Whitepaper – Allowable Cost Issues for DFARS Cybersecurity Compliance October 2021

Introduction

Cybersecurity is a big – and expensive – issue for small DoD contractors and sub-contractors handling Controlled Unclassified Information or CUI. In June 2019 the DoD declared loudly that "Security is an allowable cost. Amen, right?". At the same conference the DoD speaker noted that "Only 1% of [Defense Industrial Base] companies have implemented all 110 controls from the National Institute of Standards and Technology." However, DoD guidance is currently limited on issues such as allocating these significant costs across multiple contracts, recurring vs. non-recurring costs and pre- vs. post- contact expenditures.

A 2020 case study looking at recurring cybersecurity costs for small contractors found hundreds of hours of annual costs as shown at right. This does not include the typically hundreds of hours needed to create an initial system security plan (SSP).

	2 Staff	7 Staff	20 Staff
Estimated Hours/year	217	411	830
IT Manager	98	187	371
Compliance Officer	118	224	460
% Full Time Equivalent	10%	20%	40%

This whitepaper will focus on cybersecurity cost issues for newly regulated small contractors up to 50 staff. As many as 1/4 of small DoD subcontractors are expected to leave this market over cybersecurity issues.

Literature Review

In July 2019 a commenter noted "It's clear that the cost of cybersecurity is a cost of doing business--specifically with the U.S. Government and from review of FAR 31.205, there is no prohibition on the allowability of cybersecurity costs. The better question is: can the cost be charged directly to a single contract and fully recovered? To that, I think the answer which your contracting officer (and likely DCAA) will provide is that the cost provides a benefit to multiple final cost objectives (contracts), and as a result, should be recovered via an indirect allocation for any contractor who has more than one government contract with the DFARS cybersecurity requirement(s). What that means, in practical terms, is that depending on your indirect rate structure, the likely place is either G&A, overhead, or maybe even a new service center."

An August 2020 article noted that "Once a contract is awarded, I can certainly see cybersecurity as an overhead cost. Yearly renewals for security licenses, full time cybersecurity engineers, regular penetration testing, audit and certification costs all make sense. These will continue over the life of your contract." However cybersecurity

costs prior to contract award are another issue. Increased overhead costs due to cybersecurity may impact bidding success.

Some official guidance was provided in the September 2020 DFARS Interim Cybersecurity Rule. On page 61514 of the Federal Register article a sample cost calculation is provided for CMMC Level 3 certification.

"Contractors pursuing a Level 3 Certification **should have already implemented** the 110 existing NIST SP 800–171 security requirements. Therefore, the estimated engineering costs per small entity is associated with implementation 23 new requirements (20 CMMC practices and 3 CMMC processes)."

This assumption ignores the fact that 80% of contractors audited by DCMA for 800-171 compliance failed the audit. A different audit found 0% of audited contractors to be fully compliant and "Small to mid-sized companies, on average, successfully implemented 34% of the controls."

"The estimated **nonrecurring engineering cost** per entity per assessment/ recertification is $26,214. The estimated **recurring engineering cost** per entity per year is $41,666."

Annual recurring costs may presumably be expensed as overhead or charged directly to the contact requiring CMMC compliance. Non-recurring costs may need to be capitalized.

Page 61512 notes that "It is estimated that the burden to make the system security plan and supporting documentation available for review by the DoD assessors, prepare for demonstration of requirements implementation, and to conduct post review activities is **304 hours per entity**". While this is more realistic than the earlier DoD estimates of 110 hours for SSP creation, it falls short of industry estimates of 400+ hours for SSP creation alone.

While limited to small sites the ACRMS 3535™ video boot camp developed for Air Force SBIR contractors reduces SSP creation times to less than 30 hours for sites up to 50 staff. Larger sites can use similar software from Modulo or other vendors.

