We Are Passionate About Helping Secure Your Sensitive Data & Infrastructure.

Title 48: Federal Acquisition Regulations System
PART 252—SOLICITATION PROVISIONS AND CONTRACT CLAUSES
Subpart 252.2—Text of Provisions And Clauses

252.204-7012 Safeguarding covered defense information and cyber incident reporting.

As prescribed in 204.7304c, use the following clause:

SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING (OCT 2016)

(a) *Definitions.* As used in this clause—

Adequate security means protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information.

Compromise means disclosure of information to unauthorized persons, or a violation of the security policy of a system, in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object, or the copying of information to unauthorized media may have occurred.

Contractor attributional/proprietary information means information that identifies the contractor(s), whether directly or indirectly, by the grouping of information that can be traced back to the contractor(s) (*e.g.*, program description, facility locations), personally identifiable information, as well as trade secrets, commercial or financial information, or other commercially sensitive information that is not customarily shared outside of the company.

Controlled technical information means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Controlled technical information would meet the criteria, if disseminated, for distribution statements B through F using the criteria set forth in DoD Instruction 5230.24, Distribution Statements on Technical Documents. The term does not include information that is lawfully publicly available without restrictions.

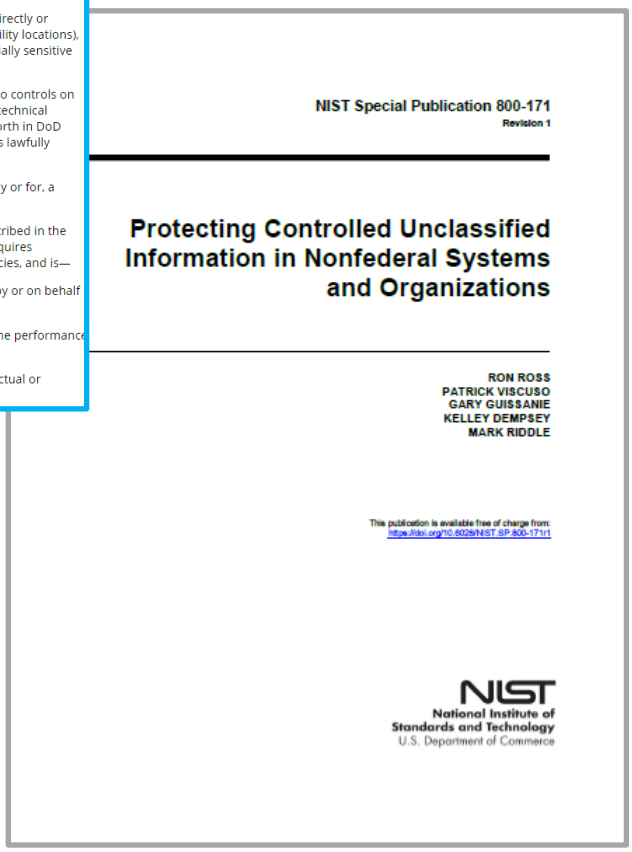
Covered contractor information system means an unclassified information system that is owned, or operated by or for, a contractor and that processes, stores, or transmits covered defense information.

Covered defense information means unclassified controlled technical information or other information, as described in the Controlled Unclassified Information (CUI) Registry at *http://www.archives.gov/cui/registry/category-list.html*, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Governmentwide policies, and is—

(1) Marked or otherwise identified in the contract, task order, or delivery order and provided to the contractor by or on behalf of DoD in support of the performance of the contract; or

(2) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract.

Cyber incident means actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein.



NIST Special Publication 800-171
Revision 1

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

RON ROSS
PATRICK VISCUSO
GARY GUISSANIE
KELLEY DEMPSEY
MARK RIDDLE

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-171r1

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

An Alternative Perspective Towards DFARS Cybersecurity Compliance & Its Relevance to the Greater Business Community

Bo Birdwell
03.28.2018

CONTENTS

The Defense Contractor Requirement

Many companies are becoming aware of the fact they are indirectly working for the Department of Defense. Whether you are a manufacturer, a software developer, or a university, you are now becoming inundated with terms, which six months ago, were only on the periphery of your awareness. Terms such as: DFARS[1], NIST[2], 800-171[3], cyber incident[4], and covered defense information[5].

