ignyte™
ASSURANCE PLATFORM

Understanding the CMMC Framework for Your Business

Contents

Understanding CMMC Compliance

Cybersecurity is foundational to service and product procurement and organizations should not trade it along with cost, schedule, and performance. In any supply chain, there is a need for players to protect controlled unclassified information (CUI). Executive Order 13556 established CUI as an umbrella term for unclassified information that requires protection.

Taking this into account, various bodies, including the Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S)), DoD stakeholders, University Affiliated Research Centers (UARCs), Federally Funded Research and Development Centers (FFRDC), and industry have collaborated to develop the Cybersecurity Maturity Model Certification (CMMC) that was released to the public on January 31, 2020.

CMMC is a combination of an array of cybersecurity standards and best practices mapped across multiple maturity levels ranging from cyber hygiene to advanced. In this case, each CMMC level comprises of processes and controls that enable organizations to minimize risk against a set of cyber threats. With different levels, it becomes affordable and straightforward for small businesses to implement CMMC. On the other hand, third-parties leverage the model to conduct audits and inform risk in organizations.

The CMMC effort is built upon existing DFARS 252.201-7012 that is based on trust by adding a verification aspect with respect to cybersecurity requirements. Stakeholders integrate CMMC into the Defense Federal Acquisition Regulation Supplement (DFARS) and apply it as part of stipulations in the procurement process and contract award. The DoD specifies the required CMMC level in requests for information (RFIs) and requests for proposals (RFPs).

IMPORTANCE OF CMMC COMPLIANCE

The loss of CUI from the Defense Industrial Base (DIB) poses a risk to the national economic security and in a broad sense the national security. In effect, DIB should devise measures to protect CUI and reduce the risk.

According to the Council of Economic Advisors, malicious cyber activity costs the U.S. economy between $57 billion and $ 109 billion in 2016. In the same vein, the Center for Strategic and International Studies (CSIS), in partnership with McAfee, estimate that the world might lose more than $600 billion or 1% of the global economy to cybercrime annually. Common cybersecurity threats that encourage the development and adoption of CMMC include:

Overseas Threats
A sophisticated threat originating from overseas and setting a stage for conflict

Cyberattacks
Widespread cyberattacks that occur in the U.S.

Critical Infrastructure Threats
Hackers targeting critical infrastructure and community lifelines

Business continuity and resilience
Impacts of cyberattacks on continuity and business resilience

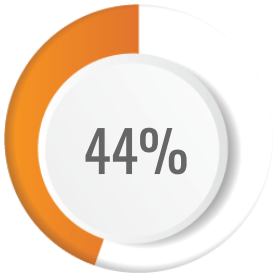
National Emergency
Cyberattacks causes national security emergency

Download the free Ignyte's CMMC DFARs Compliance Toolkit

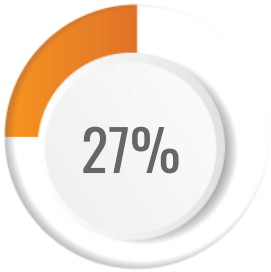
In the current cyberspace circumstances, an organization should implement new strategies and measures to combat the soaring cybercrime impacts. CMMC is a promising model that encompasses several maturity levels to help organizations to introduce and maintain cyber hygiene and progress to advanced cybersecurity postures.

DOD intends to migrate and deploy the new CMMC framework to assess and improve the security posture of the Defense Industrial Base (DIB). In this case, CMMC ensures that appropriate security practices and processes are in place to mitigate cyberattacks and protect CUI residing industry partners' networks.

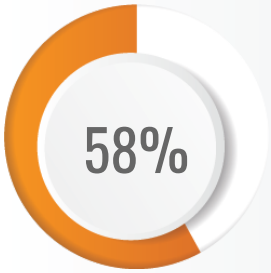
Indeed, the lack of CMMC certification disqualifies your business from participating in contracts that require it. Besides, apart from possibly becoming a federal-wide framework, the cybersecurity field might consider CMMC as part of the international standards, considering that stakeholders developed it in line with the U.S. allies' cybersecurity standards. Katie Arrington, the Pentagon's CISO for acquisition and sustainment, said that CMMC "will become a federal standard for the whole government," and the cybersecurity field might amplify it beyond defense acquisition purposes. According to the CISO, "the CMMC will become the basis for global cybersecurity standard."



respondents said they were still working to meet the NIST 800-171 requirements



respondents admitted they are unprepared for a cyber breach.



of contractors surveyed were unfamiliar with the initiative, according to the Tier 1 Cyber study.

Survey conducted by National Defense Magazine.

