

CYBERSECURITY INSURANCE—

MITIGATING COMPLIANCE RISK
UNDER THE *DFARS* AND OTHER
FEDERAL REGULATIONS





RITY

BY

WALTER J. ANDREWS
LORELIE S. MASTERS
MICHAEL S. LEVINE
AND LATOSHA M. ELLIS



AS CYBERATTACKS AND OTHER DATA LOSS INCIDENTS CONTINUE TO PLAGUE CONTRACTOR INFORMATION SYSTEMS, BUSINESSES HAVE MITIGATED THIS RISK BY IMPLEMENTING AND ENHANCING SAFEGUARDS.

Protecting sensitive or confidential information is a particular challenge for prime defense contractors, whose business models entail collaborative work with affiliates and downstream subcontractors. While a prime contractor's systems may be state-of-the-art, downstream systems may not be so robust. To paraphrase the adage, a security chain is "only as strong as its weakest link."

So, how is a government prime contractor to mitigate the potential financial risks associated with downstream data breaches or releases due to faulty or inadequate safeguards? As a threshold matter, due

diligence regarding a subcontractor's systems by the prime contractor's subject matter experts, together with apt contract safeguards, will provide a baseline level of comfort. However, financial risks associated with subcontractor-level data breaches or releases (whether or not resulting from a subcontractor's failure to comply with contract requirements) may result in financial liability to the prime contractor.

In these instances, a robust insurance program may be the solution to "backstop" these financial risks.

DFARS 252.204-7012: THE GOVERNMENT'S RESPONSE TO CONTRACTOR CYBERSECURITY RISK

In response to increased government contractor exposure to cyberattacks and data breaches, the federal government has issued regulations governing the level of cybersecurity required for those engaging in work with the government. One of the most rigorous of these rules applies to defense contractors and is found in the *Defense Federal Acquisition Regulation Supplement (DFARS)*.

This is DFARS 252.204-7012, "Safeguarding Covered Defense Information and Cyber

Incident Reporting,” which aims, among other things, to protect the IT supply chain and unclassified information systems of government contractors by ensuring primes and their subcontractors have “adequate security” in place.¹ The clause defines *adequate security* as “protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of, information.”²

Under this clause, the Department of Defense (DOD) requires contractors to maintain “adequate [cyber] security on all covered contractor information systems” that process, store, or transmit covered defense information and comply with more than 100 federal cybersecurity guidelines.³ Contractors that do business—or are considering doing business—with the DOD must assess whether their cybersecurity programs meet certain minimum security standards. Furthermore, DOD contractors and subcontractors are required to report, among other things, cyber incidents that result in an actual or potential adverse effect on—

- A covered contractor’s information system,
- Covered defense information residing on the covered contractor’s information system, or
- The contractor’s ability to provide operationally critical support.⁴

Troubling for some prime contractors are the clause’s mandatory “flow-down” provisions.⁵ These provisions require prime contractors to impose, or “flow down,” the DFARS requirements to their downstream subcontractors if those subcontractors handle covered defense information or provide operationally critical support.⁶ The stakes connected to noncompliance with the DFARS cybersecurity requirements, including the flow-down requirements, are high. At an extreme, the federal government may suspend or debar prime contractors from doing business with the government due to the noncompliance, or due to a failure to demonstrate sufficient system integrity at the contractor level or subcontractor level.⁷

At this time, it remains unclear the extent to which prime contractors will be liable for the actions or inactions of subcontractors or other third-party vendors under the DFARS following a data or privacy breach. There has been no public reporting of such events. However, adequate cyber insurance can help a government contractor mitigate the wide-ranging financial risks.

As with any insurable risk, however, defining the scope of risk to be insured is critical. Only after that scope is defined can a policyholder ensure that its risk profile is properly protected.

