Analyzing the Incident Response and Reporting Requirements of DFARS 252.204-7012

By

Jeremy B. Blevins

A Cyber Policy Paper

Submitted to the Faculty of

Utica College

May 2017

In Partial Fulfillment of the Requirements for the Degree of
Master of Professional Studies (MPS) in Cyber Policy and Risk Analysis

Analyzing the Incident Response and Reporting Requirements of DFARS 252.204-7012

Abstract

The purpose of this paper is to evaluate the incident response and cyber reporting requirements of DFARS clause 252.204-7012 and provide a viable solution for satisfying those requirements. 252.204-7012 was originally published in the fall of 2013 with the title *Safeguarding of unclassified controlled technical information* (Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, 2013), but since that time it has undergone several revisions. Its current iteration is titled *Safeguarding Covered Defense Information and Cyber Incident Reporting*. Irrespective of these changes, the purpose of 252.204-7012 remains the same: the protection of sensitive, albeit unclassified information that is in the possession of defense contractors. This research will explore the requirements of DFARS 252.204-7012 section (c) “Cyber incident reporting requirement” and section (g) “Cyber incident damage assessment activities” (Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, 2016). The basic security requirements in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations* section 3.6 "Incident Response" will be analyzed to establish an operational incident-handling capability. (National Institute of Standards and Technology, 2016). This research will provide contractors with information needed to create a process to satisfy both the control and reporting requirements of DFARS 252.204-7012.

Table of Contents

Statement of Problem ... 1

Literature Review ... 3

DFARS 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting ... 3

NIST SP 800-171 Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations ... 8

Frequently Asked Questions (FAQs) Regarding the Implementation of DFARS Subpart 204.73 and PGI Subpart 204.73, DFARS Subpart 239.76 and PGI Subpart 239.76 ... 10

The CIS Critical Security Controls for Effective Cyber Defense (Version 6.1) .. 11

Presidential Policy Directive (PPD)/PPD-41 ... 13

Summary of Literature Review ... 14

Discussion of the Findings ... 14

Major Findings ... 15

Limitations of the Paper ... 24

Recommendations ... 25

Understand What is Required ... 25

Pick a Framework ... 25

Involve the Appropriate Departments ... 26

Document, Document, Document ... 26

Understand the Costs. 26

Do Not Do Nothing.. 27

Conclusions... 27

References... 29

Appendix A 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting 33

Appendix B Selected NIST SP 800-53 Controls 38

IR-2 Incident Response Training 38

IR-4 Incident Handling 38

List of Tables

Table 1 4

Table 2 8

Table 3 17

List of Figures

Figure 1 CSC 1 System Entity Relationship Diagram....................................... 12

Statement of Problem

In order to do business with the United States federal government, private industries must abide by the Federal Acquisition Regulation (FAR), which “is established for the codification and publication of uniform policies and procedures for acquisition by all executive agencies”. The FAR consists of fifty-three parts (U. S. General Services Administration, 2014, pp. 1.1-1). Additionally, entities that desire to do business with the Department of Defense must also comply with the Defense Federal Acquisition Regulation Supplement (DFARS), which itself consists of sixty-nine parts further subdivided into two hundred and ninety-nine subparts (Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, 2009). It is through this sea of regulation that the enterprising defense contractor must navigate.

While there is a myriad of research opportunities to explore in the expanse of the FAR and DFARS, this paper is focused on DFARS 252.204-7012 *Safeguarding Covered Defense Information and Cyber Incident Reporting* (hereafter “252.204-7012”); specifically, incident response and reporting requirements. As alluded to in its title, 252.204-7012 is aimed at protecting sensitive government information that has been entrusted to private companies, and the reporting requirements if something adverse happens to that information. In other words, reporting the occurrence of adverse cyber event is just as essential as protecting the data in the first place.

This problem is not constrained to those held contractually to the FAR and DFARS, as evinced in Presidential Policy Directive (PPD-41). PPD-41 acknowledges “Cyber incidents are a fact of contemporary life, and significant cyber incidents are occurring with increasing frequency, impacting public and private infrastructure located in the United States and abroad" (The White House Office of the Press Secretary, 2016). It is in light of this reality that 252.204-7012 becomes such a critical regulation.

From the initial draft of 252.204-7012 and release for public comment, the clause has been fraught with ambiguity, as evinced in the public comments dating back to November 2013. The Federal Register recorded industry concerns, with comments addressing conflicts with other federal regulations and poorly defined requirements (Government Publishing Office, 2013, pp. 69273-69282).

As 252.204-7012 has matured over the past several years, a major change from the original version of this clause was the removal of a set of controls defined in a table enumerating the "Minimal Security Controls for Safeguarding", based on NIST SP 800-53 *Security and Privacy Controls for Federal Information Systems and Organizations*, (Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, 2013) and the replacement of the table's enumerated controls with a completely new, stand-alone document: NIST SP 800-171 *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*, hereafter referred to as "SP 800-171" (Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, 2016). When 252.204-7012 was originally written, SP 800-171 did not exist, necessitating the table of controls from SP 800-53. The table of controls was essential because contractors had no guidance of which controls from SP 800-53 to implement otherwise.

Additionally, two areas of 252.204-7012 represent a particular challenge for contractors: *(c) Cyber Incident Reporting Requirement* and *(g) Cyber Incident Damage Assessment Activities*. While SP 800-171 provides the general control requirements that must be met, it does not provide clear guidance on how to manage incident response, and does not address at all the reporting requirements of *(g)*. The question this research will answer is this: how does an organization implement a DFARS-compliant incident response capability that addresses Cyber incident damage assessment activities to satisfy 252.204-7012 requirements? In other words, what are the minimum criterion required to implement and maintain a compliant cyber incident response and reporting capability?

This paper will review DFARS 252.204-7012, NIST SP 800-171, and other relevant literature to determine what constitutes DFARS-compliant incident response capability that addresses Cyber incident damage assessment activities and provide a working model of such a response capability.

Literature Review

DFARS 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting

252.204-7012 was originally released in November 2013 under the title *Safeguarding of unclassified controlled technical information*. One of the major differences in this early version of the clause and subsequent revisions is that the original revision specified a list of controls from NIST SP 800-53 *Assessing Security and Privacy Controls in Federal Information Systems and Organizations* (Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, 2013). This list of controls caused confusion among contractors, as can be seen in the public comments in Federal Register Volume 78, Number 222. Several respondents suggested that the variety of SP 800-53 controls lead to a wide interpretation because that Special Publication was written for federal systems and not contractor owned systems. Implementing these controls on contractor systems could be burdensome on personnel. Additionally, there were suggestions that this hurts competition as less sophisticated firms are unable to enter the contractor marketspace because of the cost of implementing the controls. Another respondent suggested NIST controls should not be specified, and should be selectable by the program office. A respondent suggested that a list of controls is not sufficient and context/guidance is needed (Government Publishing Office, 2013, p. 69274). Subsequent changes to 252.204-7012 sought to address these concerns by removing the table of SP 800-53 controls and replacing it with SP 800-171, which was written to address non-federal systems.

In the most recent version, last revised October 2016, the name of the 252.204-7012 was changed to *Safeguarding covered defense information and cyber incident reporting*. This title represented a clarification within the Federal government to scope the clause down from the ambiguous "unclassified controlled technical information" (UCTI) to "covered defense information" (CDI). In other words, with this change, it was much clearer what information a contractor must protect under 252.204-7012. The differences in the sections in this version of the clause and the original are shown in

Table 1.

