The CMMC And The NIST 800-171

A Whitepaper Written For KAMIND IT, Inc.

By Ravi Das

Table of Contents

Introduction....3
The Background Into The NIST SP 800 -171....3
The Differences Between The FCI And The CUI....4
The CMMC....5
The CMMC Version 1.0....5
The CMMC Version 2.0....7
What Is New In The CMMC 2.0 – The Self-Assessments of Controls....7
What Is New In The CMMC 2.0 – The Maturity Levels....7
What Is New In The CMMC 2.0 – The Domains....8
What Is New In The CMMC 2.0 – The Use Of Waivers & POA&Ms....9
A Summary Of The Differences....10
The CMMC 2.1....10
The NIST 800-171....14
The NIST SP 800-171 Version 2....15
The NIST SP 800-171 Version 3....15
The Changes....15
The Details....15
Other Areas Of Concern....16
The Details: Other Areas Of Concern....16
Other Updates....17
Conclusions....19
Sources....20

Introduction

Most people who are involved with doing work for the United States Federal Government, especially for the Department of Defense (hereinto referred to as the "DoD") have at least heard of the NISTS Special Publication 800-171. In this whitepaper, we do a deeper dive into the last version of it that has recently come out, is known as the "R3".

The Background Into The NIST SP 800 -171

The DoD releases two kinds of datasets that contracts work with when they are fulfilling a contract that they have been awarded by them. They are as follows:

1) The CUI:

   This is an acronym that stands for "Controlled Unclassified Information". It can be technically defined as follows:

   "Controlled Unclassified Information is unclassified information the United States Government creates or possesses that requires safeguarding or dissemination controls limiting its distribution to those with a lawful government purpose. CUI may not be released to the public absent further review."

   (SOURCE: 1).

   In other words, while these kinds of datasets are confidential in nature, under certain circumstances, they can be shared "freely" with other entities from within the Federal Government. For instance, members of Congress can get access to and discuss these datasets, but within certain guidelines. Also as mentioned, CUI datasets cannot be released for public consumption under any circumstances.

2) The FCI:

   This is an acronym that stands for "Federal Contract Information". It can be technically defined as follows:

   "Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) are types of data that are collected, created, transmitted or received as a requirement of fulfilling the obligations of the contract – to develop or deliver a product or service."

   (SOURCE: 2).

   In many ways similar to that of the CUI datasets, FCI datasets are also available for consumption for the different entities in the Federal Government that need them, under certain circumstances. But once again, they cannot be released to the public whatsoever.

The Differences Between The FCI And The CUI

While the FCI datasets and the CUI datasets may appear to be similar to one another from the outset, in reality, there are subtle differences between them. They are as follows:

1) The Level Of Compliance:

   The FCI datasets are protected under the FAR 52.204-21, which is also known as the "Basic Safeguarding of Covered Contractors Information Systems". However, the CUI datasets are protected under the NIST 800-171, which is entitled the "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations".

2) The CMMC Requirements:

   This is a topic that will be addressed in the next section of this whitepaper. But for right now, the FCI datasets are addressed in Maturity Level 1 of the CMMC, whereas the CUI datasets are addressed at the Maturity Level 2 of the CMMC. The controls that are mandated to protect the FCI datasets are also required under Maturity Level 1 of the CMMC. Whereas, the controls that are mandated to protect the CUI datasets are mandated under Maturity Level 2 of the CMMC.

3) The Mandates:

   It is Executive Order 13556 that established the framework for the management of the CUI datasets. For the FCI datasets, the frameworks that have been established by the United States military, and the National Aeronautics and Space Administration (NASA) , that are used primarily for the management of the CUI datasets.

4) The Markings:

   The CUI datasets are pieces of information that are marked and identified as requiring protection to a high degree. In contrast, the FCI datasets are pieces of information that is not specifically marked for public release, but their subject to being protected with only minimal levels of Cybersecurity Controls.

5) The Labelling:

   It is the specific entity that receives and makes use of the CUI that is ultimately responsible for labeling it as such. In contrast to this, is no classification system or labelling that are required for the FCU datasets.

6) The Subsets:

At the present time, there are no classification subsets for the FCI datasets. But for the CUI datasets, there are two of them, which are:

- The CUI Basic:

  This requires no specific handling or dissemination controls fo any type or kind.

- The CUI Specified:

This requires 100% protection of the information contained from within the datasets, the controls that are needed to safeguard them are completely provided.