STEP 1: DEFINE THE CYBERSECURITY RISK RELATED TO SUBCONTRACTORS

As an initial step, it is important for prime contractors to become knowledgeable about their subcontractors’ capabilities and vulnerabilities as they relate to cybersecurity. A proper assessment begins with an understanding of the existing contractual obligations the subcontractor has to the prime contractor, and vice versa. This should start with a review of the prime’s subcontracts to ensure subcontractors are required to address cybersecurity issues, including those arising under the DFARS.

What Subcontracts Should Require

Both new and existing subcontracts should require the subcontractor to—

- Implement and maintain the DFARS’ specific security measures, including requiring the subcontractor to notify the prime contractor of noncompliance or cyber incidents that may affect the information of the federal customer or the prime contractor;
- Purchase cyber insurance and related coverages with sufficient limits and list the prime contractor as an additional insured; and
- Include in the subcontracts’ cybersecurity indemnification clause exceptions for any relevant exclusions for the subcontractors’ failure to comply with the DFARS’ cybersecurity requirements.⁸

These precautions will enable the prime contractor to find coverage under the subcontractor’s insurance policy in the event of a data or privacy breach.

Data Considerations

Prime contractors also need to know the type of data that will be shared, accessed, stored, or maintained on subcontractors’ systems, and should determine whether—

- The data are classified,
- The subcontractor understands the applicable statutory requirements the DFARS imposes concerning data,
- The contract with the subcontractor is subject to federal regulations aside from the DFARS, and
- Subcontractors’ insurance and cybersecurity processes are sufficiently robust to adequately respond to reasonably anticipated threats.

Prime contractors should understand what, if any, security measures subcontractors have in place to safeguard data. Such verification can range from allowing subcontractors to self-certify compliance with the DFARS to the prime contractor periodically auditing or testing the subcontractors’ systems. Understanding the type of data on a subcontractor’s system and the risk control measures in place allows the prime contractor to assess the potential exposure the subcontractor has for a data or privacy breach.

STEP 2: INSURING RISKS ARISING FROM DFARS COMPLIANCE

The second step is to ensure that the prime contractor’s insurance program sufficiently contemplates coverage for its specific DFARS-related financial exposures related to work with subcontractors. This process begins with a careful examination of representations and warranties provided to prospective insurers. This also includes reviewing any post-inception endorsement or modification based on changing circumstances.

Determine Current Coverage Under Existing Policies

As a threshold matter, a prime contractor should inspect the insurance coverage in



BE PREPARED FOR THE TEST OF YOUR CAREER

With **NCMA's Online Prep Courses**

You've set your goal for the year—now it's time to make sure you meet it. Elevate your career in less than three months. Over 80% of participants pass the exam with NCMA's help. Make sure your career doesn't get left behind.

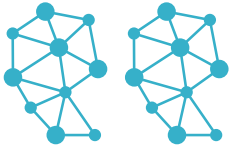
CFMTM
CERTIFIED FEDERAL CONTRACT MANAGER



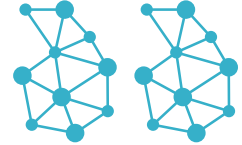
CPMTM
CERTIFIED PROFESSIONAL CONTRACT MANAGER

Register today at www.ncmahq.org/certopc

 **NCMA**
NATIONAL CONTRACT MANAGEMENT ASSOCIATION
CONNECTING TO
CREATE WHAT'S NEXT



...A SECURITY CHAIN IS 'ONLY AS STRONG AS ITS WEAKEST LINK!'



its existing policies. It may be that some coverage for a cyber event is already available in the “traditional” and other insurance policies that may fall outside the general category of “cyber insurance.” For example, “commercial general liability” (CGL) primary, umbrella, and excess policies may provide some coverage for invasion of privacy or privacy/confidentiality allegations.⁹ Meanwhile, “directors and officers” (D&O) insurance may cover derivative and other shareholder actions brought against the board of directors for alleged failures to act consistent with their duties of care and loyalty to the corporation or to exercise proper business judgment in preparing for or dealing with a cyber event. A strong D&O insurance program, coupled with fiduciary liability insurance to protect trustees of the company’s benefit plans, may respond to some of the notification expenses to comply with federal breach notification laws and certain penalties arising from a cyber event.