Table 1

Comparison of Sections in Original and Current Versions of DFARS 252.204-7012

November 2013	October 2016
(a) Definitions	(a) Definitions
(b) Safeguarding requirements and procedures for unclassified controlled technical information.	(b) Adequate security
(c) Other requirements	

(d) Cyber incident and compromise reporting	(c) Cyber incident reporting requirement
	(d) Malicious software
(e) Protection of reported information	(e) Media preservation and protection
	(f) Access to additional information or equipment necessary for forensic analysis
	(g) Cyber incident damage assessment activities
	(h) DoD safeguarding and use of contractor attributional/proprietary information
	(i) Use and release of contractor attributional/proprietary information not created by or for DoD
	(j) Use and release of contractor attributional/proprietary information created by or for DoD
(f) Disclaimer	(k) Disclaimer
	(l) Other safeguarding or reporting requirements
(g) Subcontracts	(m) Subcontracts

The full text of 252.204-7012 is enumerated in Appendix A. The most relevant sections to the matter of incident response and reporting are detailed below.

Section (a) of the clause defines the essential terms. This is necessary because the terms can have different meanings in other contexts. Such a term is “Covered defense information”, which the clause limits in scope to only specific information the contractor possesses that that has certain marking and handling requirements that was either provided to the contractor by the government or developed by the contractor in support of a particular government contract. Another definition that would be ambiguous without a definition in the clause is “Rapidly report”, which in the context of the clause means 72 hours (Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, 2016).

Section (b) outlines the “Adequate Security” requirements of the clause. This stipulates a contractor’s minimum security requirements to be compliant. Any systems operated by the contractor that process covered defense information must implement subsections (1), (2), and (3), with the exception of cloud computing services, which are regulated by DFARS 252.239-7010, Cloud Computing Services. Of importance is (2)(i) which mandates the requirements specified in SP 800-171 must be implemented. Even more critical is (2)(ii)(A) which states that contractors must implement SP 800-171 “as soon as practical, but not later than December 31, 2017”. (2)(ii)(B) requires that contractors must submit in writing any variances to implementing SP 800-171 to the Contracting Officer. These requests will be adjudicated by the DoD Chief Information Officer (CIO). (2)(ii)(C) allows for contractors to send a copy of any previously adjudicated variances for new/ different contracts stipulating 252.204-7012. Finally, (2)(ii)(D) stipulates that any external cloud services the contractor implements that fall under purview of the 252.204-7012 must implement security requirements that are commensurate with the Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline, and the cloud service provider must comply with paragraphs (c) through (g) of 252.204-7012.

Section (c) outlines the cyber incident reporting requirements. This section is one of the most critical areas of 252.204-7012 because it stipulates what a contractor must do when a cyber incident involving covered defense information is discovered. These requirements include conducting a “review for evidence of compromise” of the system(s) involved, “rapidly reporting” the incident to a defined DoD portal, developing a cyber incident report, and obtaining a “DoD-approved medium assurance certificate”. This certificate is used to digitally sign and or encrypt all information that is provided to the DoD.

Sections (d), (e), (f), and (g) deal with the handling of malware related to an incident, preservation of system images, forensic analysis, and the potential for DoD to engage in a more formal damage assessment should it been deemed necessary.

Sections (h), (i), (j), (k), and (l) provide verbiage for contractual/ legal elements of 252.204-7012.

Finally, Section (m) deals with the requirement of this clause on subcontracts. contractors must flow down the requirements of this clause to all parties who they subcontract to perform activities related to the particular contract that originally included 252.204-7012. It requires a subcontractor to notify the prime contractor, or a subcontractor who let out a subcontract to it, if it cannot must vary from the control requirements in SP 800-171. It also requires the sub to likewise flow back up the reporting chain any cyber incidents that must be reported under this clause (Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, 2016).

In reviewing this regulation, it becomes apparent that despite its brevity, it has huge implications on contractors. This will become apparent upon the analysis of SP 800-171, which serves as the foundation for cyber controls required to be compliant with the clause.

NIST SP 800-171 Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations

SP 800-171 was released in June 2015 and last revised in January 2016. While the publication is based on FIPS Publication 200 and NIST SP 800-53, SP 800-171 makes it clear that while the requirements outlined within it are what has to be satisfied (National Institute of Standards and Technology, 2016, p. v). Whereas SP 800-53 is written to provide baseline controls for various types of information for federal systems, 800-171 applies to CUI for non-federal systems.

With that in mind, SP 800-171 is divided into three chapters and five appendices. Chapter One is an introduction to the publication. Chapter Two deals with the fundamentals of protecting CUI in non-federal systems. Chapter Three enumerates the actual controls to be implemented. Appendix A contains the document's references. Appendix B is the glossary. Appendix C is the list of acronyms. Appendix D maps the SP 800-171 requirements to SP 800-53 controls. Appendix E details the tailoring criteria.

The brunt of SP 800-171 lies in Chapter 3, titled "The Requirements". Within this chapter, fourteen families of requirements are established, as seen in Table 2.

Table 2

Enumeration of NIST SP 800-171 requirements.

Section	Family Name
3.1	Access Control
3.2	Awareness and Training
3.3	Audit and Accountability
3.4	Configuration Management
3.5	Identification and Authentication
3.6	Incident Response

3.7	Maintenance
3.8	Media Protection
3.9	Personnel Security
3.10	Physical Protection
3.11	Risk Assessment
3.12	Security Assessment
3.13	System and Communications Protection
3.14	System and Information Integrity

In each of these families are the actual requirements, for example, the first requirement under 3.6 Incident Response is 3.6.1: “Establish an operational incident-handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities.” (National Institute of Standards and Technology, 2016, p. 11). Contractors must determine, within their environments that are under the purview of DFARS 252.204-7012, how to satisfy this requirement. The dilemma is that this terse verbiage does not provide much guidance, unless one recalls Appendix D, which then maps this requirement to IR-2 and IR-4 in NIST SP 800-53, shown in Appendix B (National Institute of Standards and Technology, 2015, pp. F-103-F-106).

Bearing in mind that they are not required to satisfy all of what is stated in SP 800-53, contractors must nonetheless reference it to understand the requirement levied in SP 800-171, but they must be cognizant not to read in from SP 800-53 undue burden that would overly complicate, and exponentially increase the cost of, SP 800-171 compliance.

Frequently Asked Questions (FAQs) Regarding the Implementation of DFARS Subpart 204.73 and PGI Subpart 204.73, DFARS Subpart 239.76 and PGI Subpart 239.76

In early 2007, the Office of the Under Secretary of Defense for Acquisition, Technology and Logistics released and updated Frequently Asked Questions (FAQs) to address industry concerns over compliance with DFARS 252.204-7012. This FAQ consists of fifty-nine questions and their answers. The questions range from basics such as "What is the purpose of DFARS clause 252.204-7012?" to more technical inquiries such as "Why did the security protections required by DFARS clause 252.204-7012 change from a table of selected NIST SP 800-53 security controls to NIST Special Publication (SP) 800-171? How does NIST SP 800-171 compare to NIST SP 800-53?" These questions and answers provide a single repository for questions that contractors have been asking for the past several years.

This FAQ is important for contractors to read because it provides clarity on complying with 252.204-7012 and implementing SP 800-171. For example, Q11 asks "Who is responsible for identifying/marking CDI? How will CDI be identified?". This question is answered by stating that the Contracting Officer is responsible for either making sure covered defense information is properly marked or there is enough information in the contract, task order, or delivery order for the contractor to ascertain what information is covered defense information. As the contractor develops information that is covered defense information, they are responsible for marking what they have generated. Another question that provides insight is Q24: "Does the Government intend to monitor contractors to ensure implementation of the required security requirements?". The answer to the question is no, the government will not monitor contractor's compliance to 252.204-7012 or SP 800-171, but it begs the next question from the FAQ, Q25: “Will the DoD certify that a contractor is 100% compliant with NIST SP 800-171? Is a 3rd Party assessment of compliance required?”. The answer is that no “new oversight paradigm” was created. Interestingly the answer also states “It is up to the contractor to determine that their systems meet the requirements”. The problem with this statement is that it assumes integrity on the part of the contractor in reporting compliance to their Contracting Officer, and that they know how to satisfy the requirements in SP 800-171. The answer does go on to offer that contractors who lack cybersecurity experience “may choose to seek outside assistance” to satisfy the SP 800-171 requirements.