The CMMC

This is an acronym that stands for the "Cybersecurity Maturity Model Certification". Simply, this is where the DoD required that the Defense Industrial Base (DIB) and other related entities that are wishing to place competitive bids and eventually be awarded contracts based upon them must to come to a certain level of certification. By achieving this particular certification, it reflects that the defense contractors and their subcontractors have the needed Cybersecurity controls in order to protect both the CUI datasets and the FCI datasets. There have been two different versions of the CMMC, and an overview of both of them are provided in the next two subsections.

The CMMC Version 1.0

In this first cut, there are five different levels of Maturity Levels in which a certification can be achieved at. This was released to the public on January 31st, 2020. This version is composed of five distinct Maturity Levels, and they are as follows:

1) The CMMC Level 1:

   This is also referred to as "Basic Cyber Hygiene", and the controls that are implemented here are primarily meant for the safeguarding of the FCI datasets. More specifically, they should need to fortify the " . . . information systems that process, store or transmit Federal Contract Information."

   (SOURCE: 4).

2) The CMMC Level 2:

   This is also referred to as "Intermediate Cyber Hygiene." Achieving certification at this particular level shows to the DoD that the defense contractor (and their affiliated subcontractors) have implemented the minimum, level of controls that are needed to safeguard any kind or type of information/data that has been transmitted to them by the DoD.

3) The CMMC Level 3:

   This is also referred to as "Good Cyber Hygiene". Achieving certification at this particular level shows to the DoD that the defense contractor (and their affiliated subcontractors) have now implemented the needed controls to safeguard the CUI datasets.

4) The CMMC Level 4:

   This is also referred to as "Proactive Cyber Hygiene". Achieving certification at this particular level shows to the DoD that the defense contractor (and their affiliated subcontractors) that not

only do they have the requisite controls implemented to safeguard the CUI datasets, but they also have the ability to conduct regular Risk Assessment Analyses, and remediate any gaps, weaknesses, or vulnerabilities that have been identified. A main area of emphasis here is on the protection of the CUI datasets from Advanced Persistent Threats, also known as "APTs". This can be technically defined as follows:

"An advanced persistent threat (APT) is a sophisticated, sustained cyberattack in which an intruder establishes an undetected presence in a network in order to steal sensitive data over a prolonged period of time. An APT attack is carefully planned and designed to infiltrate a specific organization, evade existing security measures and fly under the radar."

(SOURCE: 4).

In other words, the defense contractor and their associated subcontractors need to have implemented not only the right levels of Cyber Hygiene, but also the needed controls in order to mitigate the risks of a Cyberattacker covertly entering into their IT/Network Infrastructure and launching a Data Exfiltration against the CUI datasets.

5) <u>The CMMC Level 5</u>:

This is also referred to as "Proactive Cyber Hygiene". Achieving certification at this particular level shows to the DoD that the defense contractor (and their affiliated subcontractors) can establish a set of best standards and practices to further mitigate the risks of an APT attack from happening.

Further, there are also seventeen major domains from within the CMMC 1.0 that provide further guidance to the defense contractor (and their associated subcontractors) as to how the controls should be created and deployed. These are reviewed in the matrix below:

Domain	*Description*
Domain 1	Access Control, also known as "AC".
Domain 2	Identification and Authentication, also known as "IA".
Domain 3	Media and Protection, also known as "MP".
Domain 4	Physical Protection, also known as "PE".
Domain 5	Systems and Communications, also known as "SC".
Domain 6	Systems and Information Integrity, also known as "SI".
Domain 7	Incident and Response, also known as "IR".
Domain 8	Maintenance, also known as "MA".
Domain 9	Personnel Security, also known as "PS".
Domain 10	Recovery, also known as "RE".
Domain 11	Risk Management, also known as "RM".
Domain 12	Security Assessment, also known as "CA".
Domain 13	Situational Awareness, also known as "SA".
Domain 14	Systems Communication Protection, also known as "SC".

Domain 15	System Information Integrity, also known as "SI".
Domain 16	Configuration Management, also known as "CM".
Domain 17	Awareness and Training, also known as "AT".

The CMMC Version 2.0

The second version of the CMMC, commonly referred to as the "CMMC 2.0", was just recently released on December 26th, 2023. Some of the reasons for this change include the complaints about the high cost that the defense contractors (and their associated subcontractors) experienced, and all of the administrative headaches that came about from trying to achieve a particular level of certification. In response to this, the DoD then announced the coming of the "CMMC 2.0" which actually decreased the amount of Maturity Levels that were required, and allowed for more flexibility when it came to self-attestation about the implemented controls. For example, rather than having to get an external party to do this, such as a "CMMC Third Party Assessor Organization" (also known as a "C3PAO")to this the defense contractor (and their associated subcontractors) can more or less do this on their own. In the next subsections, we take a closer look at the CMMC 2.0.