Background of Maturity Models

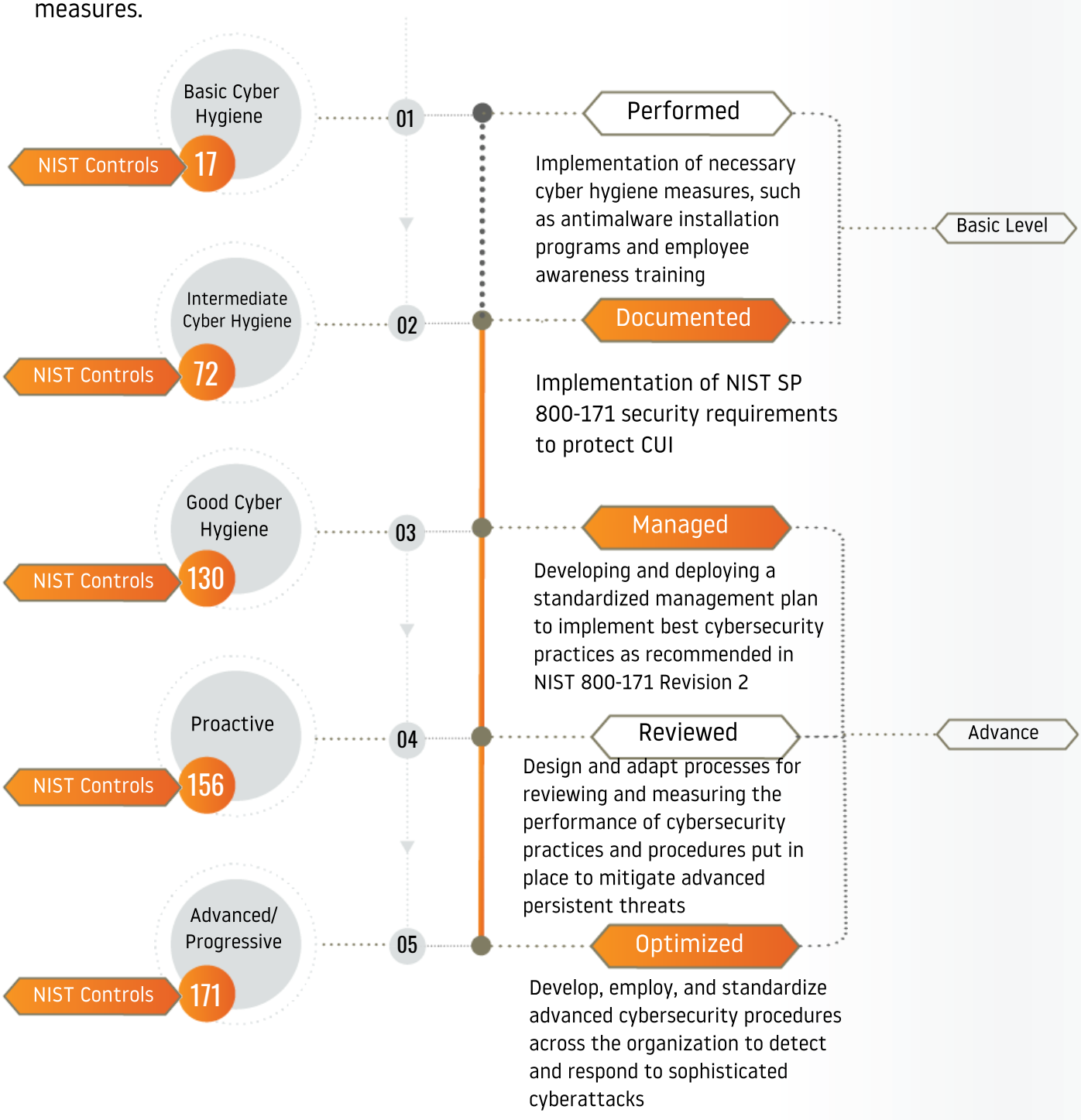
CMMC certification certifies that DOD contractors have put in place proper security controls and measures to protect valuable information like Controlled Unclassified Information (CUI). The framework is an integration of best practices from top cybersecurity standards, such as the NIST SP 800-171, NIST SP 800-53, ISO 27001, ISO 27032, AIA NAS9933, among others. Initially, the popular NIST 800-171 allowed organizations to self-assess and report their compliance, which organizations could flaw, leading to numerous successful cyberattacks. In this effect, CMMC strictly requires organizations to coordinate with accredited and independent third-party organizations to address the shortcomings familiar with existing standards.

Various Features of CMMC

CMMC is a combination of a set of levels, processes, practices, domains, and capabilities.

The Five Levels of Processes to Measure Maturity

CMMC contains five levels that range from basic cyber hygiene controls to advanced measures.