While the FAQ does provide some clarity, ultimately, some of the questions have non-committal responses that do not provide firm answers, still leaving the contractors to figure out what is required for themselves. (Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, 2017).

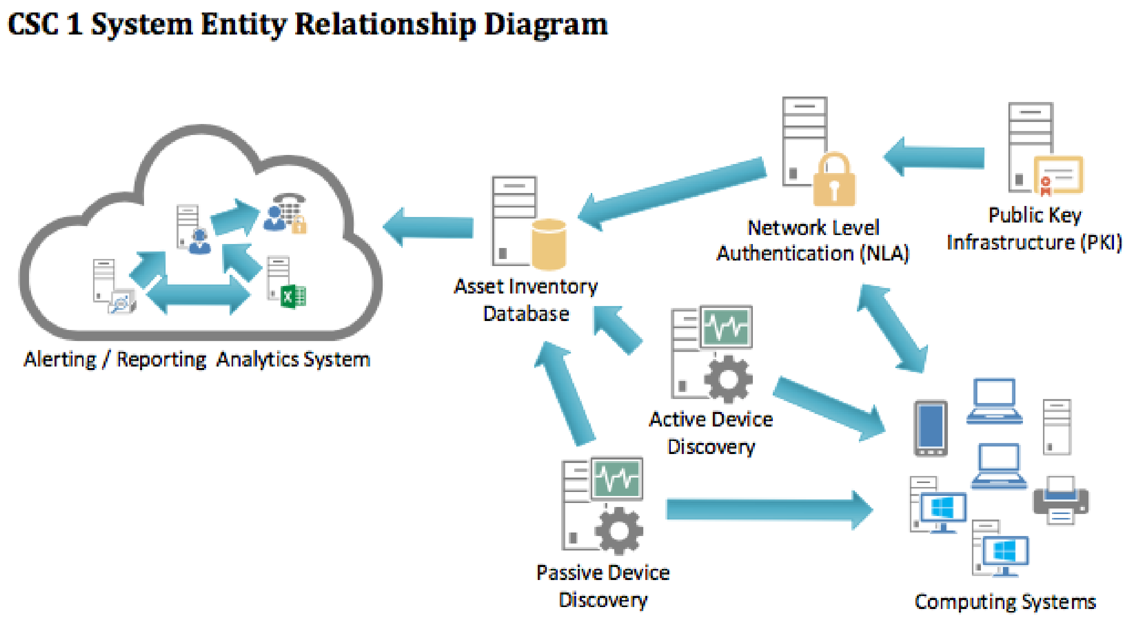
The CIS Critical Security Controls for Effective Cyber Defense (Version 6.1)

The current iteration of the Center for Internet Security consists of twenty Critical Security Control (CSC) families and seven appendices. Each of the CSCs deal with a particular security subject, such as CSC1: Inventory of Authorized and Unauthorized Devices. The document provides an explanation of why the control is critical. Each control is then further divided into sub-controls: CSC 1 has six, and contain descriptions of the actions needed for satisfaction, as in CSC1.1:

> Deploy an automated asset inventory discovery tool and use it to build a preliminary inventory of systems connected to an organization’s public and private network(s). Both active tools that scan through IPv4 or IPv6 network address ranges and passive tools that identify hosts based on analyzing their traffic should be employed. (Center for Internet Security, 2016, p. 6)

After the control descriptions, the document provides information on procedures and tools to satisfy the implementation of the control and a diagram showing the control's relationship, such as the one illustrated in Figure 1.

Figure 1 CSC 1 System Entity Relationship Diagram


CSC 1 System Entity Relationship Diagram
Alerting / Reporting Analytics System
Asset Inventory Database
Network Level Authentication (NLA)
Public Key Infrastructure (PKI)
Active Device Discovery
Passive Device Discovery
Computing Systems

(Center for Internet Security, 2016, p. 9)

The several appendices provide information on the "evolving attack model" (Appendix A), "attack types" Appendix B, the NIST Framework (Appendix C), "the National Cyber Hygiene Campaign" (Appendix D), mapping critical governance controls to the critical security controls (Appendix E), "Privacy Impact Assessment" (Appendix F), and categorization of the controls (Appendix G).

Of these, Appendix C has significant applicability with reference to the NIST 800-53 controls. While it does not map each of the CSC sub-controls to its relevant SP 800-53 counterpart, it does map the overall CSCs to relevant NIST control families. One dilemma, as evinced in CSC 4, is that the critical controls map to multiple NIST families, depending on what is being accomplished. Appendix C contains a table illustrating these mappings, with columns under the context of Cybersecurity Framework (CSF) Core labeled Identify, Protect, Detect, Respond, and Recover. CSC 4, Continuous Vulnerability Assessment and Remediation maps to NIST family RA for Identify, CM for Detect, and MI for respond (Center for Internet Security, 2016, pp. 78-79). One must conduct further analysis to determine which of the CSC sub-controls maps to which of the specific SP 800-171 requirements to make the most effective use of this document. That caveat aside, the CIS Critical Security controls provides more detail on how to actually implement security than is available in the NIST publications.

Presidential Policy Directive (PPD)/PPD-41

PPD-41 titled “United States Cyber Incident Coordination” addresses Federal government’s responsibilities in responding to any cyber incident, whether it involves the government or the private sector. In its scope, it “requires the Departments of Justice and Homeland Security to maintain updated contact information for public use to assist entities affected by cyber incidents in reporting those incidents to the proper authorities”.

PPD-41defines both “cyber incident” and “significant cyber incident”, the difference being a significant cyber event is “likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people”. It establishes guiding principles, consisting of: shared responsibility, risk-based response, respecting affected entities, unity of governmental effort, and enabling restoration and recovery. PPD-41 outlines the government’s concurrent lines of effort: threat response; asset response; and intelligence support and related activities.

Through PPD-41 the Departments of Homeland Security and Justice are tasked with providing the private sector with a means of contacting applicable government agencies regarding cyber events. As most critical infrastructure in the United States is owned and managed by the private sector, this conduit to contracting the government when a cyber event occurs is essential for national security (The White House Office of the Press Secretary, 2016).

Summary of Literature Review

If taken in a stand-alone context, 252.204-7012 leaves much to be desired for contractors looking for specific guidance in implementing a Cyber incident response and reporting capability. Adding to that the questions other contractors raised in the FAQ related to the clause and the levity expressed in PPD-4, and the task might appear daunting. The beacon of hope, however, is the guidance provided in the CIS Critical Security Controls. With it, contractors can begin to formulate a framework for developing a Cyber incident response and reporting capability.

Discussion of the Findings

Review of 252.204-7012 and NIST SP 800-171 makes clear that implementing an effective cyber incident response and reporting program requires additional guidance beyond the vague language found therein. More specificity is required to make the sections useful. One way to remedy this dilemma is to choose an additional framework to fill in some of the gaps. For the purpose of this research the CIS CSCs were selected. The CSCs provide specific guidance that is not overly burdensome can be implemented by contractors of all sizes. That guidance is not so specific, however, that it cannot be tailored to meet the unique needs of each contractors' environments.

