For defense government contractors that do business with the U.S. Department of Defense (DOD), compliance with the Defense Federal Acquisition Regulation Supplement (DFARS) is a necessity. DFARS serves as a supplement to the Federal Acquisition Regulations (FAR)—which governs federal contracting generally—and addresses cybersecurity risks that are unique to the defense contracting sector.

Since DFARS compliance is a matter of national security, it is not a matter to be taken lightly. Non-compliance can have drastic consequences, and it can lead to substantial penalties for defense contractors, their executives and board members, and their personnel. As cybersecurity risks continue to grow and evolve, DFARS compliance presents new challenges every
defense contractors need to have systems in place that they can efficiently supplement, update, and replace over time.

“DFARS compliance presents a variety of challenges for defense contractors. As contractors’ cybersecurity risks continue to evolve, they must be prepared to update their security protocols in order to maintain compliance on an ongoing basis.” – Dr. Nick Oberheiden, Founding Attorney of Oberheiden P.C.

With this in mind, here are 10 keys to DFARS compliance success in 2022:

1. **Understanding the Structure and Organization of DFARS**

The DFARS is a set of cybersecurity regulations that defense contractors must follow in order to be awarded a new DOD government contract. The DFARS regulations are extraordinarily long and complex; and, when viewing them in their aggregate, defense contractors’ compliance burden can seem overwhelming. But, by breaking down DFARS into its component parts, federal contractors can develop an effective compliance strategy, and they can build a comprehensive DFARS compliance program step-by-step.

The Defense Federal Acquisition Regulation Supplement identifies 14 areas, or “families” of compliance which are published in National Institute of Standards and Technology (NIST) Special Publication 800-171 (NIST SP 800-171). The 14 DFARS families or DFARS requirements are as follows:

- Access Controls
- Audits and Accountability
- Awareness and Training
- Configuration Management
- Identification and Authentication
- Incident Response
- Maintenance
- Media Protection
- Personnel Security
• Physical Protection
• Risk Assessment
• Security Assessment
• System and Communications Protection
• System and Information Integrity

Within each of these 14 families or DFARS compliance requirements, DFARS establishes “Basic Security Requirements” and “Derived Security Requirements”. As the National Institute of Standards and Technology (NIST) explains, “The derived security requirements, which supplement the basic security requirements, are taken from the security controls in NIST Special Publication 800-53.” NIST published a superseding version of Special Publication 800-53 in 2020, and defense contractors that developed their DFARS compliance programs before the update can use NIST’s Analysis of Updates Between 800-53 Rev. 5 and Rev. 4 to determine what modifications to their DFARS compliance programs are necessary.

2. Understanding the Purpose of DFARS

Understanding the purpose of DFARS can also assist defense contractors with compliance. The extensive cyber security requirements that apply to defense contractors under DFARS are largely intended to ensure that contractors’ cyber security protocols are up to par with those enlisted by the federal government. As NIST explains, the 14 DFARS families, “are closely aligned with the minimum security requirements for federal information and information systems described in FIPS Publication 200.” The Federal Information Processing Standards (FIPS) Publication 200 establishes the cybersecurity requirements for most federal offices and agencies.

3. Compliance Requires More Than an Understanding of DFARS

As our discussion thus far shows, developing an effective DFARS compliance program requires more than just an understanding of DFARS. Defense contractors must also comply with the FAR, and they must interpret DFARS following NIST Special Publication 800-53, FIPS
Publication 200, and the various other bodies of federal rules and regulations that DFARS incorporates by reference. So, while defense contractors can begin to grapple with compliance by breaking the process down into its component parts (i.e., the Basic Security Requirements and Derived Security Requirements within each of the 14 DFARS families), they must also expand their compliance efforts to address all pertinent external sources of authority as well.

4. A DFARS Compliance “Checklist” Isn’t Going to Cut It

Our discussion thus far should also make clear that simply adhering to an off-the-shelf DFARS compliance “checklist” isn’t enough for defense contractors to establish and maintain compliance in 2022 and beyond. Unfortunately, many companies pay heavily to promote these checklists online. In many cases, these checklists are nothing more than recitations of the Basic Security Requirements and Derived Security Requirements in the 14 DFARS families—which are already freely available online from NIST.

