SOLUTION NOTE

ADDRESSING THE CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC) 2.0 FRAMEWORK USING FOUNDATIONAL SECURITY

OVERVIEW

The US Department of Defense (DoD) released the Cybersecurity Maturity Model Certification (CMMC) version 1.0 on January 31, 2020.

In late 2021, approved program changes, designated as CMMC 2.0, defined clarifications and additional protections to better protect sensitive unclassified information used by the Department of Defense (DOD) in dealing with contractors and subcontractors. CMMC 2.0 was initially targeted to go into full effect by May 2023 and show up in contracts by July 2023.

The CMMC is the Department of Defense's (DoD) regulation designed to ensure that the Controlled Unclassified Information (CUI) resident in the Defense Industrial Base networks and systems are adequately protected by security controls and related processes. The CMMC 2.0 program is designed to enforce the protection of sensitive unclassified information that is shared by the Department with its contractors and subcontractors. The CMMC 2.0 program provides the Department increased assurance that contractors and subcontractors are meeting the cybersecurity requirements that apply to various DOD programs and the systems used to process controlled unclassified information.

CMMC 2.0 is a big change and improvement from CMMC 1.0. Most of the requirements in CMMC 2.0 are not unique to the CMMC. These requirements are published in other standards and frameworks such as NIST CSF, NIST 800-171, and NIST 800-172 and then cited for inclusion in the CMMC specifications. The CMMC is in response to the multitude of significant data breaches that have impacted defense information on contractors' information systems and networks. All DoD contractors and most, if not all, of the defense supply chain need to step up to CMMC certifications.

Foundational security using DNS, DHCP, IP Address Management (IPAM) and DNS security can be a vital part of providing the increased cyber resilience your organization will need to meet your organization's CMMC level certification requirements.

NEW CHANGES IN CMMC 2.0

CMMC 2.0 implements various changes to CMMC 1.0 which include, but are not limited to:

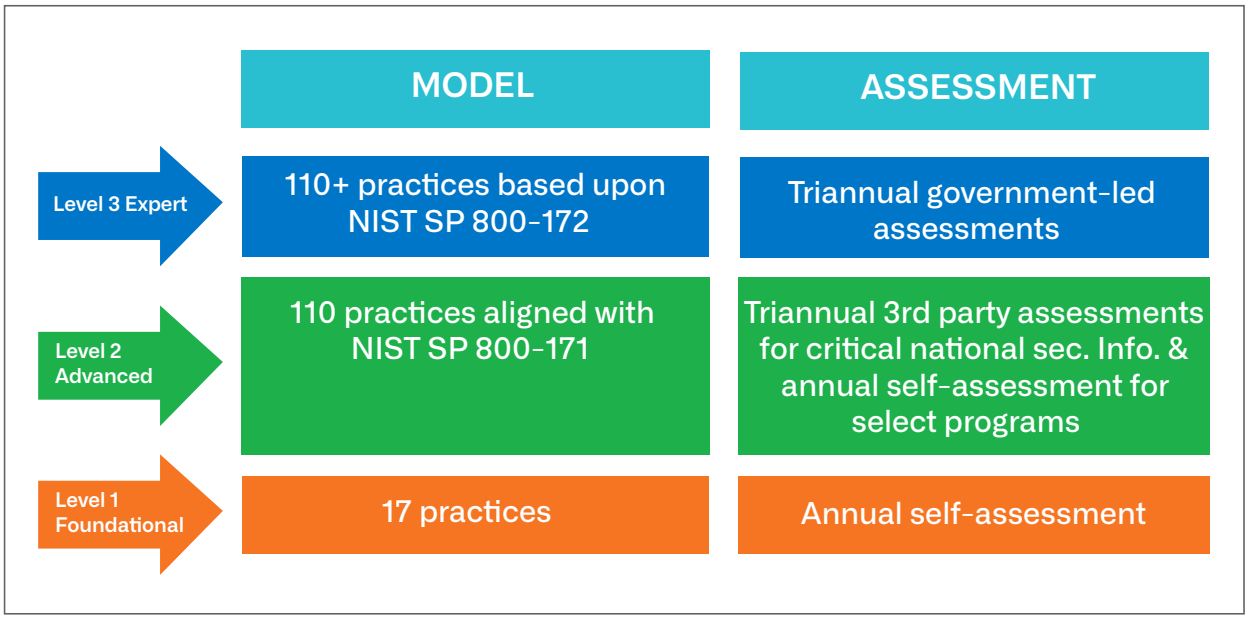
- A reduction in the CMMC levels from five to three. The new CMMC 2.0 levels are Foundational (Level 1), Advanced (Level 2), and Expert (Level 3). This greatly simplifies the CMMC specification and reduces the administrative burden across DOD contractors.
- A reduction of 20 security requirements as now CMMC fits completely within the security control framework defined in NIST SP 800-171.

- CMMC 2.0 allows for the use of Plans of Action and Milestones (POAMs). A POAM defines the remediation steps a U.S. defense industrial base (DIB) company will take to correct deficiencies identified during a security control assessment. The POAM should identify the tasks, priorities and resources required to make the plan work and remediate the deficiencies.
- Certification waivers for CMMC 2.0 will be very few and approved in highly limited circumstances.

THE CMMC 2.0 FRAMEWORK

The CMMC 2.0 associates cybersecurity best practices and processes to three key maturity levels. These include a fundamental level of cyber defense capability at Level 1 and the most advanced and capable cyber defense capabilities required at Level 3.