What Is New In The CMMC 2.0 – The Self-Assessments of Controls

As was reviewed earlier in this whitepaper, in the CMMC 1.0, there are five Maturity Levels. A defense contractor or even a subcontractor could get certified at any level they felt that they needed to, in order to bid on the appropriate contracts and projects. All of these Maturity Levels were based upon what is the known as the NIST Special Publication (SP) 800-171, which was earlier known as the DFARS clause 252.204-7012. This SP dealt specifically with the handling of just CUI datasets, and not so much the FCO ones. Also, under the CMMC 1.0, all Cybersecurity incidents had to reported to the DoD within a 72-hour timespan.

With the CMMC 1.0, defense contractors and their subcontractors cannot fill out self-assessment questionnaires on their own, rather these have to be filled out by an independent CMMC Third-Party Assessor Organization, also known as a "C3PAO").

But now, with the CMMC 2.0, these parties can now self-assess their own controls that have been put into place to protect both the CUI and FCI datasets. But, this is subject to random audit by the DoD in order to make everything all up to par, and that the self-assessment is accurate to the degree when it was first submitted. In this regard, the CMMC 1.0 has been deemed to be rigid, but this new flexibility that has been offered by the CMMC 2.0 has received a warmer reception.

What Is New In The CMMC 2.0 – The Maturity Levels

Another key difference here is in the number of Maturity Levels. As it was mentioned earlier, with the CMMC 1.0, there are five of them, but with the CMMC 2.0, there are now only three of them, which makes obtaining certification a quicker process in order to bid on the more lucrative contractors. They are as follows:

1) The CMMC Level 1:

This is also known as "Foundational". At this Maturity Level, only the basic Cybersecurity controls are deployed. The Defense contractors and their respective subcontractors can now conduct assessments on their own. The results of this must be certified by the C-Suite, and the questionnaires or checklists utilized must strictly follow the stipulations as set forth in FAR 52.204-21. This Maturity Level deals primarily with the FCI datasets.

2) The CMMC Level 2:

This is also known as "Advanced". At this Maturity Level, advanced Cybersecurity controls will need to be deployed, and detailed documentation must not only be kept about them, but also all of the processes that are involved in the IT/Network Infrastructure. This Maturity Level primarily deals with the CUI datasets. Self-assessments will also be allowed at this level as well, but for those defense contractors and subcontractors that will handle the CUI datasets that are deemed to be "Critical", must be fully assessed by the C3PAOs. Any CUI datasets that are deemed to be "Non-Critical" are not required to go through such a rigorous process.

3) The CMMC Level 3:

This is also known as "Expert". At this Maturity Level, the defense contractor (and their associated sub-contractors) are required to keep further detailed documentation on the deployment of the Cybersecurity controls. This should also contain the goals, missions, projects, resourcing, training, and the involvement of all of the parties that are involved. A key objective is to have all of this documentation map out carefully how the APT Threat Vector will be mitigated, as discussed earlier in this whitepaper. Also, this Maturity Level deals primarily with those CUI datasets that are deemed to be of the "Highest Priority". Also at this Maturity Level, all of the defense contractors and subcontractors must be certified at minimum every three years, by a "C3PAO".

What Is New In The CMMC 2.0 – The Domains

In the CMMC 2.0, there are also three less domains, when compared to the CMMC 1.0. They are as follows:

Domain	*Description*
Domain 1	Access Control, also known as "AC".
Domain 2	Identification and Authentication, also known as "IA".
Domain 3	Media and Protection, also known as "MP".
Domain 4	Physical Protection, also known as "PE".
Domain 5	Systems and Communications, also known as "SC".
Domain 6	Systems and Information Integrity, also known as "SI".
Domain 7	Incident and Response, also known as "IR".
Domain 8	Maintenance, also known as "MA".
Domain 9	Personnel Security, also known as "PS".

Domain 10	Situational Awareness, also known as “SA”.
Domain 11	Systems Communication Protection, also known as “SC”.
Domain 12	System Information Integrity, also known as “SI”.
Domain 13	Configuration Management, also known as “CM”.
Domain 14	Risk Assessment, also known as “RA”.

What Is New In The CMMC 2.0 – The Use Of Waivers & POA&Ms

Another primary tool that defense contractors and their subcontractors can use is what is known as the “Plan of Actions and Milestones, or the “POA&M” for short. This is another way to conduct a self-assessment of the controls that are already in place, but the caveat here is that this plan also has to have an actionable set of items that shows how any gaps or vulnerabilities will be remediated.