The CMMC Domains

CMMC model features 17 domains inspired by the popular cybersecurity requirements families like the NIST SP 800-171 and the Federal Information Processing Standards (FIPS) publication 200. The domains include:

- Access control (A.C.)
- Asset management (AM)
- Audit and accountability (A.U.)
- Awareness and training (AT)
- Configuration management (CM)
- Identification and authentication (I.A.)
- Incident response (I.R.)
- Maintenance (M.A.)
- Media protection (M.P.)
- Personnel security (P.S.)
- Physical protection (P.E.)
- Recovery (RE)
- Risk management (R.M.)
- Security assessment (C.A.)
- Situational awareness (S.A.)
- System and communication protection (S.C.)
- System and information integrity (S.I.)

The Specific CMMC Capabilities

Each domain of the CMMC model has a set of capabilities. In total, the 17 domains have 43 capabilities ash shown in the table below:

Domain	Capability
Access control (A.C.)	● Establish system access requirements ● Internal system access management ● Remote system access management ● Data access limitation to authorized processes and users
Asset management (AM)	● Identify and document information assets

Audit and accountability (A.U.)	• Establish audit requirements • Conduct auditing • Identify and protect audit information • Review and manage audit logs
Awareness and training (AT)	• Conduct security awareness activities • Conduct awareness training
Configuration management (CM)	• Set configuration baselines • Perform configuration and change management
Identification & Authentication (I.A.)	• Grant access to authenticated entities
Audit and accountability (A.U.)	• ncident response planning • Detect and report events • Develop and deploy a response to a detect incident • Conduct post-incident analysis • Evaluate incident response
Maintenance (M.A.)	• Manage maintenance
Media protection (M.P.)	• Media identification and marking • Media control and protection • Media sanitization • Media protection during transfer
Personnel security (P.S.)	• Screening personnel • Safeguarding CUI during personnel actions
Physical protection (P.E.)	• Limiting physical access
Recovery (RE)	• Managing backups
Risk management (R.M.)	• Risk identification and evaluation • Risk management
Audit and accountability (A.U.)	• Develop and maintain a system security plan • Define and manage controls • Conduct code reviews
Situational awareness (S.A.)	• Managing backups
Systems and communication protection (S.C.)	• Establish security requirements for systems and communications • Manage and protect communications at system boundaries
System and information integrity (S.I.)	• Detect and handle information system flaws • Identify malicious content • Perform network and system monitoring • Deploy advanced email protections

Becoming CMMC Certified

The CMMC Accreditation Body (A.B.) accredits CMMC Third-Party Assessment Organizations (C3PAOs) and individual assessors. The Office of the Under Secretary of Defense for Acquisition and Sustainment directs that "the CMMC AB will provide the requisite information and updates on its website."

Besides, the body will establish a CMMC market place that will feature a list of approved C3PAOs as well as other relevant information. This approach makes it easy for DIB industry partners to select an approved C3PAOs and schedule a CMMC assessment for specified levels.

The results of the CMMC assessment conducted by C3PAOs will not be publicized. Besides, information on specific certification level will not be revealed. However, interested parties can access information about your organization's CMMC certification publicly. Only the DOD will have access to all DIB companies' assessment results and certification levels.

Covered Entities

CMMC Accreditation Body (A.B.) reveals that there are more than 300,000 vendors in the DoD supply chain. These industry partners require CMMC assessment and certification. They include:

- Prime contractors
- Subcontractors
- Any other organization that sells or services the Department of Defense

CMMC Re-Assessment Conditions

It is essential for DIB industry partners to note that the CMMC certificate is valid for three years, after which they require a re-assessment.

In case of a cyberattack on a CMMC certified company, the DIP will not automatically lose the certification. Instead, the DoD program manager may direct the victim to conduct a re-assessment.

Read Now↦ How Much Will CMMC Certification Cost My Business?

How Ignyte Assurance Platform™ can Help

Ignyte Assurance team offers a robust and straightforward roadmap and automation for your CMMC framework certification journey. We assess your company's network, the desired CMMC maturity level, and other market forces for the framework's certification. Ignyte provides solutions that automate and take additional tasks to ease your company the burden of the CMMC compliance process.

Our team of professionals has a history of expertise in providing proper controls and documentation needed for your compliance needs. Ignyte allows businesses to check on their compliance status from an elaborate dashboard in a single global view.

ABOUT IGNYTE ASSURANCE PLATFORM™

Ignyte Assurance Platform™ is a leader in collaborative security and integrated GRC solutions for global corporations. For corporate risk and compliance officers who depend heavily on the protection of their resources, Ignyte is the ultimate translation engine for simplifying compliance across regulations, standards and guidelines. The Ignyte platform is used by leading corporations in diverse industries; such as, Healthcare, Defense, and Technology. Ignyte is headquartered in Miamisburg, Ohio and can be reached at www.ignyteplatform.com. PH: 1.833.IGNYTE1 or (937) 789-4216

Put us to the Test

Give us a call to setup a demo today at https://ignyteplatform.com/request-a-demo/

REQUEST A DEMO