CMMC MODEL 2.0 LEVELS AND DESCRIPTIONS



CMMC LEVEL 1 - FOUNDATIONAL

This level applies to organizations that must protect Federal contract information (FCI). This is very similar to the CMMC 1.0 Level 1. The controls which are used for Level 1 are found in FAR 52.204-21. This FAR covers the basic safeguarding required for Covered Contractor Information (CCI) and protecting FCI. These basic controls help protect the covered CCI systems and restrict access to authenticated and authorized users.

CMMC LEVEL 2 - ADVANCED

This level applies to organizations that are working with CUI. This is most similar to the old CMMC Level 3. CMMC 2.0 Level 2 completely maps to NIST SP 800-171 and eliminates other processes and practices that were unique to CMMC 1.0. This mapping includes 14 levels and 110 security controls delineated by NIST for the protection of CIU. The result is a complete alignment between CMMC 2.0 Level 2 and NIST SP 800-171.

CMMC LEVEL 3 - EXPERT

This level is designed to reduce the risk and impact of advanced persistent threats and to protect CIU in the most important DOD programs. CMMC 2.0 Level 3 is similar to the old CMMC 1.0 Level 5 but instead relies on requirements documented in NIST SP 800-171 and some of the controls in NIST SP 800-172.

FOUNDATIONAL SECURITY TO HELP ADDRESS CMMC REQUIREMENTS

Most defense contractors have a mix of on-premise and cloud-based resources. This has been further complicated by the recent move to increased remote access and the use of personal devices for network access. The classic perimeter defense is gone and the shift to technologies that support architectures such as Zero Trust and SASE have become compelling. DNS security provides a powerful control point that works equally well for any mix of distributed resources and users.

BloxOne® Threat Defense from Infoblox uses DNS as a security control point to provide foundational protection wherever the users and data reside, in data centers, HQ, branch, in the cloud and IoT. BloxOne Threat Defense brings critical support for security orchestration, automation and response (SOAR) solutions, reduces the time for your security operations teams to investigate and remediate cyberthreats, and helps optimize the performance of the entire security ecosystem. This, in turn, can also reduce the total cost of enterprise threat defense and help achieve CMMC certification levels.

BloxOne Threat Defense enables you to turn the core network services you rely on to run your enterprise into valuable security assets. These services, which include DNS, DHCP and IP address management (DDI), play a central role in all IP-based communications. With Infoblox, they become the foundational common denominator that enables your entire security stack to work better together to detect and anticipate threats sooner and stop them faster.

USING NIST CSF TO HELP MANAGE CYBERSECURITY RISK

The NIST Cybersecurity Framework (CSF) is a framework that can help organizations manage cybersecurity risks. CSF provides a standard language to help organizations identify, prioritize, and address cybersecurity risks. NIST CSF provides a high-level risk-based approach to managing cybersecurity risk. NIST CSF does not include all of the detailed and very specific security controls that an organization must meet to fully align and comply with NIST SP 800-171 and NIST SP 800-172.

To meet the requirements of NIST SP 800-171 and SP 800-172, an organization will need to implement the specific security controls and requirements outlined in these publications. The NIST CSF can be used to help an organization understand the cybersecurity risks to its systems and organization, and to identify and prioritize the controls that are needed to reduce those risks.

In order to address the requirements of NIST SP 800-171 and NIST SP 800-172 organizations can do the following:

- Identify the CUI that must be protected and the associated systems and personnel that require access to it.
- Utilize NIST CSF to identify and best understand the cybersecurity risks to the CUI.
- Use the correct controls from NIST SP 800-171 and SP 800-172 to protect the CUI and reduce the identified cybersecurity risks.
- Assess the effectiveness of the implemented controls over time. Validate that these controls are meeting the requirements of NIST SP 800-171 and SP 800-172 and therefore reducing cybersecurity risks.
- Continuously assess and improve the cybersecurity posture of the organization by frequently updating the controls. It is important to identify and address new cybersecurity risks.

Organizations can use the NIST CSF to effectively help meet the requirements of NIST SP 800-171 and SP 800-172 and protect CUI in nonfederal information systems and organizations.

INFOBLOX CAPABILITIES FOR MEETING CMMC CONTROLS

The following table shows how Infoblox DNS, DHCP, IPAM, BloxOne and NetMRI solutions can help support specific CMMC controls. This table maps DDI solutions to core functions/categories in NIST CSF.

NIST Core Function	NIST Core Category	Category Identifier	DDI Solution
Identify	Asseet Management	ID.AM	IPAM used in the following capacity: As the single source of truth for network assets. For automated device discovery Integration with vulnerability scanners for scanning when a device joins the network
Identify	Risk Assessment	ID.RA	Network automation tool for automated discovery and scanning of all devices on the network to identify misconfigured devices. Integration with vulnerability Management (VM) tools when something anomalous is detected
Protect	Access Control	PR.RC	Integration with Network Access Control solutions to isolate/quarantine compromised devices and prevent them from joining the network.
Detect	Anomalies and Events	DE.AE	Detect DNS tunneling and exfiltration of sensitive data.
Detect	Security Continuous Monitoring	DE.CM	Ability to forward DNS requests and DHCP lease logs to 3rd party SIEMs and other SecOps tools for continuous monitoring
Detect	Detection Processes	DE.DP	DNS Firewalling & Malware Detection using aggregated threat intelligence Detect volumetric DNS attacks DGA detection, data exfiltration, Fast flux, file-less malware using ML based analytics
Respond	Mitigation	RS.MI	DNS Firewalling and automatic incident response via ecosystem integrations using STIX, REST APIs. Rapid mitigation with ecosystem partners (e.g. NAC, Endpoint Detection and Response)
Respond	Analysis	RS.AN	DDI data and treat intel context, automated threat investigation using aggregated search tool

Corporate Headquarters
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com

Version: 20230918v1