Regarding incident response and reporting, the pertinent section of SP 800-171 is 3.6. Most of the requirements in 3.6 are addressed somewhere in the 20 critical security controls outlined in the CIS CSC, although, they are not always grouped together. Despite that, the CSCs provide the means to develop an effective incident response and reporting capability that satisfies the requirements of SP 800-171 Section 3.6.

Major Findings

SP 800-171 Section 3.6 has the following basic and derived security requirements:

> Basic Security Requirements:
>
> **3.6.1** Establish an operational incident-handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities.
>
> **3.6.2** Track, document, and report incidents to appropriate officials and/or authorities both internal and external to the organization.
>
> Derived Security Requirements:
>
> **3.6.3** Test the organizational incident response capability. (National Institute of Standards and Technology, 2016)

For so few words, much work must be done. The key word in 3.6.1 is that the incident-response capability must be “operational”: it cannot be just theoretical. When a cyber event occurs, the incident response capability needs to function properly. If the capability does not work, then the required reporting cannot occur. That puts the contractor potentially in breach of contract, will all the potential repercussions that might follow, from the issuance of a stop-work, or most drastic, the cancellation of the contract.

While not directly related to 252.204-7012, an example of the type of repercussions a contractor may face related to cyber events can be seen in the Office of Personnel Management (OPM) cancelling its contract with U.S. Investigations Services (USIS), who had been contracted to perform security investigations, in September 2014. Following this breach, OPM cancelled its contract with USIS (Davenport, 2014), and in February 2015, USIS's parent company, Altegrity Inc., filed for bankruptcy (Sandler & Tan, 2015). In addition to the cyber incident that ultimately caused USIS to lose its OPM contract, USIS has been accused of performing ineffective background checks that allowed now-notorious individuals such as Edward Snowden, the fugitive NSA leaker, and Aaron Alexis, the Navy Yard shooter, to obtain security clearances (Sandler & Tan, 2015). Even though the cyber-attack that ultimately cost USIS its contract was not cancelled directly because of 252.204-7012, it involved sensitive information similar to what 7012 seeks to protect.

The requirements of adequate preparation, detection, analysis, containment, recovery, and user response could take many forms and if not well planned, incur unnecessary cost and potential scope creep. CSC 4 provides direction. It is divided into eight (8) sub-controls, which do not directly align with SP 800-171 Section 3.6, but do, however, provide necessary guidance.

Adequate Preparation. Understanding of "adequate preparation" is critical. To ensure comprehension, the contractor should refer to Table D of SP 800-171 to determine which control from SP 800-53 that 3.6.1 aligns with, which is IR-2 (National Institute of Standards and Technology, 2016, pp. D-12). IR-2 requires federal entities to define how long after assuming the role that an incident responder must be trained to perform such IR duties. It also requires that responders be retrained when system changes require it, and that they must receive refresher training at pre-defined intervals (National Institute of Standards and Technology, 2015, pp. F-103). Additionally, within DoD, Incident Responders must maintain certifications required by the Information Assurance

Workforce Improvement Program, DoD 8570.01. These certifications are provided in Table 3.

Table 3

DoD 8570 Certification Requirements for CSSP Incident Responders

Acronym	Certification Name
CEH	Certified Ethical Hacker
GCFA	GIAC Certified Forensic Analyst
GCIH	GIAC Certified Incident Handler
SCYBER	Cisco Cybersecurity Specialist

(Defense Information Systems Agency, 2017)

While contractors are not required under either DFARS 252.204-7012 nor NIST SP 800-171 to have their incident response staff meet the certification requirements of DoD 8570, doing so ensures the responders are trained commensurate with their peers directly supporting federal systems. Additionally, having the certifications removes the ambiguity of whether or not the contractor has engaged in adequate preparation as required by SP 800-171 Section 3.6.1. An example of this might be an effort the contractor wants to bid on that stipulates DoD 8570 in the contract’s clauses. The difference between winning the contract or not might be that the contractor already has staff who possess the prerequisite certifications to perform the work.

Guidance for achieving adequate preparation can be found in CSC 17 *Security Skills Assessment and Appropriate Training to Fill Gaps*. This control deals not only with providing incident responders adequate training to do their jobs, but establishes sub-controls to address general users as well. The sub-controls provide basic guidance on implementing a security awareness program for all employees and skills assessments for critical response personnel (Center for Internet Security, 2016, pp. 59-60)

Coupling the formal certifications specified in DoD 8570 with the general security awareness training of CSC 17 covers the spectrum of knowledge needed to meet the adequate preparation requirement of SP 800-171 Section 3.6.1.

Detection. Detection of involves several tasks. The first is vulnerability scanning. CSC 4.1 advises the contractor to run perform automated vulnerability scanning against all systems on the network at least weekly. The output of this scan provides a list of vulnerabilities that can be checked against published vulnerability databases to develop understand what the risk to the environment is (Center for Internet Security, 2016, p. 17). These scans will provide the basis for adequate preparation required by SP 800-171 Section 3.6. CSC 4.3 is also related to vulnerability scans, and provides additional granularity to the scans by requiring either the utilization of locally installed agents on the systems being scanned or remote scans performed with administrative rights. Additionally, CSC 4.7 addresses the need for subsequent follow-on vulnerability scans after remediation actions were implemented to ensure the vulnerability has been mitigated. This cycle of scan-remediate-scan represents the basis of a continuous monitoring capability (Center for Internet Security, 2016, p. 18). The solution implemented by the DoD for vulnerability scanning is known internally as the Assured Compliance Assessment Solution (ACAS). ACAS consists of four components available commercially from Tenable Network Security: Security Center, Nessus User Interface, 3D Tool, and Passive Vulnerability Scanner. While some plugins may not be available outside of the DoD (Defense Information Systems Agency), opportunity exists for contractor to mimic the vulnerability scanning environment utilized within the DoD, thus providing a degree of assurance that the commercial solution would be adequate.

CSC 4.2 advises the contractor to compare the findings of the vulnerability scans against system logs. This provides the contractor an understanding of which vulnerabilities are being targeted, and which have been potentially exploited (Center for Internet Security, 2016, p. 17). This address SP 800-171's requirement to detect and analyze.

CSC 4.4 addresses the need for organizations to subscribe to vulnerability intelligence services (Center for Internet Security, 2016, p. 18). While some large contractors may have the resources to develop their own intelligence products in-house, the reality is that most organizations do not have this luxury. Another dilemma is: what does an organization do with the information from vulnerability intelligence services, (i.e. threat feeds)? Attempting to manually parse the threat feeds would be akin to "drinking from the firehose". In other words, properly addressing the vulnerability information from the threat feeds is more than a human analyst is capable of processing. It is essential then that a contractor utilizes a Security Information and Event Management (SIEM) solution that is able to ingest threat feeds and correlate them with vulnerability scans and event logs as addressed in CSC 4.2. This provides a big-picture view of what vulnerabilities exist in the environment, what activity has been seen in logs, and what emerging threats might the contractor anticipate next. In addition to SIEM, the term Unified Threat Management is used for systems capable of this correlation. Unlike ACAS, DoD does not have a unified approach to this problem space. Different SIEM/UTM solutions may be deployed, depending on the decision of the DoD element. While this doesn't give contractors an example to follow, it does allow them to seek out a solution that best fits their particular environments.

Analysis. Analysis requires the contractor to perform a “deep-dive” of their environment to determine as much information on an incident as possible. This sleuthing initially begins with know-impacted systems and the review of all information captured by the SIEM/UTM. When malware is discovered, 252.204-7012 requires that it be submitted to the DoD Cyber Crime Center (DC3). Guidance on how to perform this submission is provided by either DC3 or the Contracting Officer (Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, 2016). This submission does not preclude a contractor from performing its own analysis, but most small- and medium-sized contractors may not have the resources on staff to reverse engineer malware, or the financial capacity to outsource it. The analysis of the environment in concert with the results of any information provided back from DC3 will aid the contractor in determining how the incident occurred.