Whether your latest Department of Defense contracts include cybersecurity verbiage[6] or you received a letter stating you needed to comply with the DFARS cybersecurity requirements, you find yourself in a position of having to implement the 110 requirements contained in SP 800-171[7]. You suddenly need to understand these concepts and how they apply to your business. *Where do you begin?*

Option One is to do it yourself. You Google several "DFARS cybersecurity" topics and hit upon some *Do It Yourself* websites.[8] Many hours later, you now understand how the DFARS directs each contractor or subcontractor to:

- *Provide Adequate Security as defined within the NIST SP 800-171.*
- *Report Cyber Incidents to the Department of Defense within 72 hours.*
- *Notify Subcontractors and Suppliers of these requirements.*

You have internalized a significant amount of NIST guidance and have a newfound understanding of the magnitude of the issue before you. Armed with this information, you now realize failing to meet these requirements will likely lead to contract cancellations. You have gained an appreciation for the simple, yet profound statement: it takes approximately twelve months to gain one year of experience…and you don't have twelve months. You decide: *you need help*.

Option Two is to seek out help. Who you ask for help will often determine the type of answer you receive. For example, if you ask a software vendor, the answer will often center around their software solution. If instead, you reach out to some cybersecurity consultants, the answer begins with a network penetration test and the solution will center around addressing the vulnerabilities they identify. Alternatively, other cybersecurity consultants will treat your DFARS requirement as completely unique from anyone else's and basically re-invent the wheel at an hourly rate during your engagement. *But if you ask Cyber Forward, the answer begins with Policy and Plans grounded in the NIST and that is a different response than our competitors will give you*.[9]

Why not choose the software solution? Software solutions are part of the answer, but technology alone can never be the solution. Cybersecurity is much more about people and process, than it is about technology. Technology enables processes to operate smoothly and frees people's time, but it is not a panacea. Analogously, consider your business a house. A great firewall makes an awesome door…but the door is only one piece of total structure protecting your family and valuables. A properly configured server is the ultimate filing cabinet, but it is still only one part of your house. *We provide you the schematics for a secure house, train your people to read, and help you build the house.*

Why not choose other consultants? Likewise, many consultants simply charge by the hour. However, we are not traditional consultants. We can charge by the product because

the government has defined the products required and we can bill at a low, flat rate. *You would be surprised how inexpensive DFARS compliance can be for your organization.*

Why Begin with Policy?

"*Most requirements in NIST SP 800-171 are about policy, process, and configuring IT securely…"—Defense Procurement and Acquisition Policy Q&A, Answer to Q17.*[10]

Because the alternative is to address everything as ad-hoc…and that doesn't work. A careful reading of the SP 800-171 would show that policy documents, Incident Response or Configuration Management Plans and Training Records are not required for compliance. Many readers of the 171 would know this because it says so in Appendix E, *Tailoring Criteria*. With DFARS compliance being their primary goal, these individuals justifiably focused on the CUI[11] controls because Appendix E uses three criteria to tailor out otherwise required Moderate Baseline control measures. However, Cyber Forward reached out to the authors of the NIST SP 800-171[12] and determined what the Nonfederal Organization, or "NFO", controls defined as "EXPECTED TO BE ROUTINELY SATISFIED BY NONFEDERAL ORGANIZATIONS WITHOUT SPECIFICATION" meant. NFO controls were tailored out to ensure entities did not create duplicate CUI policy documents, plans, training records, etc. *These controls were tailored out, but it wasn't because they weren't necessary...policy and plans documents are fundamental to building an effective cybersecurity program.*

We walk in the door with a template for success. Cyber Forward delivers tailored policy documents addressing all 14 control families identified in the NIST SP 800-171, as well as an Incident Response Plan and works with your team to finalize a Configuration Management Plan. We do this because these documents form the foundation upon which to address the DFARS requirements. *This straight forward methodology saves you time and saves you money.*

What is the Cyber Forward Process?

Our process begins in policy, evolves into tested plans, is reflected through proper configuration management & monitoring, and concludes in assessment.

We start by getting you compliant. We sit down with your team and discuss the policy documents and plans we have prepared. We explain how the items in our policy documents connect to the 800-171 requirement or the more specific 800-53[13] control measure. We then conduct a gap analysis to determine what items are currently addressed, and which are not. *Often in less than two weeks, we can create a site-specific system security plan and plan of actions & milestones…and these two documents must be completed to conduct business with the Department of Defense or to sign the DFARS letter*.

