AUBURN UNIVERSITY
Office of the Vice President for Research
and Economic Development

# Cybersecurity Maturity Model Certification (CMMC)
# National Security Presidential Memorandum (NSPM-33)

UIDP FACE 2 FACE
MARCH 30, 2022

# CMMC 2.0

CMMC controls (NIST 800-171) required to bid on Government contracts; a top priority to enhance the Defense Industrial Base and meet increasing and evolving threats

CMMC 2.0 simplifies CMMC standards with additional clarity on regulatory, policy, and contracting requirements

Increasing DoD oversight to ensure technical and ethical standards are meet

Lead federal agency: DoD

# CMMC 2.0

Tiered model to meet advanced level of cybersecurity standards that align with type/sensitivity of CUI

Level 1 – foundational (maps against CMMC 1.0 level-1); basic cybersecurity hygiene; annual self-assessment

Level 2 – advanced (maps against CMMC 1.0 level-3); 110 controls aligned with NIST 800-171; triannual third-party assessments for critical national security information: annual self-assessment for select programs

Level 3 – expert (maps against CMMC 1.0 level-5); 110+ controls aligned with NIST 800-171; assessments led by government officials instead of third-party organizations

# CMMC 2.0

CMMC 2.0 includes “limited waiver” process to exclude CMMC requirements for select mission critical initiatives

DoD anticipates rulemaking to take 9-24 months…contractors are not required to comply with CMMC 2.0 until rules go into effect

Comment period “open”

# NSPM-33

JCORE subcommittee released “Recommended Practices for Strengthening the Security and Integrity of US S&T Research Enterprise”

NSPM-33 White House/OSTP directive requiring all federal research funding agencies to strengthen and standardize disclosure requirements for R&D awards and ensure research security measures at universities receiving federal funds (initially signed 01/14/2020)

Lead federal agencies:  NIH & NSF

# NSPM-33

NSPM-33 directs federal funding agencies to strengthen the protection of US government supported R&D against foreign government interference/ exploitation

Mandates research security program at institutions receiving federal funding for science and engineering research (award funding number/not expenditures) in excess of $50M/year

Comment period “open”