in prime contract settlement discussions and preserve a right for pass-through or other dispute remedies so that the prime is not too quick to settle, knowing the subcontractor is "on the hook."

REQUIRED INSURANCE CLAUSE

Obligating subcontractors to obtain insurance to cover a data breach or other cyber incident may help shift at least a portion of the risk away from prime contractors. In fashioning such clauses, prime contractors should consider requiring certificates of insurance to confirm such coverage.

CLEAR DATA ACCESS RIGHTS CLAUSE IN THE EVENT OF AN INCIDENT

Although subcontractors may balk at requests for unfettered access to information in the event of a data breach, prime contractors should consider securing access to certain technical information (e.g., logs, packet-flow information, etc.) in the event of a breach to enable the prime contractor to satisfy DOD information requests.

Step 2: Determine How Much You Need or Want to Know Regarding Your Subcontractors' Compliance

Contractors have a range of options when it comes to subcontractor compliance with flow-down clauses. When determining how thoroughly to vet and assess subcontractor cyber capability and compliance, contractors should weigh the risks associated with the work that a particular subcontractor is performing and ensure that they have all information necessary to document and, if necessary, demonstrate compliance.

At one end of the spectrum, prime contractors can flow down applicable cyber clauses to their subcontractors and do nothing else. This is, after all, what these prime contract clauses require, and contractors may be able to defend this hands-off approach on that basis. However, it is fairly high-risk, particularly when flowing down such clauses to an unsophisticated small business and then providing that business with significant amounts of covered defense information. If a significant breach occurs and the small business is the cause, the government, potential relators, private plaintiffs, and the general public will look to identify any and all responsible parties. The public, after all, knows about the Target breach, not the breach of Fazio Mechanical Services, the Target HVAC subcontractor from whom network credentials were reportedly stolen and used to infiltrate Target's networks.

Toward the other end of the spectrum are more hands-on approaches for prime contractors. These include supplier checklists, certifications of compliance, outside vendor verification, and onsite security audits. Contractors may also consider offering suppliers resources to assist with compliance, including training, information on threats and security requirements, and other available resources on cybersecurity. These approaches give the contractor reasonable insight into a supplier's cybersecurity posture and/or provide reasonable assurances of security.

The most straightforward of the more hands-on approaches, and one adopted in other flow-down contexts, is to obtain a certification or representation from the subcontractor that it has implemented the required security controls. This approach may be sufficient for instances in which the prime does not believe the subcontractor will be handling a substantial volume of covered information or, alternatively, the subcontractor already has a demonstrated history of strong information security compliance.

There may be cases, however, where merely obtaining a certification is insufficient. These may include, for example, instances in which a subcontractor will be taking a critical role in the housing, processing, or creation of covered defense information. In these circumstances, particularly those where the subcontractor is a sole-source supplier, the prime contractor may need to go beyond certification and, instead, engage in a verification process. Such a verification could take the form of a third-party security audit or even an audit by the prime contractor, depending upon the subcontractor's willingness to provide necessary access. Other "trust but verify" options include requiring subcontractors to provide copies of annual security audits or other internal security reviews.

GOT ETHICS?

THERE IS NO BETTER WAY TO STRENGTHEN YOUR ORGANIZATION

NCMA's new ***self-paced*** Ethics for Contract Management Professionals online e-course can be viewed from work or home and as many times as you want!

The highly interactive course ***explains the concepts of ethics***, allows you to ***solve ethical problems***, is filled with clickable real-world examples and provides numerous available resources. Plus, there's an evaluation at the end to ***test your knowledge***.

The course takes one hour to complete and is valued at one continuing professional education (CPE) hour.

SIGN UP TODAY AT WWW.NCMAHQ.ORG/ECOURSES.

NCMA
NATIONAL CONTRACT MANAGEMENT ASSOCIATION

The danger to the foregoing hands-on approaches is that they may provide a prime contractor with answers it does not like (e.g., that the subcontractor is noncompliant with a flow-down clause's security control requirements). Then what? In addition to adopting a mechanism for confirming subcontractor compliance, contractors need to develop protocols for how to handle key suppliers that cannot comply or are unable to make the desired representations. Depending on the importance of a supplier and the extent of the subcontractor's potential noncompliance, the prime contractor may wish to seek approval from the government to subcontract or, at a minimum, put the contracting officer on notice of how the prime contractor has interpreted and complied with its obligations relative to the subcontractor's compliance. Being upfront with the contracting officer may eliminate difficulty on the back end should the subcontractor experience a cyber incident.

As a corollary, because DOD may be unwilling to make exceptions for noncompliant suppliers, prime contractors should consider whether alternate vendors and/or suppliers for critical supplies/services are available or can be developed should their first-choice subcontractor refuse to provide a requested certification or be deemed noncompliant in some other fashion. The industry is still beginning to develop its capacity in this area, so contractors should be prepared to consider alternatives in the event that a key subcontractor cannot proceed due to inadequate security controls. Because the December 2015 interim rule affords contractors a longer timeframe for implementing the required security controls, there may be less of a need to look for other subcontractors. However, the revised clause does require contractors to implement the protections "as soon as practical," and no later than December 31, 2017. Accordingly, if a subcontractor communicates that it does not intend to comply with this requirement within that timeframe, prime contractors should consider lining up a replacement. Difficult as it may be to end a longstanding relationship or change subcontractors mid-program, absent agreement from the contracting officer, the penalties for noncompliance may be even worse.

