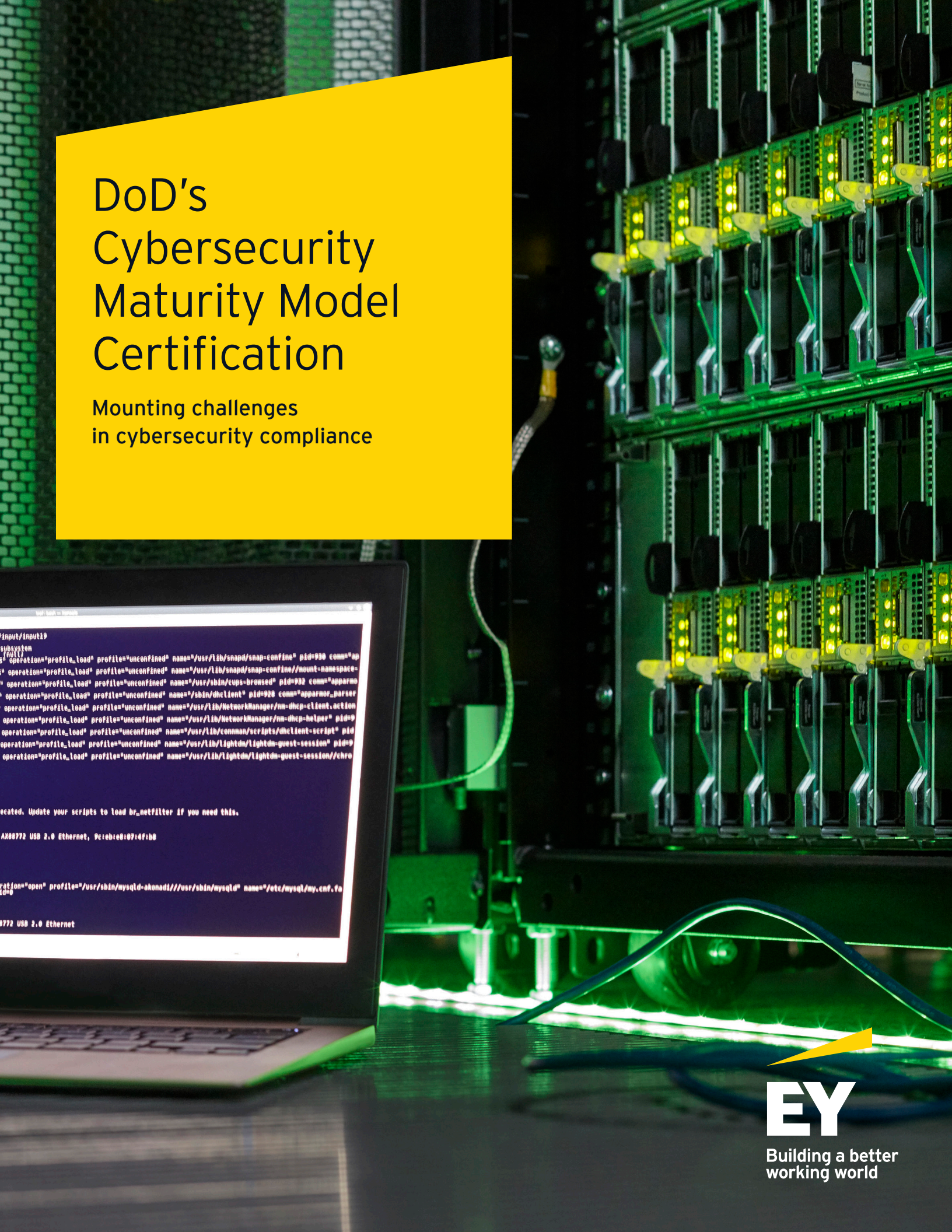
# DoD's Cybersecurity Maturity Model Certification

## Mounting challenges in cybersecurity compliance



Building a better working world

> We are seeing clients who are eager to comply with the DoD's requirements, yet are not receiving clear and consistent communication to allow for adequate planning and investment. Our Government Contract Services team provides objective guidance to help our clients make informed decisions.

Andrew Artz
Principal,
Government Contract Services

What a difference two years can make. In the summer of 2017, the Department of Defense (DoD) was preparing industry outreach events to communicate compliance expectations for Defense Federal Acquisition Regulation Supplement (DFARS) Clause 252.204-7012. This focused around requirements for contractors to draft a system security plan describing National Institute of Standards and Technology Special Publication 800-171 control implementation status and plans of actions and milestones. DoD representatives had clearly communicated that a third-party certification would not be required to attest to compliance nor would one be accepted. A self-attestation, it was said, would be sufficient.

## Confusion on all sides

Looking to where things stand today, confusion between DoD program teams and oversight roles regarding what is expected from contractors has contributed to an environment of uncertainty causing contractors to make costly assumptions, both in terms of resources and risk. Increasingly, senior DoD leadership is communicating that the requirements of the DFARS rule do not go far enough to provide the level of security required to protect sensitive defense information processed, stored or transmitted on contractor systems. On the other hand, contractors of all sizes are expressing difficulty with various requirements being imposed; whether it's the lack of markings on government data, unclear guidance around what constitutes covered defense information (CDI) under a contract, the technical implementation of certain controls given the organizational constraints of many dual-customer (defense and commercial) contractors, the challenges of monitoring and assessing their supply chains against ever-changing DoD expectations or the lack of assurance from the DoD that their efforts are sufficient to achieve compliance.