Since late 2017, DFARS 252.204-7012 has required all contractors handling CUI to self-attest that they comply with the 110 cybersecurity requirements of NIST 800-171. There was no penalty for false attestation, and 80% of contractors audited by DCMA were found to be non-compliant. This situation changed significantly with the 2020 addition of DFARS 252.204-7019 to all new DoD contracts and contract renewals.

Under the 2020 interim rule DoD contractors must first take hundreds of hours to create a system security plan (SSP). The SSP is then used to quantitatively score 800-171 compliance using the DoD Assessment Methodology or DoDAM. The DoDAM score must be filed in the Supplier Performance Risk System (SPRS) database.

The SPRS filing creates a major new liability for small contactors. A Global 100 law firm noted that "It goes without saying that contractors will need to be careful here – an inaccurate report could subject a company to exposure under the False Claims Act."(FCA) In 2019 FCA penalties, including triple damages, exceeded $3.1 billion.

Following the September 2020 guidance a December 2020 article notes "Regarding DFARS 252.204-7012 in 2013, DOD stated … that costs related to complying with DFARS 252.204-7012 are likely allowable and chargeable to indirect cost pools. (See page 69274)". It goes on to discuss "Allowable Costs Under Cost Accounting Standards (CAS)

Comment: One respondent asked if the cost associated with compliance to the DFARS changes is allowable under CAS.

Response: Cost Accounting Standards address measurement, allocation and assignment of costs. FAR 31 and DFARS 231, specifically FAR 31.201–2, address the allowability of costs. There is nothing in FAR 31 or DFARS 231 that would make costs of compliance with DFARS unallowable if the costs are incurred in accordance with FAR 31.201–2."

A useful June 2021 article discusses "The Pitfalls of Factoring in Security and CMMC Costs". Quoting from the article "To conform with contract requirements, vendors are incurring additional costs to enhance cybersecurity capabilities and architect secure enclaves, whether on premise or in the cloud. While certain costs will be non-recurring, such as hardware upgrades and related engineering, other costs will be incurred on an ongoing basis.

The costs of procuring equipment, maintaining security assessment and continuous monitoring programs, salaries of security personnel, fees of managed security service providers, and renewals of security software licenses and subscriptions, should generally be considered as allowable for reimbursement under FAR Part 31 and the associated cost principles. However, much less clear is how contractors should allocate these costs to their contracts for recovery.

What criteria should a contractor consider when determining if costs are directly benefiting a contract, and therefore should be directly charged to a specific contract? And if costs benefit multiple contracts, including commercial work, how should they be allocated to the final cost objectives in accordance with Cost Accounting Standards? Answers to these questions ultimately affect whether the costs will be considered allowable by contracting officers.

As previously stated, the guidance behind the allowability of CMMC program costs has been general and limited. Regarding cost allocation, in an interview with Federal Computer Week, Stacy Bostjanick, CMMC director of policy in the office of the undersecretary of defense for acquisition and sustainment, stated: "Up to [CMMC] Level

3 will be included in your indirect rates. So, you don't get a direct charge to do it, but you do get to recoup the cost over time; you have to spread it across all of your business.""

Summary of Existing Guidance

While DoD guidance on cybersecurity cost recovery is not extensive, some consensus items exist.

- "… from review of FAR 31.205, there is no prohibition on the allowability of cybersecurity costs."
- Non-recurring and recurring cybersecurity costs may be treated differently.
- Recurring cybersecurity costs are typically allowable as overhead costs.
- Contracts after 11/30/2020 require an SSP with a DODAM score filed in SPRS.
- A false or inaccurate DODAM score filed in SPRS, possibly revealed during a contract dispute, can result in triple damages under the False Claims Act.
- SSP creation typically requires hundreds of hours without specialized software.

Additional Information

The ACR 2 Solutions CUI references page includes short instructional videos on topics such as rapid SSP creation, tracking and managing DFARS cybersecurity tasks for reimbursement and cybersecurity as a competitive advantage.