Cybersecurity Compliance for DoD Contractors

Xact IT Solutions
There are no IT problems.. only IT solutions

www.xitx.com
856.282.4100

EXECUTIVE SUMMARY

For contractors working with the Department of Defense, it is important that they comply with the Defense Federal Acquisition Regulation Supplement (DFARS) clause, specifically the National Institute of Standards and Technology's special publication 800-171.
These clauses serve to "Safeguarding Covered Defense Information and Cyber Incident Reporting" (Section 252.204-7012), mandating that every Department of Defense contractor (and their subcontractors) need to have "adequate cybersecurity protocols" in place as referenced in NIST SP 800-171.

There are seventy-nine (79) different security controls classified into 14 families that will be identified here to help contractors and subcontractors understand what they need to achieve compliance with NIST. These have been addressed over time via NISTIR to cater to the ever-evolving cyberthreats over time, which this publication will address.

Furthermore, this publication will also delve into the phrasing of the clause to explain the relaxation provided, and how virtually any company can conduct business with the DoD. Provided they comply with DoD's newest verification mechanism; the Cybersecurity Maturity Model Certification (CMMC)

INTRODUCTION

Contractors and subcontractors are obligated by the security protocols in DFARS and NIST to maintain adequate security standards. As the clause puts it:

"Protective measures that commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information."

Without said cybersecurity protocols in place, no contractor is allowed to work for the Department of Defense and no subcontractor is allowed to work for a contractor thereof. The idea is to ensure that no military secrets find unauthorized access or use, which could be devastating for serving and retired personnel, not to mention to the military as a whole.

However, NIST 800-171 also allows some 'wiggle room', allowing alternative approaches to be observed by contractors and subcontractors to achieve the same results. Furthermore, they could seek written approval from the DoD, suggesting that,

"Alternative but equally effective security measures may be used to compensate for the inability to satisfy a particular requirement."

If that is what contractors are willing to do, they must notify the DoD via email (osd.dibcsia@mail.mil) or a physical letter no later than thirty (30) days of the date a contract was awarded. It must include details about any deficiencies in observing NIST SP 800-171.

COMPLYING WITH NIST SP 800-171

The NIST SP 800-171 covers Controlled Unclassified Information (CUI) and requirements for its storage. It is important to note what NIST and DFARS mean by the term CUI:

Controlled Unclassified Information is any information that is deemed necessary for the performance of a DoD contract, along with any supporting information relevant to the contract.

This is a rather broad definition and can mean any type of information. Put simply, contractors may identify whether they're working for DoD and the GENERAL nature of what they're doing without delving into any specifics.

NISTIR – THE 2020 UPDATES

NISTIR stands for NIST Interagency or Internal Report and includes reports of findings via research and development. These include background information about FIPS and SPs as well. The new update basically acts as an instruction manual for SPs, including NIST SP 800-171.

NISTIR has released numerous publications from time to time, while in 2020 their reports mostly catered to:

- 5G Cybersecurity
- Cloud security
- Network behavior of IoTs (Internet of Things)
- Cryptographic standards (such as module validation programs, key generation, and other mechanisms)
- Supply chain risks, and
- Maintaining overall cybersecurity hygiene

NIST rules are applicable to all parties included in a contract, while the leniencies are applicable to both as well. NISTIR looks to guide all parties involved in maintaining the overall security of military and operational information security.

Involved parties must maintain a suitable cyberenvironment at all times to ensure CUI will be stored, processed, and transmitted safely. This doesn't just include establishing secure lines of communication or ensuring that computer systems are safeguarded from unauthorized access, but also ensuring that employees involved in the contract are practicing the necessary security and privacy protocols with regards to information.

Here is a quick overview of 2020 publications and how they're going to change the requirements of becoming a DoD contractor.