We take the time to help you become secure. Over the course of months, we can help your organization implement the items identified in the plan of action & milestones. When the time is right, usually 30-60 days after completing the last item in the plan of action & milestones, we can assist your organization in conducting the security assessment. *A security assessment is key because it documents the items discussed in the system security plan were implemented and how that was accomplished.*

Cybersecurity is bigger than the Defense Contractor Community

The threat is not hypothetical. The sheer number of events within public awareness today regarding cyber-attacks makes what should be frightening appear routine. Recent examples include Russian attacks against our critical infrastructure[14], Chinese theft of our intellectual property[15], Iranian state-sponsored hacking into our universities[16], as well as North Korea & Wannacry[17]. Each one in and of itself, is indicative of a significant threat to our nation, in both the public and private sector. The White House released a report in February 2018, estimating malicious cyber activity cost the U.S. economy between $57 billion and $109 billion in 2016.[18] *Corporate entities can no longer consider cybersecurity as simply another non-revenue generating expenditure, it must become part of core business operations.*

Our processes translate beyond DFARS Compliance: We apply the same proven pragmatism found in our Department of Defense work to our non-Department of Defense clients, including those who are involved in Critical Infrastructure. Because of the important part that critical infrastructure plays in the functioning of our current way of life, it has become a primary target of those who wish to both disrupt and sew discord. We believe a proper defense from such threats begins with a clear understanding of potential targets and a systems security plan that informs their protection.

Sector Specific Certifications. Whether it is FERC, HIPAA, FINRA, GDPR or PCI, Cyber Forward can aid your organization comply with applicable regulatory guidance and help you secure your sensitive data and infrastructure. These additional requirements are imbedded into the new policy set as required. Policies for critical infrastructure partners are often more complex and the plan of action & milestones requires greater oversite.

A globally applicable cybersecurity methodology. We preach a unifying truth regarding cyber security: *implementing nationally-recognized Best Practices[19] works*.

Data classification is essential. Frederick the Great was correct when he famously said, “He who defends everything defends nothing.” Most organizations can recognize their proverbial “crown jewels”; however, rarely are these digital items securely segregated from non-critical, (and necessarily, more accessible) less sensitive data.

User education is critical. No matter which source you listen to, you will find that social engineering [20] plays a prevalent role in cyber-attacks. Although most organizations reinforce the concept of not clicking on links or opening attachments in emails, few organizations emphasize properly marking documents, reporting potential cyber incidents, or the dangers of storing sensitive data on their local (or personal) machines.

Deliberate configuration management and routine patching prevent a preponderance of attacks. Every network relies on switches and routers to operate. Ensuring these devices remain patched often falls to the bottom of the priority list because if they operate, no one complains. Unfortunately, new vulnerabilities are identified weekly, and patches pushed monthly. An organization which fails to patch its infrastructure risks grave consequences. In the author’s