The POA&M was not at all allowed under the CMMC 1.0, but with the CMMC 2.0, it is now allowed. In fact, defense contractors and subcontractors can also use this as a path to achieve CMMC certification for their particular level that they are trying to achieve. But, along with the plan of action as just described, there must also be a concrete deadlines set in place as well.

Although the DoD has not exactly specified per se what kinds and types of controls can be used in the POA&M, they do highly recommend that the defense contractors and the subcontractors follow closely the guidelines that are outlined by the NIST Special Publication 800-171. Also, certain high value activities surrounding the protection of the CUI datasets cannot be included in the POA&M.

These include the following:

- Any type of Identity & Authentication Management processes or processes;
- Any Security Awareness Training programs for your employees or subcontractors;
- Any control-based audits, reviews, analyses, reporting processes, and record archiving;
- Any kind of portable storage destruction techniques;
- Any Risk Assessments, such as conducting Vulnerability, Penetration Testing, or Threat Hunting exercises.

A Summary Of The Differences

The key differences between the CMMC 1.0 and the CMMC 2.0 is illustrated below:

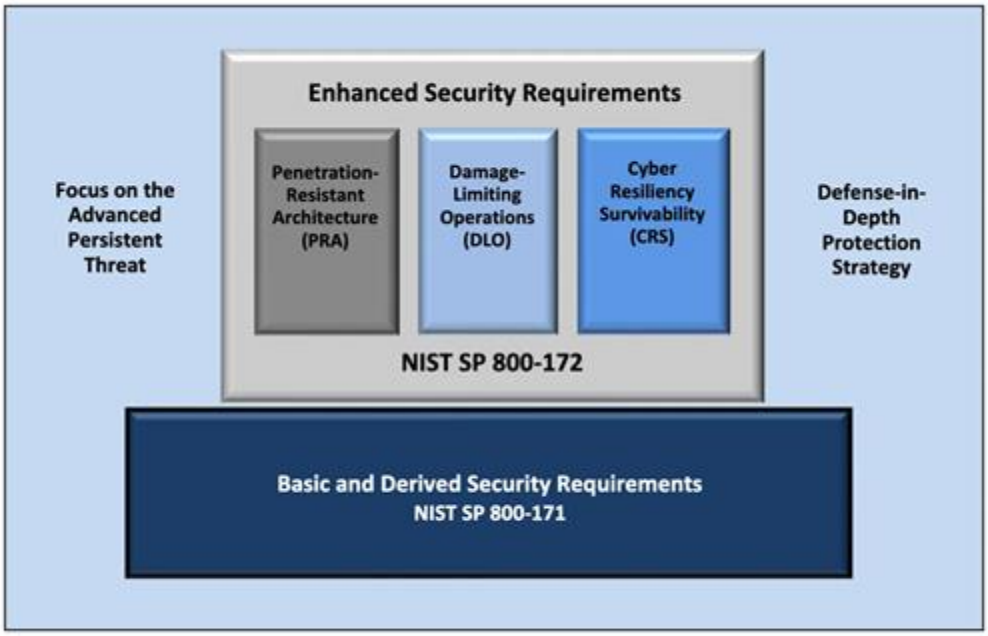


FIGURE 1: MULTIDIMENSIONAL (DEFENSE-IN-DEPTH) PROTECTION STRATEGY

(SOURCE: 6).

The CMMC 2.1

Just recently, there was an even newer version of the CMMC 2.0 that came out, but this time it is called the "CMMC 2.1". Although there are no significant changes to be expected, the only ones are updates to the language in some of the domains. They are as follows:

1) Access Control (AC):

   There are two updates:

- AC.L3-3.1.21: This states that stronger levels of encryption must be used when it comes to managing network devices. Not only must the data be encrypted, but any type of communications (whether it is hard wired or wireless) must also be encrypted as well. There can be no Plaintext messages sent under any circumstances.

- AC.L3-3.1.22: Tighter controls need to be put into place when it comes to accessing the CUI and FCI datasets using remote protocols (such as RDP).

  NOTE: This directly impacts Maturity Level 3.

2) Audit and Accountability (AU):

The changes proposed to this Domain reflect the updates that have been made to the NIST 800-171 Special Publication. This document forms the backbone for iterations of the CMMC, from Version 1 to Version 2 to the anticipated Version 2.1. This includes the following:

- AU.L2-3.2.5: This mandates that any auditing tools aby any entity must be protected as much as possible, which includes unauthorized access, deletion, and modifications.

- AU.L3-3.2.9: Any audited events must get more careful scrutinization.

NOTE: This directly impacts Maturity Levels 2 and 3.