Other lines of insurance coverage that may provide some limited protections against a cyber event, depending on the claim and the scope of coverage the prime contractor has, include “employment practices liability,” “crime coverage,” “technology errors and omissions,” and “kidnap and ransom” policies. Identifying the gaps between policies is crucial to ensure the risk transfer and insurance protection are as seamless as possible. Regular review of insurance programs is key to helping companies determine how any existing and/or new insurance programs should be structured, and whether new

insurance coverage or additional limits are necessary, to ensure maximum coverage for DFARS-related exposures.

Insurance Application Considerations

With respect to the application process, prime contractors should devote particular attention to renewal policies (as opposed to new coverages). Insurance renewal applications often incorporate representations made in prior applications—including answers on the company processes regarding subcontractors. These answers deserve careful consideration because insurers may argue at the point of claim that coverage is void due to some (often technical or unrelated) “misrepresentation.” It is important, therefore, to review both the application itself as well as any incorporated documents and statements. Ideally, language should be included in the application that negates prior representations and warranties in favor of only those representations and warranties that are to be contained in the renewal policy or policies.

Prime contractors should also be mindful of warranties made with respect to the contractor’s work, the oversight of subcontractors, and the conduct of other vendors or third parties. Risk-control measures in insurance applications should be described generally and broadly. Prime contractors should work diligently to adhere to the disclosed measures subsequent to the application so as not to risk claims of rescission by the insurer.

As an example, in *Columbia Casualty Co. v. Cottage Health Systems*,¹⁰ the insurer sued the policyholder to void coverage, alleging that the insured’s application represented that the policyholder would implement certain risk-control security measures and failed to do so, resulting in a data breach. The insurer further asserted that the breach resulted from a third-party vendor’s network failure that allegedly affected 32,000 confidential medical records. This “breach” made these records fully accessible via the internet because the third-party vendor had not installed encryption software or taken other reasonable measures to protect the data. The case—filed in May 2016—remains pending and shows the importance of making careful representations in policy applications to avoid unnecessary coverage disputes.

Thoroughly Review Insurance Policies

In addition to diligence in the application process, a thorough review of the policy form(s) and all endorsements should be done to ensure the coverage obtained is consistent with the scope and extent of cybersecurity measures in place with the various subcontractors. These reviews are important at the time of purchase or renewal for the company and at the time of contracting with any subcontractors or vendors whose security measures may affect the prime contractor. A thorough understanding of the contractual relationship with subcontractors and the extent of their cybersecurity capabilities and vulnerabili-



ties is crucial at this step. When properly executed, the review should inform the contractor whether an existing cyber insurance policy is sufficient to protect against any alleged noncompliance with the DFARS due to subcontractor noncompliance.

COVERAGE


Generally, well-structured cyber and related insurance policies and programs will cover a variety of liability losses that may result from a data breach, including the costs to defend claims by state regulators and the fines and penalties that may result from noncompliance with the DFARS. However, unlike other lines of coverage (e.g., CGL and “first-party property” insurance policies), cyber and related insurance policies lack uniformity and vary widely from one market to the next. Particularly with cyber liability insurance, there is no “one-size-fits-all” policy or program. Rather, there is a wide variety of cyber insurance forms and coverage options with large differences in pricing and underwriting guidelines.

Meticulous attention should be paid to the definition of the “insured network” and to the insured entities. Likewise, as subcontractors evolve or change, a subcontractor’s risk profile may change, requiring it to make post-inception modifications to coverage. Key definitions like “computer system” and “computer fraud” need to be coordinated across potentially applicable insurance programs to avoid unintended gaps in coverage.

Some insurers or markets have much more sophistication, and capacity, than others. Some insurers are more likely to pay claims or negotiate at the point of claim, particularly where there is an ongoing or long-term business relationship with the insurer. The ability to obtain these modifications and engage in fruitful negotiations at the point of claim varies widely among insurers. This emphasizes the importance of considering these issues at the time of procurement of insurance and contracting with subcontractors and other vendors.