Containment. While analysis is being conducted, the contractor must ensure the incident does not spread to other systems. Contractors may be tempted to just pull all impacted systems offline and wipe them, but this might damage the evidence trail that the DoD may request should it pursue a formal damage assessment. Containment can be managed through the implementation of written incident response procedures. CSC 19.1 addresses this aspect and includes that the contractor should define personnel roles and have defined procedures for phases of incident handling (Center for Internet Security, 2016, p. 66)(Center for Internet Security, 2016). Additionally, it is advisable for contractors to implement a chain of custody form for all media involved in the incident. This will facilitate auditable tracking of who has handled the media and where it has been stored. While the notion of “chain of custody” is law enforcement concept, it is wholly applicable to cyber events, especially with the requirement in 252.204-7012 to maintain either original drives for images of those drives for further analysis should the government determine it necessary. A chain of custody form should address six elements:

- What is the evidence?
- How did the handler of the media get it?
- When was the media collected (e.g. when was the drive pulled from the system)?
- Who all has handled the media?
- Why did a particular person handle the media?
- Where has the media been transported to, and where was it stored while it was there? (Scalet, 2005)

More important from a cyber perspective, however, is keeping the cyber incident from spreading to other systems. This can be achieved by implementing reactive tools that are able to automatically shut off ports and services when malicious activity occurs. One such tool is an intrusion detection and prevention system (IDPS). An IDPS is a tool for “identifying possible incidents, logging information about them, attempting to stop them, and reporting them to security administrators”. The topic of IDPSes is even important enough to justify its own NIST Special Publication: 800-94 *Guide to Intrusion Detection and Prevention Systems (IDPS)*. NIST outlines four types of IDPS technologies: a) network-based, b) wireless, c) network behavior analysis (NBA), and d) host-based. The bulk of 800-94 addresses these types of IDPSes (National Institute of Standards and Technology, 2007).

Within the DoD, the DISA Endpoint Security System is utilized. This is better known by the legacy acronym “HBSS”, which stands for Host-Based Security System. HBSS consists of several McAfee components, which include desktop antivirus, host-based firewall, and ePO, the e-Policy Orchestrator, which provides the backend to manage the desktop components (McAfee, 2012). Because HBSS is based on commercial packages, a contractor can buy all the components needed to implement a HBSS-like solution that is able to monitor events and respond to them remotely, and possibly automatically, based on configuration, thus satisfying the containment requirement. Certainly, the same could be done with another vendor’s products, as there is no requirement to implement exactly the products currently deployed by the DoD.

Recovery. CSC 10 addresses data recovery and is broken into four sub-controls. CSC 10.1 outlines the requirement to perform regular backups of information, with frequent backups being required for sensitive information. This is essential to restore a known-good copy of information that might be compromised via malware infection. The control recommends that in addition to backing up data, the operating system and application software also should be backed up regularly. The purpose of this is to restore the whole system to its known-good state. CSC 10.2 addresses testing backups so that integrity is verified. CSC 10.3 addresses physical safeguards of the backup media. CSC 10.4 addresses properly handling encryption keys related to backups to prevent the inadvertent loss of the ability to decrypt the backup (Center for Internet Security, 2016, p. 36)(Center for Internet Security, 2016)

In addition to CSC 10, contractors also have the resource of NIST SP 800-184, *Guide for Cybersecurity Event Recovery*. This guide goes well beyond the simple recovery of data to the restoration of activities following a cyber event. It includes information on enterprise resiliency, recovery planning, and continuous improvement (National Institute of Standards and Technology, 2016). By implementing both CSC 10 and 800-184, a contractor can establish a robust recovery capability.

User response activities. User response activities is a very vague term until one cross-references it with the table in Appendix D of SP 800-171 to see that it refers to incident handling, which is addressed in IR-4 of SP 800-53. Using it as guidance, one is able to ascertain that response activities are those that involve monitoring the environment and performing the actions discussed above (National Institute of Standards and Technology, 2015, pp. F-105)(National Institute of Standards and Technology, 2015). Performing these activities can be more clearly understood by implementing several of the CSC controls not previously discussed, such as CSC 6 *Maintenance, Monitoring, and Analysis of Audit Logs*, CSC 8 *Malware Defenses*, and CSC 13 *Data Protection* (Center for Internet Security, 2016).

Track, document and report incidents. CSC 19 addresses Incident Response and Management. This control consists of seven sub-controls that deal with having written incident response procedures, assigned duties, time standards for reporting events, points-of-contact for 3rd party vendors who are under contract to provide response services, the publication of incident response reporting information, and the execution of response tests, which will be addressed in more detail below (Center for Internet Security, 2016, pp. 66-67). Additionally, contractors must report incidents to the government per 252.204-7012. By having a robust incident response capability and defined reporting processes, the information provided to the government will be much more likely to contain enough information to ascertain the depth and threat of a particular cyber event.

Test incident response capability. All the effort put into planning and developing incident response capabilities would be fruitless if the capability is not tested. To alleviate this, contractors can look to CSC 20 *Penetration Tests and Red Team Exercises* for guidance. The CSC's eight sub-controls walk the contractor through planning a testing capability that allows them to satisfy this SP 800-171 requirement (Center for Internet Security, 2016, pp. 70-71). Given that many small- to medium-sized contractors will not likely have the resources to staff a team of ethical hackers, CSC 20 provides them the framework to understand what to expect of outside vendors performing this function.

Limitations of the Paper

This paper was limited in scope to the cyber incident response and reporting requirements of DFARS 252.204-7012. This implied several constraints. The first constraint was the target audience, which was primarily U.S. defense contractors. They are the only entities bound to 252.204-7012, because to be a defense contractor means the organization has a defense contract.

The second constraint was that incident response and reporting requirements are only applicable to systems that process covered defense information, or the information itself. If the contractor is able to segregate other systems from covered defense information, then those systems are out of scope for 252.204-7012. The organization may or may not use the same incident response procedures for non-covered defense information data at their discretion. Likewise, they are not accountable to report incidents involving non-covered defense information in the same manner as they are for covered defense information.

The third constraint was the limited academic research available on this topic. There are several commercial companies who provide services for meeting 252.204-7012 compliance, but their methods are proprietary information. Likewise, the policies, processes, and procedures that individual companies have developed for compliance are proprietary information.

Recommendations

Understand What is Required

The greatest recommendation is to understand what is required. A lack of understanding can cause a contractor to either under-implement, which runs the risk of causing the suspension or revocation of a contract, or possibly as bad, to over-implement, and incur unnecessary cost that causes the incident response and reporting capability to be a poor return on investment. Either of these can cause distrust amongst leadership in the capabilities of the cyber incident response team and especially that team's leader(s).

Pick a Framework

Some aspects of complying with the cyber incident response and reporting requirements of DFAS 252.204-7012 are subjective and implementation is at the discretion of each contractor of the uniqueness of each system that processes covered defense information. That being said, it is imperative that contractors select some methodology and follow it. NIST SP 800-171 tells a contractor what must be done, but not how to do it. This paper has recommended the CSC Critical Security Controls as the supplemental guidance needed to satisfy compliance with the cyber incident response and reporting requirements. Where those controls have not specifically addressed an SP 800-171 requirement, specific other NIST documents have been recommended. All of this requires orderly processes to be created and followed.