3) Awareness and Training (AT):

The change here includes the following:

- AT.L3-3.3.6: The goal here is to provide further security training into Insider Threats, and how to make all employees aware of them, and the proper channels to use when reporting a possible breach.

4) Configuration Management (CM):

The updates the following:

- CM.L3-3.4.9: This deals primarily with Threat Hunting, especially focusing on those variants which are lurking inside the IT and Network Infrastructure. But this takes things one step further by adding tools which increases the detection of them, which will result in a quicker response rate in terms of mitigation.

NOTE: This directly impacts Maturity Level 3.

5) Identification and Authentication (IA):

The changes here are:

- IA.L3-3.5.11: This mandates the usage of MFA to those employee accounts that are deemed to be non-privileged in nature. This is designed to increase the overall security of the Cyber environment.

NOTE: This directly impacts Maturity Level 3.

6) Incident Response (IR):

The updates here include:

- IR.L3-3.6.9: This mandates the creation of a specific Cyber Incident Response team. But the goal here is to not just to respond, but to also have other functionalities such as investigations,

conducting forensics exams, and having the ability to enhance or put in new controls in order to prevent future security breaches from happening.

- IR.L3-3.6.10: The Incident Response Plan must be tested on a regular basis, and updated accordingly.

  NOTE: This directly impacts Maturity Level 3.

7) Maintenance (MA):

   The change here are:

- MA.L3-3.7.5: This requires that all devices and storage mechanisms must be purged of all data before it can be destroyed or even reused. The proper procedures have to be followed in order to ensure the total eradication of information and data.

  NOTE: This directly impacts Maturity Level 3.

8) Media Protection (MP):

   The update here is:

- MP.L3-3.8.8: This requires that any and all devices that contain specifically the CUI data must have tight access controls associated with them, in an effort to prevent data leakage, whether intentional or not.

  NOTE: This directly impacts Maturity Level 3.

9) Personnel Security (PS):

   The enhancement here is:

- PS.L3-3.9.4: This strictly mandates and enforces that only full authenticated employees can enter the place of a Defense Contractor, or their respective Subcontractors.

  NOTE: This directly impacts Maturity Level 3.

10) Physical Protection (PE):

    The change here includes the following:

- PE.L3-3.10.5: This requires all forms of wireless devices must have the highest levels of protection on them. This includes the following: wireless access points, laptops, tablets, mobile phones, and other mobile devices.

  NOTE: This directly impacts Maturity Level 3.

11) Recovery (RE):

There are two enhancements here:

- RE.L3-3.11.4: This requires that ***incremental backups*** must be made of all CUI, FCI, and other related datasets on a regular basis.

- RE.L3-3.11.5: This requires that ***full backups*** must be made of all CUI, FCI, and other related datasets on a regular basis.

NOTE: This directly impacts Maturity Level 3.

12) Risk Management (RM):

There are two updates here:

- RM.L3-3.12.7: This requires that risk assessments must be done on a regular basis, using the appropriate framework or methodology. This is in an effort to properly calculate the risk tolerance, and to deploy the appropriate controls.

- RM.L3-3.12.8: This stipulates that when the risk assessment has been conducted, the appropriate plan must be enforced to mitigate the calculated as much as possible to the lowest level that is possible.

NOTE: This directly impacts Maturity Level 3.

13) Security Assessment (CA):

There are two requirements:

- CA.L3-3.13.5: This stipulates the use of proper tools to continuously monitor any vulnerabilities that may exist in the IT and Network Infrastructures. This include such items as Penetration Testing and Vulnerability Scanning.

- CA.L3-3.13.6: This enforces the above, in that any vulnerabilities found must be remediated quickly.

NOTE: This directly impacts Maturity Level 3.

14) Situational Awareness (SA):

There are two updates, which are as follows:

- SA.L3-3.14.1: This requires that the proper feeds be used when it comes to collecting any intel about Cyber threats or variants.

- SA.L3-3.14.2: This stipulates that any intel received must be shared with the appropriate stakeholders.

NOTE: This directly impacts Maturity Level 3.

15) System and Communications Protection (SC):

This has four updates:

- SC.L3-3.15.9: This requires that the highest levels of encryption must be used when it comes to the management of network devices and other peripherals.

- SC.L3-3.15.10: On a theoretical basis all forms of network traffic must be denied, and only the approved data packets can move forward to their destinations.

- SC.L3-3.15.11: This mandates the total elimination of creating simultaneous network connections, and accessing resources in the external environment (unless it has been approved).

- SC.L3-3.15.12: The principles of Cryptography must be used when it comes to protecting the CUI datasets.

