



DEPARTMENT OF DEFENSE

6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

CHIEF INFORMATION OFFICER

MEMORANDUM FOR SENIOR PENTAGON LEADERSHIP
COMMANDERS OF THE COMBATANT COMMANDS
DEFENSE AGENCY AND DOD FIELD ACTIVITY DIRECTORS

SUBJECT: Requirement for Applying Baseline Controls for Controlled Unclassified Information Systems

As part of the Department's response to Section 1742 (a) of the William M. (Mac) Thornberry National Defense Authorization Act (NDAA) for Fiscal Year 2021 (FY21) (Public Law 116-283), *Cyber Security Practices and Capabilities in the Department of Defense*, and per the Legal Authority in Title 32 Code of Federal Regulations (CFR) Part 2002, the Department has identified specific security measures for information systems identified as handling controlled unclassified information (CUI).

Per Federal Information Processing Standards (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, a moderate confidentiality impact level meets the requirements for CUI Basic. To mirror the practices and capabilities of the Cybersecurity Maturity Model Certification (CMMC) framework for Level 3, the Department has identified that the minimum requirement for confidentiality and integrity is the moderate impact level; along with the additional enhancements within the National Institute of Standards and Technology (NIST) 800-53 security control SA-12 Supply Chain Protection.

The additional enhancements for SA-12 include:

- (1) Acquisition Strategies/Tools/Methods,
- (2) Supplier Reviews,
- (7) Assessments Prior to Selection/Acceptance/Update,
- (10) Validate as Genuine and Not Altered,
- (13) Critical Information System, and
- (15) Processes to Address Weaknesses or Deficiencies

Components are to ensure those information systems that process CUI have a valid Authorization to Operate (ATO) and implement the relevant security measures to achieve the CMMC-like or other appropriate capability and performance threshold (i.e., at least a moderate impact level for both confidentiality and integrity) prior to the March 1, 2022, suspense specified in Section 1742, NDAA, FY21.

The Department recognizes that the Risk Management Framework (RMF) teams may find it necessary to tailor, also known as modifying, a control set in response to increased risk from threat of vulnerability changes or variations in risk tolerance. As such, document all-tailoring decisions in the security plan for the system per current RMF policy. Additionally, components will update the CUI System Level Plan of Actions and Milestones (POA&M) template by January 17, 2022, for existing CUI information systems that will not achieve the moderate impact level for confidentiality and integrity or will not have a valid authorization by

March 01, 2022. The template offers a minimum criteria baseline with the expectation that scheduled completion date(s) will not exceed January 01, 2027. At this time, there is no exception to policy.

The DoD CIO point of contact on this matter is David Shugart, at (703) 545-2210, or david.a.shugart.civ@mail.mil.

Mark G. Hakun
Acting DoD DCIO for Cybersecurity /
DoD Senior Information Security Officer

Attachments:
As Stated