While a checklist can be useful for making sure a DFARS compliance program has not overlooked any major issues, a checklist is not an adequate tool for building a custom-tailored DFARS compliance program—which is what the DOD expects and what is required under federal law. Instead, defense contractors must work with their counsel and consultants to assess their specific cybersecurity risks, how DFARS applies to their specific operations and defense assets or services, and what is necessary to be able to demonstrate compliance to the DOD when necessary.

5. Conducting an Internal Cybersecurity and DFARS Risk Assessment

To assess their risks and obligations, defense contractors should begin with an internal audit. While there is no need to reinvent the wheel, defense contractors need to make sure they have a clear understanding of what is necessary not only to establish and maintain DFARS compliance but to prove DFARS compliance as well. As conducting this assessment requires an in-depth understanding of what it takes to maintain a DFARS-compliant cybersecurity program,
defense contractors will generally need to begin working with outside DFARS compliance counsel and consultants at this stage of the process.

As you can see from the list of the 14 DFARS compliance families above, compliance involves much more than implementing industry-standard digital security measures and protocols. Generally speaking, companies that are new to working with the DOD will not have the requisite controls in place, and defense contractors that have not recently revisited their DFARS compliance programs may well need to make updates or improvements in 2022.

6. Assembling a DFARS Compliance Team

Given the complexities of DFARS compliance and the fact that defense contractors must ably manage DFARS compliance on an ongoing basis, defense contractors must assemble a DFARS compliance team. This team should include internal personnel with appropriate reporting roles who have received adequate training in DFARS compliance, as well as outside lawyers and consultants who are available to assist with compliance as needed. Involving all internal and external members of the compliance team in the program development phase will help ensure not only that the contractor’s DFARS compliance program is adequately custom-tailored and comprehensive, but that all members of the team have an in-depth understanding of the program and how it interacts with and impacts the contractor’s operations as well.

7. Appointing a Compliance Officer

In addition to assembling a DFARS compliance team, defense contractors should also appoint a compliance officer who holds primary responsibility for daily management and oversight of their DFARS compliance program. Depending on a contractor’s size and the volume of business it does with the DOD, this may be a stand-alone position, or it may be an additional role assigned to the company’s Chief Compliance Officer or Chief Information Officer. In any case, the individual tasked with ensuring continuing DFARS compliance should have a thorough understanding of the contractor’s compliance program and its compliance
obligations, and he or she should have ongoing access to the company’s DFARS compliance counsel and consulting firm.

8. Building and Implementing a Custom-Tailored DFARS Compliance Program

Now we get to the step of the building and implementing a DFARS compliance program. It is important that defense contractors do not rush this process, as moving forward without an adequate understanding of what is necessary or without a high-performing team can lead to significant wasted effort and resources. With the groundwork laid, contractors can methodically address their compliance obligations under DFARS and all other pertinent rules and regulations.

After building their compliance programs step-by-step, contractors can then move on to implementation. This alone will typically be a multi-step process, with requirements ranging from implementing new physical and logical security protocols to providing appropriate training to employees at various levels within the organization.

9. Ongoing Auditing, Monitoring, and Enforcement of DFARS Compliance

Ongoing auditing, monitoring, and enforcement are all essential components of effective DFARS compliance and risk management. Defense contractors need to be able to demonstrate to the DOD that their operations are DFARS-compliant, and they need to be able to identify and address any intrusions or compliance failures immediately. DFARS compliance programs should include sections devoted to each of these areas, and compliance officers should ensure proper execution and documentation on an ongoing basis.

10. Being Prepared for Your Company’s DFARS Compliance Obligations to Change

Finally, as we mentioned in the introduction, the evolving nature of defense contractors’ cybersecurity risks means that contractors’ DFARS compliance obligations will change over
time. What worked in 2021 might not work in 2022, and what is adequate today might not be adequate tomorrow. As a result, defense contractors should not review their DFARS compliance programs as static entities, but rather as living documents that need to be reviewed, supplemented, and updated over time. With this approach to DFARS compliance, defense contractors can manage their risk effectively, and they can be prepared to demonstrate compliance when called upon to do so.

Oberheiden P.C. © 2022