The NIST 800-171

One of the primary reasons why this whitepaper has provided an extensive overview into the all of the different versions of the CMMC (versions 1.0, 2.0, and 2.1) is the driving force behind all of them is the NIST SP (Special Publication) 800-171. It is a detailed document that has been set forth by the National Institutes of Standards and Technology, also known simply as "NIST). The technical definition of this extensive documents is as follows:

"NIST SP 800-171 is a NIST Special Publication that provides recommended requirements for protecting the confidentiality of controlled unclassified information (CUI). Defense contractors must implement the recommended requirements contained in NIST SP 800-171 to demonstrate their provision of adequate security to protect the covered defense information included in their defense contracts, as required by DFARS clause 252.204-7012."

(SOURCE: 7).

Just like the CMMC, the NIST SP 800-171 document has gone three distinct phases of updates, and the first version of it can be downloaded at this link:

http://cyberresources.solutions/NIST_800_171_WP/NIST.SP.800-171.pdf

The NIST SP 800-171 Version 2

The second version of the NIST 800-172 did not contain any significant changes from the original version. The only key difference in the second version is that it now required that Defense Contractors (and their associated subcontractors) had to hire an external third party (such as the C3PAO) in order to fully verify that the needed controls and safeguards were in place to protect both the FCI datasets and the CUI datasets.

The NIST SP 800-172 R2 can be downloaded at this link:

http://cyberresources.solutions/NIST_800_171_WP/NIST.SP.800-171_R2.pdf

The NIST SP 800-171 Version 3

The third version of the NIST 800-171 was released on May 10th, 2023. However, in this version, there are significant changes than when compared to the NIST 800-172 R2. One of the driving factors behind the NIST 800-172 R3 are the constant dynamics that are occurring in the Cybersecurity Threat Landscape at the present time.

The NIST SP 800-172 R3 can be downloaded at this link:

http://cyberresources.solutions/NIST_800_171_WP/NIST.SP.800-171_R3.pdf

The next section will detail the significant changes that have been made in the NIST SP 800-172 R3

The Changes

The updates in the NIST SP 800-172 R3 reflect the following, overall objectives:

- Further use of Cryptography.
- Stricter policies in terms of software usage.
- The use of Multifactor Authentication (also known as “MFA”).
- Having set of best practices and standards for mitigating Supply Chain Cyber Risks.
- Havning more documentation with regards to the location of the FCI datasets and the CUI datasets in their respective databases.

The Details

The details of the above are as follows:

1) The Use Of Cryptography:

   The NIST 800-172 reflects changes that address the advancements being made in Cryptography, which also includes the use of it to mitigate the risks that are posed by Quantum Computing

Threats, as well as the need for more robust Encryption based methods. Also, it allows for a certain amount of flexibility so that the defense contractors a much greater flexibility in implementing various types of Cryptographic controls, so as long as the FCI datasets and the CUI datasets are fully protected.

2) The Software Storage:

The NIST 800-171 R3 now has much stricter control over software usage, and the policies to do this have to be created and set forth, especially when it comes to the installation and maintenance of software packages that store and process the CUI datasets., especially those that process or store CUI. Also, thorough documentation must be kept in this regard.

3) The Use Of MFA:

The NIST 800-1712 no mandates that Multi-Factor Authentication (MFA) must be used in the entire IT/Network Infrastructure across all of the end user accounts. In this regard, at least three more differing authentication methods must be used.

4) The Supply Chain Cyber Risks:

The NIST 800-172 R3 now introduces stringent requirements for managing and mitigating these kinds of risks in the Cyber Supply Chain, especially when Third Party Vendors are used. Also, the defense contractor must have a thorough process of vetting before any subcontractors can be onboarded.

Other Areas Of Concern

Apart from the above, there are also other areas of concerns that the NIST 800-171 R3 also addresses which are:

- Security Policies
- Assessments Of Controls
- CUI and FCI Location

The details of these are reviewed in the next subsection.

The Details: Other Areas Of Concern

1) The Security Policies:

The NIST 800-172 R3 mandates that all Security Policies must be updated on a regular basis, not only to keep up with the evolving Cyber Threat Landscape, but to come also into compliance with the data privacy laws of the GDPR, CCPA, HIPAA, etc. Also, the key stakeholders must be involved in this process, from beginning to end.

2) The Assessments Of Controls:

The NIST 800-172 R3 greatly stresses the sheer importance of having independent based Risk Assessments be done not only to validate the effectiveness of security controls, but to make sure that any gaps or weaknesses are fully remediated. But there is some allowance so that the defense contractors (and their associated subcontractors have some flexibility as well.