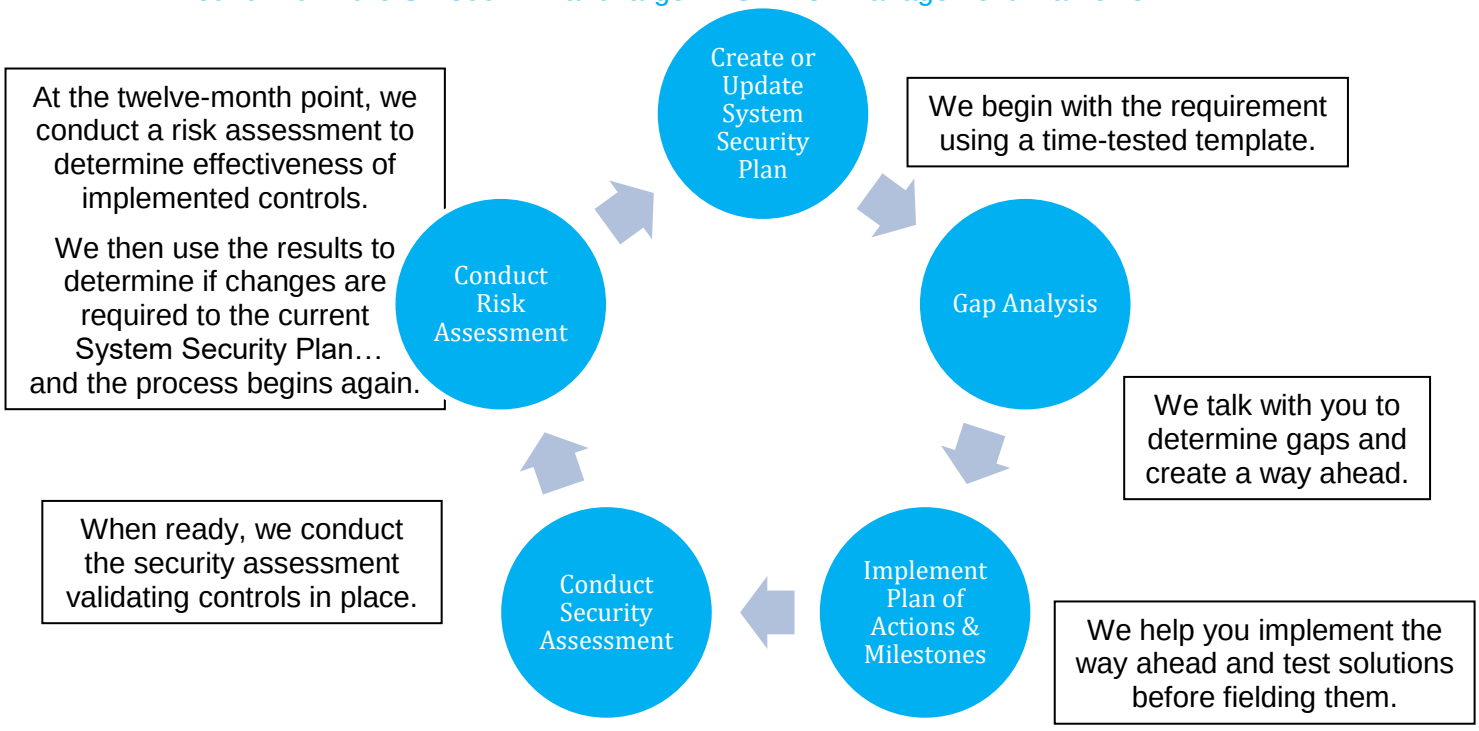
opinion, if an attacker controls your infrastructure, they control your network…and can wreak havoc within your organization or indiscriminately pilfer sensitive data.

Implementation requires focus. The concepts above will resonate with many organizations. Some may have tried implementing data classification, user education, and/or deliberate configuration management & routine patching previously. Unfortunately, many find these actions cannot be accomplished as hobbies, nor are they something easily pushed solely into the realm of the IT department (excluding portions of configuration management and patching). Cyber Forward has decades of experience implementing complex plans of actions for organizations of various sizes. Experience matters, and we can aid our partners overcome some of the more vexing challenges because we have seen them before.

Visual Depictions of Our Process

KEY FINDING 1: We focus on developing the foundation of the house (policies/processes/education) before buying new doors and bigger locks for the windows (infrastructure solutions) or asking a thief to try to break in (penetration testing).

KEY FINDING 2: We follow a deliberate process, which addresses all requirements found within the SP 800-171 and larger NIST Risk Management Framework.



Who is Cyber Forward?

CORE VALUES

Servant Leadership

Cyber Forward employees lead for the benefit of those led, not for self-promotion. Our clients can rely upon Cyber Forward employees to do the right thing regardless of circumstance and to embody the Biblical concepts of the Golden Rule and Love your neighbor as yourself in all interactions.

Passion

Our passion is to elevate corporate America's cyber defenses to military grade. Our clients can expect Cyber Forward employees to go the extra mile to address their concerns and our dedication to this cause will be readily apparent. We stand behind our products and services.

Process Oriented

We actively listen to our client's unique circumstances and leverage the most robust risk management framework in the world to protect their sensitive data. We do this by leveraging nationally-recognized best practices to equip our clients to secure sensitive data and operations.

Client Security

We began Cyber Forward because we are tired of our nation's adversaries gaining access to America's most sensitive technologies through footholds in small businesses. This passion translates into a mission imperative to secure your sensitive data. We will not rest until our clients can identify their sensitive data, manage the risk associate with and continually monitor its access.