Publication	Date	Publication	Overview
5G Cybersecurity: Preparing a Secure Evolution to 5G	04/13/2020	-	A phased approach towards 5G use case scenarios and how 5G security features can be utilized
VMware Hybrid Cloud Infrastructure as a Service (IaaS) Environments	04/13/2020	SP1800-19	For IT professionals to implement a secure cloud infrastructure
Characterizing Network Behavior of Internet of Things Devices	04/11/2020	-	Demonstration on using device characterization techniques in order to secure Internet of Things (IoT) communications
Access Control Guidance for Cloud Systems	04/01/2020	SP 800-210	Guide to setting cloud access control characteristics for cloud service models including IaaS, PaaS, and SaaS.
Cryptographic Mechanisms	03/31/2020	SP800-175B Rev. 1	Guidance and standards towards using cryptography on information during transmission and in storage

Critical Cybersecurity Hygiene	03/30/202	-	An overall cybersecurity guidance
Managing the Security of Mobile Devices in the Enterprise	03/24/2020	SP800-124 Rev. 2	Technological and strategy recommendations towards making mobile devices more secure.
Key-Derivation Methods in Key-Establishment Schemes	03/24/2020	SP800-56C Rev. 2	Using "hybrid" secrets and conditions for using multiple instances of key expansion.
CMVP Validation Authority Updates	03/20/2020	SP800-140 to 800-140F	Revisions and additions to existing SP 800-140 series NIST.
Integrating Cybersecurity and Enterprise Risk Management (ERM)	03/19/2020	NISTIR-8286	Overview of ERM and how it can be implemented
Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Solutions	03/18/2020	NISTIR-8170	Guide to Enterprise Telework and remote access for employees in light of coronavirus
Zero Trust Architecture	03/17/2020	-	Guide to implementing an infrastructure which eliminates any trust assumption from users and networks
Impact Analysis Tool for Interdependent Cyber Supply Chain Risks	03/13/2020	NISTIR-8272	Guide to implementation of Cyber Supply Chain Risk Management (C-SCRM) tool to secure interconnected supply chains.
Digital Identity Guidelines	03/02/2020	SP800-63-3	An overview of guidelines to enhance and secure digital identity.

NIST SP AND NISTIR COMPLIANCE – Why Is It Necessary?

Time to time, the Department of Defense (DoD) will seek third party external contractors or suppliers to work for them. This may include performing a certain service or supplying something that DoD can't procure themselves without significant costs.

In doing so, sensitive data (CUI) is often shared with contractors such as operation details, military personnel involvement, or something as trivial as dates and timestamps. If proper steps to ensure security of this information aren't observed, it could threaten national security, not to mention provide loopholes to enemies of the state to exploit.

Adequate protection of CUI in federal as well as nonfederal systems can mean the federal government can successfully go through with the assigned missions and operations without any hitches.

ACHIEVING NIST COMPLIANCE

Complying with NIST is synonymous to achieving impeccable security standards, but it is important to note that:

"Perfection is sought after, but isn't the standard."

This is why NIST and DFARS allow incident reporting and mitigation of risks that follow. However, it is a failsafe and there are reprimands nonetheless if the contractor is found guilty. Having said that, where NIST compliance officers aren't looking for perfection, they also suggest that,

"Most compliance issues are a result of poor configuration management."

This means that in order to implement adequate security measures in terms of CUI, contractors and subcontractors are obligated to incorporate sufficient information-protection measures to minimize the probability of mishandling of information.

FAMILIES OF CONTROL

NIST defined the security requirements in its Special Publication 800-171 in fourteen (14) different "families" of control to make them easy to understand and implement. Each family represents a certain number of basic security requirements carried forward form the FIPS 200 and a certain number of derived security requirements carried forward from NIST SP 800-53.

The "Basic Security Requirements" can be defined as the goals of implementing each security measure, those measures being the "Derived Security Requirements."

Here is a table showing the fourteen different families, what they represent, and the number of requirements under each family.