Involve the Appropriate Departments

Additionally, as with any contract clause, both the legal and contracting departments should be involved, at least at a high level, in developing the cyber incident response and reporting capability. If there is an event, assuredly, both of these departments will be involved. Likely, the incident responders will not deal directly with the government contracting officer or Prime contractor, but will flow information through the contracts department to those entities. On top of legal and contracts, the contractor's security department will serve as liaison between federal agencies, such as the Defense Security Service (DSS), and the Federal Bureau of Investigation (FBI), depending on the severity of the cyber incident.

Document, Document, Document

To facilitate all these reporting requirements, a good document trail is essential. As referenced in the section on Containment, forms, such as a Chain of Custody form, provide a trail to ensure that media has been handled correctly, so that if necessary, it can serve as admissible evidence. Likewise, checklists and documented procedures show that the contractor has made a best effort post-incident to facilitate accurate reporting.

Understand the Costs.

While not explicitly stated, complying with the cyber incident response and reporting requirements will require contractors to expend capital. For small- and medium-sized contractors, this may take the form of outsourcing of services and staff. For larger contractors, this will likely mean bringing those resources in-house. Ultimately, this will have to be seen as the cost of doing business with the Department of Defense and being able to work on contracts that involve covered defense information. This is a matter than cannot be entered into lightly. With the December 31st, 2017 deadline for compliance approaching, it is the ultimate recommendation of this paper that contractors leverage available resources, specifically the CSC Critical Security Controls, to satisfy DFARS 252.204-7012 compliance.

Do Not Do Nothing

While the worst thing a contractor can do is misinterpret (i.e. lie) about its compliance with 252.204-7012, the next to the worst thing that it can do is not make an effort to implement a cyber incident response and reporting capability. This is one of the core components of 7012. Cyber incidents will occur, what a contractor does following them may be the difference in getting past the event or facing the consequences of non-compliance. Doing nothing to implement a cyber incident response and reporting capacity is essentially making a decision to no longer be a defense contractor.

Conclusions

In the course of this paper, the topic of compliance with DFARS 252.204-7012, with a specific focus on its incident response and reporting requirements has been discussed. After reviewing the relevant literature, including 252.204-7012 and SP 800-171 themselves, the study evaluated the feasibility of applying the CSC Critical Security Controls to satisfy compliance. Based on this research, it was possible to build a compliance effort around the CSC controls, with additional clarity provided in other documents in the NIST Special Publication series.

By attempting to compare this study with other existing studies, it became apparent that compliance with 252.204-7012 has not been a topic of much academic research. Most of what has been written on 252.204-7012 has either been written by federal offices themselves, or vendors seeking to assist contractors with meeting compliance. To be sure, satisfying compliance with 252.204-7012 with its SP 800-171 requirements is no easy task, but it is essential because that which is to be protected is some of the most sensitive unclassified information that exists; covered defense information.

While there were definitely limitations with this study, it does provide the information needed for a contractor to understand the compliance requirements related to cyber incident response and reporting and execute on their implementation ahead of the December 31st 2017 deadline.

Ultimately, it is up to each contractor to interpret the requirements and roll out a solution. Failure to do so has multiple consequences. Non-compliance may result in breach of contract and the potential for a contractor to lose business. Even more critical, however, is that it may result in the compromise of covered defense information that could have a negative impact on national security. With the significant consequences in mind, it is imperative that all contractors aim for success.

References

Center for Internet Security. (2016, August 31). *The CIS Critical Security Controls for Effective Cyber Defense Version 6.1*. Retrieved March 16, 2017, from https://www.cisecurity.org/critical-controls/documents/CSC-MASTER-VER61-FINAL.pdf

Davenport, C. (2014, September 09). *USIS contracts for federal background security checks won't be renewed*. Retrieved April 23, 2017, from The Washington Post: https://www.washingtonpost.com/business/economy/opm-to-end-usis-contracts-for-background-security-checks/2014/09/09/4fcd490a-3880-11e4-9c9f-ebb47272e40e_story.html?utm_term=.a31a61e140af

Defense Information Systems Agency. (2017, February 16). *DoD Approved 8570 Baseline Certifications*. Retrieved April 09, 2017, from http://iase.disa.mil/iawip/Pages/iabaseline.aspx

Defense Information Systems Agency. (n.d.). *Assured Compliance Assessment Solution (ACAS)*. Retrieved 04 09, 2017, from http://disa.mil/Cybersecurity/Network-Defense/ACAS

Government Publishing Office. (2013, November 18). *Federal Register Volume 78, Number 222*. Retrieved March 20, 2017, from https://www.gpo.gov/fdsys/pkg/FR-2013-11-18/html/2013-27313.htm

McAfee. (2012, March 06). *U.S. Department of Defense Extends McAfee Key Role in Largest IT Security System Deployment*. Retrieved April 13, 2017, from https://www.mcafee.com/us/about/news/2012/q1/20120306-02.aspx

National Institute of Standards and Technology. (2007, February). *The topic of IDPSes is even important enough to justify its own NIST Special Publication: 800-94 Guide* *to Intrusion Detection and Prevention Systems (IDPS)* . Retrieved April 13, 2017, from http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf

National Institute of Standards and Technology. (2015, January 22). *SP 800-53 Security and Privacy Controls for Federal Information Systems and Organizations.* Retrieved March 25 2017, from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

National Institute of Standards and Technology. (2016, December). *NIST Special Publication 800-184 Guide for Cybersecurity Event Recovery*. Retrieved April 13, 2017, from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-184.pdf

National Institute of Standards and Technology. (2016, January 16). *SP 800-171 Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations.* Retrieved March 16, 2017, from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171.pdf

Office of the Under Secretary of Defense for Acquisition, Technology and Logistics. (2009, October 15). *DFARS Table of Contents.* Retrieved March 20, 2017, from http://www.acq.osd.mil/dpap/dars/dfars/html/r20110916/tochtml.htm

Office of the Under Secretary of Defense for Acquisition, Technology and Logistics. (2013, November). *Safeguarding of Unclassified Controlled Technical Information.* Retrieved March 16, 2017, from http://web.archive.org/web/20140331131434/http://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm#252.204-7012

Office of the Under Secretary of Defense for Acquisition, Technology and Logistics. (2016, October). *DFARS 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting.* Retrieved from http://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm#252.204-7012

Office of the Under Secretary of Defense for Acquisition, Technology and Logistics. (2017, January 27). *Frequently Asked Questions (FAQs) regarding the implementation of DFARS Subpart 204.73 and PGI Subpart 204.73 DFARS Subpart 239.76 and PGI Subpart 239.76.* Retrieved March 26, 2017, from http://www.acq.osd.mil/dpap/pdi/docs/FAQs_Network_Penetration_Reporting_and_Contracting_for_Cloud_Services_(01-27-2017).pdf

Sandler, L., & Tan, A. (2015, February 09). *Altegrity Files Bankruptcy After 'State-Sponsored' Breach*. Retrieved April 23, 2017, from Bloomberg: https://www.bloomberg.com/news/articles/2015-02-09/altegrity-files-for-bankruptcy-after-losing-vetting-contracts

Scalet, S. D. (2005, December 01). *How to Keep a Digital Chain of Custody*. Retrieved April 13, 2017, from http://www.csoonline.com/article/2118807/investigations-forensics/how-to-keep-a-digital-chain-of-custody.html

The White House Office of the Press Secretary. (2016, July 26). *Presidential Policy Directive (PPD)/PPD-41* . Retrieved March 16, 2017, from https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident

U. S. General Services Administration. (2014, May 29). *Federal Acquisition Regulation.* Retrieved March 20, 2017, from https://www.acquisition.gov/sites/default/files/current/far/pdf/FAR.pdf

Appendix A 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting

As prescribed in 204.7304(c), 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.

"Forensic analysis" means the practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data.

"Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

"Malicious software" means computer software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. This definition includes a virus, worm, Trojan horse, or other code-based entity that infects a host, as well as spyware and some forms of adware.

