IMMEDIATE RELEASE

# Strategic Direction for Cybersecurity Maturity Model Certification (CMMC) Program

NOV. 4, 2021

Today, the Department of Defense announced the strategic direction of the Cybersecurity Maturity Model Certification (CMMC) program, marking the completion of an internal program assessment led by senior leaders across the Department.

The enhanced “CMMC 2.0” program maintains the program’s original goal of safeguarding sensitive information, while:

- Simplifying the CMMC standard and providing additional clarity on cybersecurity regulatory, policy, and contracting requirements;
- Focusing the most advanced cybersecurity standards and third-party assessment requirements on companies supporting the highest priority programs; and
- Increasing Department oversight of professional and ethical standards in the assessment ecosystem.

Together, these enhancements:

- Ensure accountability for companies to implement cybersecurity standards while minimizing barriers to compliance with DoD requirements;
- Instill a collaborative culture of cybersecurity and cyber resilience; and
- Enhance public trust in the CMMC ecosystem, while increasing overall ease of execution.

“CMMC 2.0 will dramatically strengthen the cybersecurity of the defense industrial base,” said Jesse Salazar, Deputy Assistant Secretary of Defense for Industrial Policy. “By establishing a more collaborative relationship with industry, these updates will support businesses in adopting the practices they need to thwart cyber threats while minimizing barriers to compliance with DoD requirements.”

The CMMC program includes cyber protection standards for companies in the defense industrial base (DIB). By incorporating cybersecurity standards into acquisition programs, CMMC provides the Department assurance that contractors and subcontractors are meeting DoD's cybersecurity requirements.

The DIB is the target of increasingly frequent and complex cyberattacks by adversaries and non-state actors. Dynamically enhancing DIB cybersecurity to meet these evolving threats, and safeguarding the information that supports and enables our warfighters, is a top priority for the Department. CMMC is a key component of the Department's expansive DIB cybersecurity effort.

The internal assessment of CMMC was co-chaired by: Mieke Eoyang, Deputy Assistant Secretary of Defense for Cyber Policy; David Frederick, Executive Director of U.S. Cyber Command; David McKeown, Deputy Chief Information Officer for Cybersecurity; and Jesse Salazar, Deputy Assistant Secretary of Defense for Industrial Policy; and included senior leaders from 18 components across the Department.

For more on the changes, visit https://www.acq.osd.mil/cmmc/index.html.