## A change in approach

Building frustration with current evaluation and compliance effectiveness is giving way to a reconsideration of the approach initially established by the DoD. A new cybersecurity certification for DoD contractors named the Cybersecurity Maturity Model Certification, or CMMC, is being developed. It is envisioned that to receive the certification, a contractor will undergo a third-party audit from an accredited assessor adhering to federally developed standards. The intention is that the certification will provide assurance to the DoD and prime contractors that certified organizations can be trusted to utilize CDI, allowing for the validation of cybersecurity capabilities across the entire defense industrial base. Incorporated in this envisioned CMMC, is a scoring program whereby contractor cyber capabilities are measured against cybersecurity standards. The higher a contractor's score, the more eligible they will be to bid on and be awarded contracts.

## Compliance in limbo

Given the 180-degree change in the DoD's approach — from reliance on contractor self-assessment to a third-party certification model — contractors are left wondering how their efforts to comply with the DFARS requirements will be evaluated going forward. Many are now anticipating that the combination of the release of new standards and new evaluation criteria and methods will result in prior efforts being rendered obsolete. The continuous nature of cybersecurity always meant that ongoing assessments would be required and that compliance would continue to be a moving target, but the continually changing approaches and standards of the DoD have left much of the industry in a position where compliance is seen as a moving target as well. While a certification model would establish consistent standards and a certification from an accredited assessor would remove judgments by the contractor from the equation, it raises new concerns, such as the following:

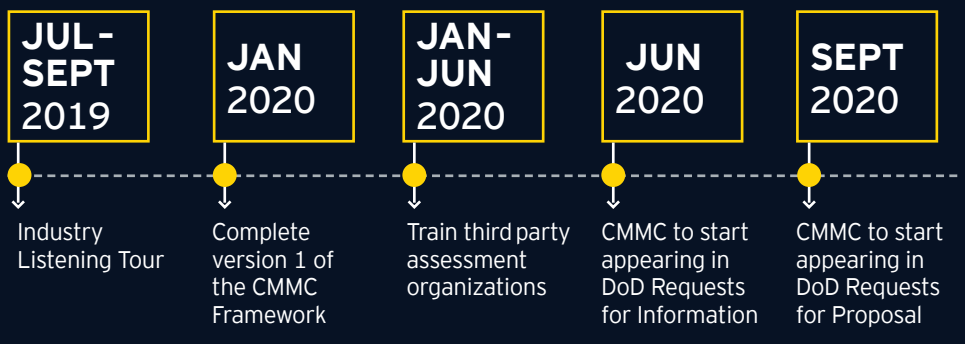
- Lack of industry involvement in standards development
- Lack of information on vetting and qualification of third-party assessors
- Lack of clarity on a contractor's recourse in the case of disputed assessment results
- Unclear how existing DFARS clause and Contractor Purchasing System Review requirements will be impacted by the CMMC audits

Through all of this, one thing that has not changed is the DoD's increasing focus on the cybersecurity risks facing the defense industrial base. With the shift away from self-assessment and attestation, contractors would be well-advised to seek an objective assessment of their capabilities against industry-leading practices and regulatory requirements in preparation for the newly envisioned federal cyber oversight environment.

## The EY US Government Contract Services Differentiator

EY Government Contract Services professionals have worked with government contractors across numerous industries to evaluate their development and use of CDI, conduct system assessments, draft system security plans and provide objective evaluations of DFARS compliance. Our professionals possess multidisciplinary skills and experience in interpreting government contracting regulations, corporate governance, internal control design and conducting cybersecurity evaluations. Our unique perspective provides our clients with insights to develop comprehensive approaches to compliance with federal cybersecurity requirements.

**An eye to the future:** Projected timeline of the CMMC program rollout




## Contacts


**Bob Malyska**
*Americas Government Contracts Leader*
Ernst & Young LLP
+1 214 969 8628
robert.malyska@ey.com

**Andrew Artz**
*Principal*
Ernst & Young LLP
+1 703 747 1480
andrew.artz@ey.com

**Michael Tomaselli**
*Senior Manager*
Ernst & Young LLP
+1 703 747 1070
michael.tomaselli@ey.com

**Courtney Black**
*Senior Manager*
Ernst & Young LLP
+1 214 969 9604
courtney.black@ey.com

**Edward Morley**
*Senior Manager*
Ernst & Young LLP
+1 617 585 0425
edward.morley@ey.com

**Amy Benedict**
*Senior Manager*
Ernst & Young LLP
+1 312 879 3248
amy.benedict@ey.com


**EY** | Assurance | Tax | Transactions | Advisory

**About EY**
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. For more information about our organization, please visit ey.com.

**About EY Forensic & Integrity Services**
Dealing with complex issues of fraud, regulatory compliance and business disputes can detract from efforts to succeed. Better management of fraud risk and compliance exposure is a critical business priority – no matter the size or industry sector. With approximately 4,500 forensic professionals around the world, we will assemble the right multidisciplinary and culturally aligned team to work with you and your legal advisors. We work to give you the benefit of our broad sector experience, our deep subject-matter knowledge and the latest insights from our work worldwide.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.



SCORE no. 06747-191US
1907-3227981
ED None




**ey.com/forensics**