"Media" means physical devices or writing surfaces including, but is not limited to, magnetic tapes, optical disks, magnetic disks, large-scale integration memory chips, and printouts onto which covered defense information is recorded, stored, or printed within a covered contractor information system.

''Operationally critical support'' means 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.

"Rapidly report" means within 72 hours of discovery of any cyber incident.

"Technical information" means technical data or computer software, as those terms are defined in the clause at DFARS 252.227-7013, Rights in Technical Data—Noncommercial Items, regardless of whether or not the clause is incorporated in this solicitation or contract. Examples of technical information include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code.

(b) *Adequate security*. The Contractor shall provide adequate security on all covered contractor information systems. To provide adequate security, the Contractor shall implement, at a minimum, the following information security protections:

(1) For covered contractor information systems that are part of an Information Technology (IT) service or system operated on behalf of the Government, the following security requirements apply:

(i) Cloud computing services shall be subject to the security requirements specified in the clause 252.239-7010, Cloud Computing Services, of this contract.

(ii) Any other such IT service or system (i.e., other than cloud computing) shall be subject to the security requirements specified elsewhere in this contract.

(2) For covered contractor information systems that are not part of an IT service or system operated on behalf of the Government and therefore are not subject to the security requirement specified at paragraph (b)(1) of this clause, the following security requirements apply:

(i) Except as provided in paragraph (b)(2)(ii) of this clause, the covered contractor information system shall be subject to the security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and

Organizations" (available via the internet at http://dx.doi.org/10.6028/NIST.SP.800-171) in effect at the time the solicitation is issued or as authorized by the Contracting Officer.

(ii)(A) The Contractor shall implement NIST SP 800-171, as soon as practical, but not later than December 31, 2017. For all contracts awarded prior to October 1, 2017, the Contractor shall notify the DoD Chief Information Officer (CIO), via email at osd.dibcsia@mail.mil, within 30 days of contract award, of any security requirements specified by NIST SP 800-171 not implemented at the time of contract award.

(B) The Contractor shall submit requests to vary from NIST SP 800-171 in writing to the Contracting Officer, for consideration by the DoD CIO. The Contractor need not implement any security requirement adjudicated by an authorized representative of the DoD CIO to be nonapplicable or to have an alternative, but equally effective, security measure that may be implemented in its place.

(C) If the DoD CIO has previously adjudicated the contractor's requests indicating that a requirement is not applicable or that an alternative security measure is equally effective, a copy of that approval shall be provided to the Contracting Officer when requesting its recognition under this contract.

(D) If the Contractor intends to use an external cloud service provider to store, process, or transmit any covered defense information in performance of this contract, the Contractor shall require and ensure that the cloud service provider meets security requirements equivalent to those established by the Government for the Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline (https://www.fedramp.gov/resources/documents/) and that the cloud service provider complies with requirements in paragraphs (c) through (g) of this clause for cyber incident reporting, malicious software, media preservation and protection, access to additional information and equipment necessary for forensic analysis, and cyber incident damage assessment.

(3) Apply other information systems security measures when the Contractor reasonably determines that information systems security measures, in addition to those identified in paragraphs (b)(1) and (2) of this clause, may be required to provide adequate security in a dynamic environment or to accommodate special circumstances (e.g., medical devices) and any individual, isolated, or temporary deficiencies based on an assessed risk or vulnerability. These measures may be addressed in a system security plan.

(c) *Cyber incident reporting requirement.*

(1) When the Contractor discovers a cyber incident that affects a covered contractor information system or the covered defense information residing therein, or that affects the contractor's ability to perform the requirements of the contract that are designated as operationally critical support and identified in the contract, the Contractor shall—

(i) Conduct a review for evidence of compromise of covered defense information, including, but not limited to, identifying compromised computers, servers, specific data, and user accounts. This review shall also include analyzing covered contractor information system(s) that were part of the cyber incident, as well as other information systems on the Contractor's network(s), that may have been accessed as a result of the incident in order to identify compromised covered defense information, or that affect the Contractor’s ability to provide operationally critical support; and

(ii) Rapidly report cyber incidents to DoD at http://dibnet.dod.mil.

(2) *Cyber incident report.* The cyber incident report shall be treated as information created by or for DoD and shall include, at a minimum, the required elements at http://dibnet.dod.mil.

(3) *Medium assurance certificate requirement*. In order to report cyber incidents in accordance with this clause, the Contractor or subcontractor shall have or acquire a DoD-approved medium assurance certificate to report cyber incidents. For information on obtaining a DoD-approved medium assurance certificate, see http://iase.disa.mil/pki/eca/Pages/index.aspx.

(d) *Malicious software*. When the Contractor or subcontractors discover and isolate malicious software in connection with a reported cyber incident, submit the malicious software to DoD Cyber Crime Center (DC3) in accordance with instructions provided by DC3 or the Contracting Officer. Do not send the malicious software to the Contracting Officer.

(e) *Media preservation and protection*. When a Contractor discovers a cyber incident has occurred, the Contractor shall preserve and protect images of all known affected information systems identified in paragraph (c)(1)(i) of this clause and all relevant monitoring/packet capture data for at least 90 days from the submission of the cyber incident report to allow DoD to request the media or decline interest.

(f) *Access to additional information or equipment necessary for forensic analysis*. Upon request by DoD, the Contractor shall provide DoD with access to additional information or equipment that is necessary to conduct a forensic analysis.

(g) *Cyber incident damage assessment activities*. If DoD elects to conduct a damage assessment, the Contracting Officer will request that the Contractor provide all of the damage assessment information gathered in accordance with paragraph (e) of this clause.

(h) *DoD safeguarding and use of contractor attributional/proprietary information*. The Government shall protect against the unauthorized use or release of information obtained from the contractor (or derived from information obtained from the contractor) under this clause that includes contractor attributional/proprietary information, including such information submitted in accordance with paragraph (c). To the maximum extent practicable, the Contractor shall identify and mark attributional/proprietary information. In making an authorized release of such information, the Government will implement appropriate procedures to minimize the contractor attributional/proprietary information that is included in such authorized release, seeking to include only that information that is necessary for the authorized purpose(s) for which the information is being released.

(i) *Use and release of contractor attributional/proprietary information not created by or for DoD.* Information that is obtained from the contractor (or derived from information obtained from the contractor) under this clause that is not created by or for DoD is authorized to be released outside of DoD—

(1) To entities with missions that may be affected by such information;

(2) To entities that may be called upon to assist in the diagnosis, detection, or mitigation of cyber incidents;

(3) To Government entities that conduct counterintelligence or law enforcement investigations;

(4) For national security purposes, including cyber situational awareness and defense purposes (including with Defense Industrial Base (DIB) participants in the program at 32 CFR part 236); or

(5) To a support services contractor ("recipient") that is directly supporting Government activities under a contract that includes the clause at 252.204-7009, Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information.

(j) *Use and release of contractor attributional/proprietary information created by or for DoD.* Information that is obtained from the contractor (or derived from information obtained from the contractor) under this clause that is created by or for DoD (including the information submitted pursuant to paragraph (c) of this clause) is authorized to be used and released outside of DoD for purposes and activities authorized by paragraph (i) of this clause, and for any other lawful Government purpose or activity, subject to all applicable statutory, regulatory, and policy based restrictions on the Government's use and release of such information.

(k) The Contractor shall conduct activities under this clause in accordance with applicable laws and regulations on the interception, monitoring, access, use, and disclosure of electronic communications and data.