Truth

Truth is immutable. Cyber Forward accepts truth as a strength which bolsters our ability to secure information critical to the protection of our nation's freedom. As such, we will be open, honest and transparent about your security needs. We will discuss your true needs, identify weaknesses and discuss opportunities for improvement

What We Do: Cyber Forward is helping secure America's military supply chain one link at a time. We aid corporate America stop the leakage of sensitive data into our adversary's hands and help lock down sensitive data and infrastructure so that you will not become another statistic highlighting the cyber onslaught facing our nation.

How We Do It: Cyber Forward takes a technology-agnostic approach to apply the Defense Federal Acquisition Regulation Supplement cyber security requirements (e.g. 48 CFR 252.204-7012). We deliver 14 concise policy documents addressing the 110 specified requirements within the National Institute of Science and Technology (NIST) Special Publication (SP) 800-171. We guarantee that all clients will receive a system security and plan of action & milestones consistent with the requirements outlined in 48 CFR 252.204-7012 and NIST SP 800 SP-171.

Why We Do It: We protect America's warfighters by stopping adversaries from using our own information and innovations against us.

Three Differentiators

1. Led and formed by veterans with Service Disabled ownership.

2. Technology agnostic product emphasizing policy & process, user education, and sound configuration management.

3. Leadership team with unrivaled expertise in cyber warfare, information security, and defending the largest networks on Earth.

THANK YOU.

FOR MORE INFORMATION CONTACT BO BIRDWELL
Bo@cyber4ward.com
https://www.linkedin.com/in/bobirdwell/
https://www.cyber4ward.com

Endnotes

[1] DFARS stands for Defense Federal Acquisition Regulation Supplement.
[2] NIST stands for National Institute of Science and Technology.
[3] NIST SP 800-171 refers to the NIST Special Publication (SP) 800-171r1, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations* (Dec '16, incorporating updates as of 2-20-2018).
[4] Cyber incident refers to Cyber incident means actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein.
[5] Covered defense information means unclassified controlled technical information or other information, as described in the Controlled Unclassified Information (CUI) Registry that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Governmentwide policies, and is—
(1) Marked or otherwise identified in the contract, task order, or delivery order and provided to the contractor by or on behalf of DoD in support of the performance of the contract; or
(2) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract.
[6] Either a reference to 48 CFR 252.204-7012, *Safeguarding covered defense information and cyber incident reporting* (Oct '16) or 48 CFR 252.204-7008, *Compliance with safeguarding covered defense information controls* (Oct '16).
[7] NIST SP 800-171 refers to the NIST Special Publication (SP) 800-171r1, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations* (Dec '16, incorporating updates as of 2-20-2018).
[8] Two such websites include: http://gtpac.org/cybersecurity-training-video/ and https://nvlpubs.nist.gov/nistpubs/hb/2017/NIST.HB.162.pdf
[9] Cyber Forward policies address the requirements conveyed in the SP 800-171, control measures explained in the SP 800-53 and Best Practices drawn from ~ 30 NIST publications referenced in the SP 800-171A (DRAFT).
[10] Network Penetration Reporting and Contracting for Cloud Services (DFARS Case 2013-D018), Frequently Asked Questions (FAQs) regarding the implementation of DFARS Subpart 204.73 and PGI Subpart 204.73, January 27, 2017 (https://www.acq.osd.mil/dpap/pdi/docs/FAQs_Network_Penetration_Reporting_and_Contracting_for_Cloud_Services_(01-27-2017).pdf).
[11] CUI stands for Controlled Unclassified Information.
[12] The author reached out to Mr. Kelley Dempsey and Mr. Gus Guissanie in late June and early July of 2017. We exchanged emails and discussed the NFO topic over the phone.
[13] NIST SP 800-53 refers to the NIST SP 800-53r4, *Security and Privacy Controls for Federal Information Systems and Organizations* (April 2013, includes updates as of 1-22-2015).
[14] https://www.us-cert.gov/ncas/alerts/TA18-074A
[15] https://ustr.gov/sites/default/files/Section%20301%20FINAL.PDF
[16] https://home.treasury.gov/news/press-releases/sm0332
[17] https://www.whitehouse.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/
[18] https://www.whitehouse.gov/wp-content/uploads/2018/02/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf, p. 1.
[19] The term Best Practices can be loosely interpreted. Cyber Forward utilizes NIST cybersecurity publications, Center for Internet Security (CIS) Benchmarks, and Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGS).
[20] A useful definition of social engineering is "tricking people into divulging personal information or other confidential data." Definition from The Tech Terms Dictionary, https://techterms.com/definition/social_engineering