3) The CUI and FCI Location:

The NIST 800-172 R3 emphasizes the importance of independent assessments to validate the effectiveness of security controls, especially as they relate to the FCI datasets and the CUI datasets. Also a certain degree of customization is also allowed so that the defense contractor (and their associated subcontractors) can create more robust and effective environments.

Much more specific detail on the above updates can be found at this link:

https://redspin.com/white-papers/exposed-the-hidden-changes-in-nist-sp-800-171-rev-3/

Other Updates

Other noteworthy updates have also been made to the NIST SP 800-171 R3, and they are as follows:

- Increasing the level of clarity of the content in the document for the end user.

- Separating out the distinction of what "Basic Security" and "Derived Security" is.

  *Basic Security can be technically defined as follows:

  "The set of minimum-security controls defined for a low-impact, moderate-impact, or high-impact information system."

  (SOURCE: 8).

  Derived Security can be technically defined as follows:

  "Derived requirements list specific controls or processes that implement those goals."

  (SOURCE: 9).

- The Implementation of "Organization Defined Parameters", also known as "ODPs" for short. This is technically defined as follows:

  "Organization-defined parameters are used in the SP 800-53 controls to provide flexibility to federal agencies in tailoring controls to support specific organizational missions or business functions and to manage risk."

  (SOURCE: 10).

  In other words, each defense contractor (and their associated subcontractor) can deploy the needed controls that is unique and specific to their particular environment. But this is on the condition that these controls will offer maximum security to the FCI datasets and the CUI datasets.

- Three new Security Requirements were also implemented, which are as follows:

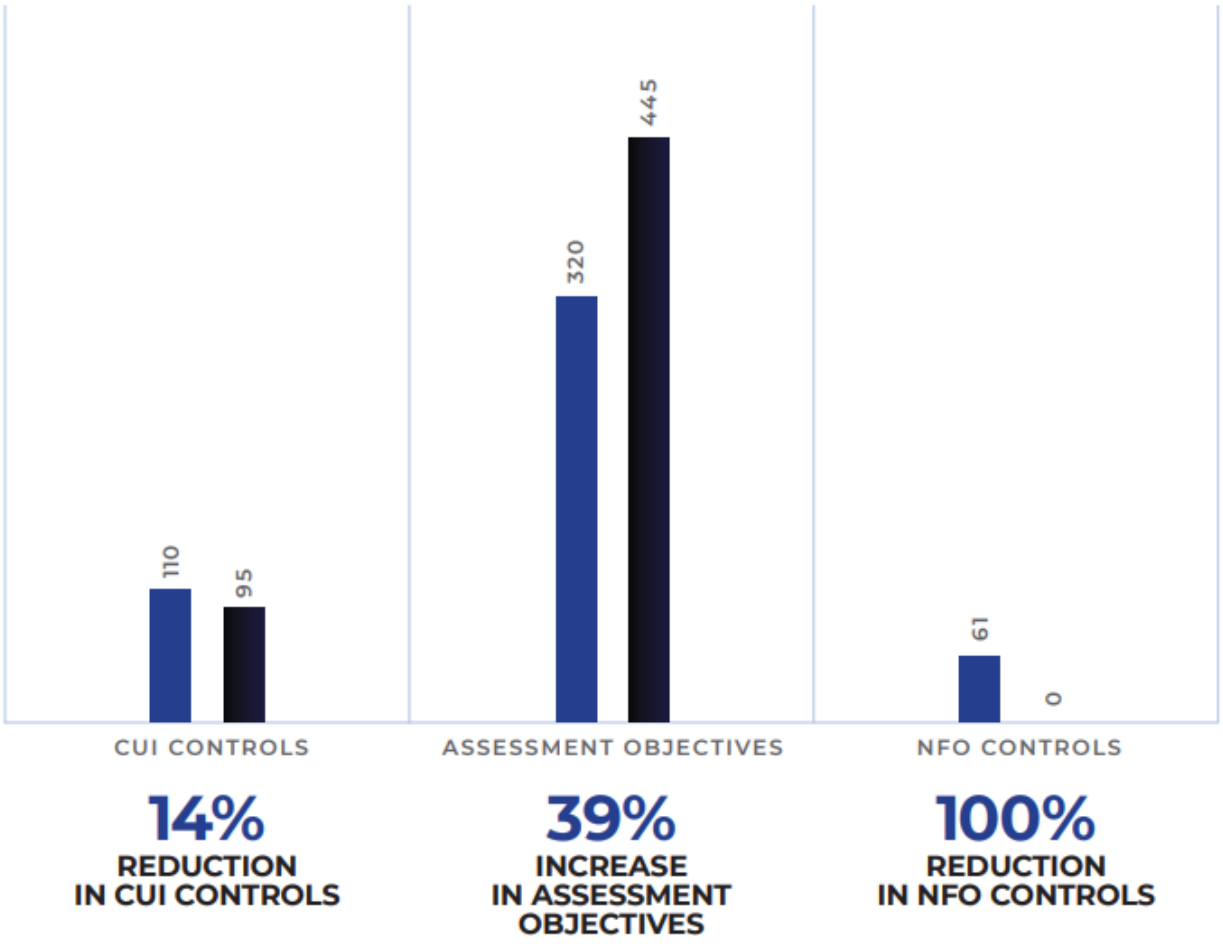
  *Planning (also known as "P").