Control Family	Abstract	Basic Requirements	Derived Requirement
Access Control	Controlling who has access	2	20
Awareness/Training	Training/educating about incidents	2	1
Audit/Accountability	Ensuring information is stored and used responsibly	2	7
Configuration Management	Establishing/maintaining consistency of information	2	7
Identification/Authentication	Authentication of data files and personnel	2	9
Incident Response	*See section "Incident Reporting" below*	2	1
Maintenance	Data maintenance and regular checkups	2	4
Media Protection	Media access control and maintenance	3	6
Personnel Security	Security of key personnel	2	0
Physical Protection	Protection of servers and storage physically	2	4
Risk Assessment	Assessing the prevalence of cybercrimes	1	2
Security Assessment	Assessing the situation of cybersecurity	3	0
System & Communications Protection	Protection of existing security and communications systems	2	14
System & Information Integrity	Maintaining the integrity of systems and information stored	3	4
	Total	**30**	**79**

INCIDENT RESPONSE & REPORTING UNDER NIST 800-171

Under NIST SP 800-171, "incident" refers to a "cyber incident," a rather broad term if looked at closely. It is defined as:

Any network compromise that has an "adverse effect" or a "potentially adverse effect" on the network, CUI, or the ability to execute a critical operation or contract requirements.

Another phrase used for defining incident is,

"Activities considered to be essential to the mobilization, deployment, or sustainment of the Armed Forces in a contingency operation."

In case of any incident, contractors and subcontractors are to report it immediately. Even attempted intrusions, successful or not, should be reported to the handler, who will then report it to the relevant authorities. In case of a breach, steps would be taken to mitigate the damage of stolen information and inquiry may also be conducted on the contractor or subcontractor to see whether NIST and DFARS requirements were being followed or not.

CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC) – What is It?

The Cybersecurity Maturity Model Certification (CMMC) is an effort by Department of Defense to ensure that every contractor and subcontractor with access to CUI is compliant with DFARS, NIST, and other cybersecurity protocols necessary for ensuring information safety.

DoD announced this system mid-2019 and has several requirements, each identifying a 'level' of cybersecurity compliance. As usual, all contractors or sub-contractors working with DoD will have to comply with at least level 1 of CMMC. **Here is a quick overview of the levels and how it's determined:**

Level 1 - Requires the bare minimum-security compliance, i.e., 17 NIST 800-171 Requirements

Level 2 - 7 cybersecurity compliance practices must be followed along with 65 NIST 800-171 requirements

Level 3 - 20 cybersecurity compliance practices must be followed along with 110 NIST 800-171 requirements

Level 4 - 46 cybersecurity compliance practices must be followed along with 110 NIST 800-171 requirements

Level 5 - 61 cybersecurity compliance practices must be followed along with 110 NIST 800-171 requirements

The DoD is currently training third-party assessment organizations (3PAOa), which will be done with around April/May 2020. Contractors will be able to make Request for Information about CMMC by June 2020, while Request for Proposals will find CMMC by August or September of 2020.

This signifies that existing and new **contractors must comply with CMMC protocols by fall 2020, at the latest.**

WHAT EXACT IT SOLUTIONS CAN DO TO HELP

Military secrets have always been closely guarded, and as the Department of Defense invites more and more contractors to carry out operations, the risk for these secrets spilling out increases as well. This is where NIST, DFARS, and CMMC compliance play their roles in safeguarding this information.

However, implementation of these security protocols might be trickier than the ordinary firewall security measures. These control "families" need to be incorporated on an infrastructural level, requiring architectural planning and implementation.

Xact IT Solutions has been doing this for clients ever since these requirements were set forth by doing the following:

- Identifying information security gaps in architecture policies and system design.
- Implementing enhancements and threat mitigation AI via advanced security engineering, giving companies minimum to no disruptions in their IT services.
- Offering cyber operations support 24/7 to maximize cybersecurity.
- Using a proactive approach to assess and mitigate risks.

Since mid-2019, more and more contractors and subcontractors have been trying to comply with NIST 800-171 requirements along with other compliance practices. We have successfully helped countless companies climb the ranks in terms of trusted contractors and reach the maximum CMMC level.

For more information on cybersecurity compliance for DoD, contact us at **marketing@xitx.com** or get in touch via phona at **856.282.4100**.

Xact IT Solutions
There are no IT problems.. only IT solutions

www.xitx.com