What is clear from this discussion is that one solution is not best in all circumstances. Although the recently extended deadline for implementation of the *DFARS* security measures recognizes that 100-percent compliance across the entire DOD supply chain is simply impracticable in the short term, the requirement to comply by December 2017 still exists, and this additional time will not lessen the compliance costs on small- to mid-sized businesses in the DOD supply chain. In meeting this final deadline, there also should be some recognition that a risk-based approach is reasonable in this area—one that considers the specific cyber threats to suppliers, the security controls and reporting procedures in place at suppliers, and the type and significance of data that suppliers may have or receive. A similar risk-based approach was recently adopted by the Defense Contract Management Agency in connection with DOD's counterfeit parts detection and avoidance rules.[3] It is likewise the only reasonable and feasible approach for supply chain cybersecurity.

Step 3: Team with Suppliers to Implement Best Practices to Prepare for and Respond to a Breach

The final step builds on the work done as part of Step 1, and involves contractors taking measures to shore up internal defenses and lay the procedural groundwork for strong cyber compliance. Contractors should implement policies and procedures to foster a culture of compliance within the company. This involves proactive training on cyber obligations, as well as a cyber incident/crisis management response plan with clear roles and responsibilities assigned to each stakeholder.

This step should include creating an inventory of reporting obligations to comply with in the event of an incident. Further, contractors should identify the "go-to" personnel for responding to such incidents and should

assign backups for each of those positions to ensure redundancy in the response system. As part of this, contractors may wish to establish relationships with key external stakeholders, such as the law enforcement and government personnel to whom the company has reporting obligations.

In addition to crafting procedural protections, contractors should familiarize themselves with certain threat trends, such as the fact that contractors' systems are more likely to be attacked after business hours and during holidays because attackers are keenly aware of when companies are more likely to have their guard down. Recognizing this fact and ensuring vigilant surveillance and response capabilities at all times are critical attributes of effective response plans.

When striving to incorporate UCTI compliance into daily operations for those contracts that continue to contain the legacy clause, contractors should recognize that confirming the sensitivity of data may not be as easy as ascertaining whether something has been marked with a distribution statement. Contractor personnel tasked with ensuring compliance with the updated or legacy *DFARS* clauses should work closely with their respective project teams to assess the scope of work being performed and its connection to national security. Erring on the side of overprotection will help shore up contractor defenses at all tiers.

Indeed, DOD's interim rule only further expands the potential categories and types of information that may be subject to compromise—and therefore reporting—under the updated clause. Rather than addressing just UCTI, the revised clause now applies to not only the same information that would qualify as UCTI, but also "[a]ny other information, marked or otherwise identified in the contract, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and governmentwide policies (e.g., privacy, proprietary business information)."[4] This expansion of the categories and types of information subject to potential cyber incidents and reporting suggests that contractors must re-double their efforts to implement appropriate security controls, policies, procedures, and training. Whereas contractors may have previously complied with the UCTI clause by isolating such information to specific areas on their information system, the interim rule's significant expansion of the types of data subject to the clause is likely to render that compliance strategy quite difficult, if not impossible.

Finally, contractors should encourage and team with their subcontractors to adopt similar best practices to prepare for and respond to breaches. Contractors may want to consider involving certain key or small business suppliers in their training programs, or to host a separate training on supply chain cybersecurity. Prime contractors may consider making forensic resources available to the subcontractor in the event of a breach. Notwithstanding a supplier's inability to comply with the security controls of the updated *DFARS* clause, prime contractors should also emphasize and prioritize the requirement that suppliers report all cyber incidents and comply with all preservation requirements. Emphasizing a teaming approach will best ensure the parties properly assess, report, and ultimately recover from cyber incidents.

Conclusion

There is no question that government contractors are facing an ever-increasing maze of cybersecurity compliance requirements. With the recent release of the National Institute of Standards and Technology Special Publication 800-171, the changes DOD has made to the "Covered Defense Information and Cyber Incident Reporting" clause and the ongoing rule-making from the National Archives and Records Administration, we anticipate in the near term that nearly all federally funded procurement contracts and grants will contain some form of cybersecurity compliance requirements—requirements that primes likely will have to flow down to their subcontractors.

Now is the time to focus on enhancing both your own cyber compliance and the security of your supply chain. **CM**

ABOUT THE AUTHORS

PHILLIP R. SECKMAN is a partner with Dentons' Government Contracts Practice Group and his practice spans a broad range of subjects related to federal procurement law, state and local procurement law, and complex federal regulatory issues. He concentrates his practice in the areas of commercial item acquisitions, GSA Schedule contracting, cybersecurity compliance and internal investigations, and bid protests (both federal and state).

ERIN B. SHEPPARD is counsel with Dentons' Government Contracts Practice Group and regularly counsels clients on breach response, cybersecurity legislative and regulatory developments, and in the development of cybersecurity compliance programs. She has extensive experience counseling clients on a broad array of contract matters, including bid protests, performance disputes, claims, terminations, regulatory compliance, cybersecurity, data rights, Freedom of Information Act responses, and internal investigations.

MICHAEL J. MCGUINN is a senior managing associate with Dentons' Government Contracts Practice Group and represents clients in a broad range of government contract matters, including contract claims, internal investigations, and regulatory compliance issues. He concentrates his practice in the areas of cybersecurity, contractor business systems, contract changes, and commercial item acquisitions.

Send comments about this article to cm@ncmahq.org.

ENDNOTES

1. 80 *Fed. Reg.* 51,739-48.
2. 80 *Fed. Reg.* 81,472-74.
3. *See* DCMA INST 1205 (July 6, 2015).
4. 80 *Fed. Reg.* 51,745-46.