(l) *Other safeguarding or reporting requirements*. The safeguarding and cyber incident reporting required by this clause in no way abrogates the Contractor's responsibility for other safeguarding or cyber incident reporting pertaining to its unclassified information systems as required by other applicable clauses of this contract, or as a result of other applicable U.S. Government statutory or regulatory requirements.

(m) *Subcontracts*. The Contractor shall—

(1) Include this clause, including this paragraph (m), in subcontracts, or similar contractual instruments, for operationally critical support, or for which subcontract performance will involve covered defense information, including subcontracts for commercial items, without alteration, except to identify the parties. The Contractor shall determine if the information required for subcontractor performance retains its identity as covered defense information and will require protection under this clause, and, if necessary, consult with the Contracting Officer; and

(2) Require subcontractors to—

(i) Notify the prime Contractor (or next higher-tier subcontractor) when submitting a request to vary from a NIST SP 800-171 security requirement to the Contracting Officer, in accordance with paragraph (b)(2)(ii)(B) of this clause; and

(ii) Provide the incident report number, automatically assigned by DoD, to the prime Contractor (or next higher-tier subcontractor) as soon as practicable, when reporting a cyber incident to DoD as required in paragraph (c) of this clause.

(End of clause)

Appendix B Selected NIST SP 800-53 Controls

IR-2 Incident Response Training

Control: The organization provides incident response training to information system users consistent with assigned roles and responsibilities:

a. Within [Assignment: organization-defined time period] of assuming an incident response role or responsibility;
b. When required by information system changes; and
c. [Assignment: organization-defined frequency] thereafter.

Supplemental Guidance: Incident response training provided by organizations is linked to the assigned roles and responsibilities of organizational personnel to ensure the appropriate content and level of detail is included in such training. For example, regular users may only need to know who to call or how to recognize an incident on the information system; system administrators may require additional training on how to handle/remediate incidents; and incident responders may receive more specific training on forensics, reporting, system recovery, and restoration. Incident response training includes user training in the identification and reporting of suspicious activities, both from external and internal sources. Related controls: AT-3, CP-3, IR-8.

Control Enhancements:

(1) Incident Response Training | Simulated Events
The organization incorporates simulated events into incident response training to facilitate effective response by personnel in crisis situations.

(2) Incident Response Training | Automated Training Environments
The organization employs automated mechanisms to provide a more thorough and realistic incident response training environment.

References: NIST Special Publications 800-16,800-50.

IR-4 Incident Handling

Control: The organization:

a. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery;
b. Coordinates incident handling activities with contingency planning activities; and
c. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implements the resulting changes accordingly.

Supplemental Guidance: Organizations recognize that incident response capability is dependent on the capabilities of organizational information systems and the mission/business processes being supported by those systems. Therefore, organizations consider incident response as part of the definition, design, and development of mission/business processes and information systems. Incident-related information can be obtained from a variety of sources including, for example, audit monitoring, network monitoring, physical access monitoring, user/administrator reports, and reported supply chain events. Effective incident handling capability includes coordination among many organizational entities including, for example, mission/business owners, information system owners, authorizing officials, human resources offices, physical and personnel security offices, legal departments, operations personnel, procurement offices, and the risk executive (function). Related controls: AU-6, CM-6, CP-2, CP-4, IR-2, IR-3, IR-8, PE-6, SC-5, SC-7, SI-3, SI-4, SI-7.

Control Enhancements:

(1) Incident Handling | Automated Incident Handling Processes
The organization employs automated mechanisms to support the incident handling process.
Supplemental Guidance: Automated mechanisms supporting incident handling processes include, for example, online incident management systems.

(2) Incident Handling | Dynamic Reconfiguration
The organization includes dynamic reconfiguration of [Assignment: organization-defined information system components] as part of the incident response capability.
Supplemental Guidance: Dynamic reconfiguration includes, for example, changes to router rules, access control lists, intrusion detection/prevention system parameters, and filter rules for firewalls and gateways. Organizations perform dynamic reconfiguration of information systems, for example, to stop attacks, to misdirect attackers, and to isolate components of systems, thus limiting the extent of the damage from breaches or compromises. Organizations include time frames for achieving the reconfiguration of information systems in the definition of the reconfiguration capability, considering the potential need for rapid response in order to effectively address sophisticated cyber threats. Related controls: AC-2, AC-4, AC-16, CM-2, CM-3, CM-4.

(3) Incident Handling | Continuity of Operations
The organization identifies [Assignment: organization-defined classes of incidents] and [Assignment: organization-defined actions to take in response to classes of incidents] to ensure continuation of organizational missions and business functions.
Supplemental Guidance: Classes of incidents include, for example, malfunctions due to design/implementation errors and omissions, targeted malicious attacks, and untargeted malicious attacks. Appropriate incident response actions include, for example, graceful degradation, information system shutdown, fall back to manual mode/alternative technology whereby the system operates differently, employing deceptive measures, alternate information flows, or operating in a mode that is reserved solely for when systems are under attack.

(4) Incident Handling | Information Correlation

The organization correlates incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response.

Supplemental Guidance: Sometimes the nature of a threat event, for example, a hostile cyber attack, is such that it can only be observed by bringing together information from different sources including various reports and reporting procedures established by organizations.

(5) Incident Handling | Automatic Disabling of Information System

The organization implements a configurable capability to automatically disable the information system if [Assignment: organization-defined security violations] are detected.

(6) Incident Handling | Insider Threats - Specific Capabilities

The organization implements incident handling capability for insider threats.

Supplemental Guidance: While many organizations address insider threat incidents as an inherent part of their organizational incident response capability, this control enhancement provides additional emphasis on this type of threat and the need for specific incident handling capabilities (as defined within organizations) to provide appropriate and timely responses.

(7) Incident Handling | Insider Threats - Intra-Organization Coordination

The organization coordinates incident handling capability for insider threats across [Assignment: organization-defined components or elements of the organization].

Supplemental Guidance: Incident handling for insider threat incidents (including preparation, detection and analysis, containment, eradication, and recovery) requires close coordination among a variety of organizational components or elements to be effective. These components or elements include, for example, mission/business owners, information system owners, human resources offices, procurement offices, personnel/physical security offices, operations personnel, and risk executive (function). In addition, organizations may require external support from federal, state, and local law enforcement agencies.

(8) Incident Handling | Correlation with External Organizations

The organization coordinates with [Assignment: organization-defined external organizations] to correlate and share [Assignment: organization-defined incident information] to achieve a cross- organization perspective on incident awareness and more effective incident responses.

Supplemental Guidance: The coordination of incident information with external organizations including, for example, mission/business partners, military/coalition partners, customers, and multitiered developers, can provide significant benefits. Cross-organizational coordination with respect to incident handling can serve as an important risk management capability. This capability allows organizations to leverage critical information from a variety of sources to effectively respond to information security-related incidents potentially affecting the organization’s operations, assets, and individuals.

(9) Incident Handling | Dynamic Response Capability

The organization employs [Assignment: organization-defined dynamic response capabilities] to effectively respond to security incidents.
Supplemental Guidance: This control enhancement addresses the deployment of replacement or new capabilities in a timely manner in response to security incidents (e.g., adversary actions during hostile cyber attacks). This includes capabilities implemented at the mission/business process level (e.g., activating alternative mission/business processes) and at the information system level. Related control: CP-10.

(10) Incident Handling | Supply Chain Coordination

The organization coordinates incident handling activities involving supply chain events with other organizations involved in the supply chain.
Supplemental Guidance: Organizations involved in supply chain activities include, for example, system/product developers, integrators, manufacturers, packagers, assemblers, distributors, vendors, and resellers. Supply chain incidents include, for example, compromises/breaches involving information system components, information technology products, development processes or personnel, and distribution processes or warehousing facilities.

References: ExecutiveOrder13587; NIST Special Publication 800-61.