CONCLUSION

The DFARS imposes a variety of cybersecurity requirements on contractors, including the expectation that prime contractors

oversee and require subcontractors to comply with DFARS cybersecurity requirements. As such, prime contractors should not assume their cyber and related coverage—or the insurance programs of their subcontractors and third-party vendors—adequately addresses cyber liability that may result from a failure to comply with the DFARS’ cybersecurity requirements. Further, prime contractors should also consider insurance issues in conjunction with indemnification and potentially other means of addressing or transferring risk. While the scope of prime contractors’ liability in this regard is uncertain, prime contractors can meet their obligations under the DFARS and mitigate cybersecurity risk by consulting with experienced coverage counsel to ensure their—or their subcontractors’—cyber and related insurance programs will respond if potential liability arises related to DFARS compliance. 

NCMA X COLLABORATE

Post about this article on
NCMA Collaborate at
<http://collaborate.ncmahq.org>.

WALTER J. ANDREWS, ESQ.

- ▶ Partner, Hunton Andrews Kurth
- ▶ Heads the firm’s insurance coverage practice

✉ wandrews@HuntonAK.com

LORELIE S. MASTERS, ESQ.

- ▶ Partner, Hunton Andrews Kurth
- ▶ Nationally recognized litigator and author on insurance and international arbitration

✉ lmasters@HuntonAK.com

MICHAEL S. LEVINE, ESQ.

- ▶ Partner, Hunton Andrews Kurth
- ▶ Nationally recognized litigator, author, and lecturer on insurance and indemnity issues

✉ mlevine@HuntonAK.com

LATOSHA M. ELLIS, ESQ.

- ▶ Associate, Hunton Andrews Kurth
- ▶ Expert in insurance recovery issues—including cyber risks

✉ lellis@HuntonAK.com

This article presents the views of the authors, which do not necessarily reflect those of Hunton Andrews Kurth LLP, its clients, or NCMA. The information presented is for general information and education purposes. No legal advice is intended to be conveyed. Readers should consult with legal counsel with respect to any legal advice they require related to the subject matter of this article.

ENDNOTES

1. *Federal Register* 78, no. 69 (Nov. 18, 2013) 268; *Federal Register* 78, no. 69 (Nov. 18, 2013) 273.
2. DFARS 252.204-7012(a).
3. DFARS 252.204-7012(b).
4. *Federal Register* 81, no. 192 (Oct. 4, 2016) 68312 (amending 32 C.F.R. pt. 236), available at <https://www.federalregister.gov/documents/2016/10/04/2016-23968/departement-of-defense-dods-defense-industrial-base-dib-cybersecurity-cs-activities>.
5. See DFARS 252.204-7012(m).
6. *Operationally critical support* is defined as “supplies or services designated by the government as critical for airlift, sealift, intermodal transportation services, or logistical support that is essential to the mobilization, deployment, or sustainment of the Armed Forces in a contingency operation.” (DFARS 252.204-7012(a).)
7. See *Federal Acquisition Regulation (FAR)* Subpart 9.4.
8. Note: Further consideration of these contract issues may be advisable given the interplay between insurance and indemnification as a means of transferring risk.
9. Note: Umbrella policies deserve a specific focus.
10. *Columbia Casualty Co. v. Cottage Health Systems* (Case No. 16CV02310, Superior Court of California, County of Santa Barbara, filed May 31, 2016), case information available through <https://portal.sbdcourts.org/CASBPORTAL/>.

This article presents the views of the authors, which do not necessarily reflect those of Hunton Andrews Kurth LLP or its clients. The information presented is for general information and education purposes. No legal advice is intended to be conveyed; readers should consult with legal counsel with respect to any legal advice they require related to the subject matter of the article. Receipt of this article does not constitute an attorney-client relationship. Prior results do not guarantee a similar outcome. Attorney advertising.