*Systems and Service Acquisition (also known as “SA”).

*Supply Chain Risk Management (also known as “SR”).

- The NIST completely eradicated the mapping of the NIST SP 800-53 security controls to the ISO 27001 security controls. In its place, the NIST SP 800-171, R3, will be mapped to the NIST SP 800-53 security controls

Finally, an illustration of the key differences between the NIST SP 800-171 R2 and the NIST SP 800-171 R3 are illustrated in the diagram below:



Number of Changes to Security Requirements

Type of Change	Change Description	Number
No significant change	Editorial changes to requirement; no change in outcome.	18
Significant Change	Additional detail in requirement, including more comprehensive detail on and foundational tasks for achieving the outcome of the requirement.	49
Minor Change	Editorial changes. Limited changes in level of detail and outcome of requirement.	18
New Requirement	Newly added requirement in IPD SP 800-171 Rev 3.	26
Withdrawn Requirement	Requirement withdrawn.	27
New Organization-defined Parameter (ODP)	*Note: New ODPs can apply to all change types with the exception of withdrawn requirements. Each requirement includes one or more new ODPs.*	53
	Total Number of Security Requirements in Draft SP 800-171 Rev 3	**138**

(SOURCE FOR BOTH DIAGRAMS: 11).

Conclusions

In the NIST SP 800-171 R3, there are certain key terminologies that are used, which are as follows:

1) No Significant Change:

   This means that there are “Editorial changes to requirement; no change in outcome."

2) Significant Change:

   This means that there is “Additional detail in requirement, including more comprehensive detail on and foundational tasks for achieving the outcome of the requirement.”

3) Minor Change:

   This means that there are “Editorial changes. Limited changes in level of detail and outcome of requirement”.

4) Withdrawn Requirement:

   This means that the Requirement [has been] withdrawn.”

5) New Organization-defined Parameter (“ODP”):

   This means that “New ODP's can apply to all change types with the exception of withdrawn requirements. Each Requirements includes one or more new ODPs.”

   (SOURCE: 12).

If you have any questions as to what is covered in this whitepaper, or need help in deploying the NIST SP 800-171 R3 for your business, please contact us today.

Sources

1) https://www.dodcui.mil/Portals/109/Documents/Info%20Paper%20on%20DoD%20CUI%20Program.pdf?ver=De5b7M5cuVTQtuo11DId5A%3D%3D
2) https://www.cybernc.us/fci-cui/#:~:text=Federal%20Contract%20Information%20(FCI)%20and,deliver%20a%20product%20or%20service.
3) https://soundwayconsulting.com/fci-and-cui-basics-for-cmmc-compliance/ https://www.nextlabs.com/cybersecurity-maturity-model-certification-cmmc-requirements-explained/
4) https://www.crowdstrike.com/cybersecurity-101/advanced-persistent-threat-apt/
5) https://www.cuicktrac.com/cmmc-compliance/cmmc-levels/
6) https://techcommunity.microsoft.com/t5/public-sector-blog/the-basics-of-cmmc-2-0-and-preparation-recommendations/ba-p/3057526
7) https://www.cimcor.com/blog/nist-800-171-revision-3-key-changes-and-compliance-requirements
8) https://csrc.nist.gov/glossary/term/security_control_baseline
9) https://www.encomputers.com/2023/01/dfars-and-nist-800-171-ultimate-guide/
10) https://insidecybersecurity.com/daily-news/final-update-nist-cui-publications-features-organization-defined-parameters-agencies#:~:text=%E2%80%9COrganization%2Ddefined%20parameters%20are%20used,%2D171%20and%20800%2D171A.
11) https://www.cimcor.com/blog/nist-800-171-revision-3-key-changes-and-compliance-requirements
12) https://www.sharetru.com/blog/nist-800-171-revision-3-what-you-need-to-know