**DEPARTMENT OF DEFENSE**
6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

MEMORANDUM FOR: SEE DISTRIBUTION

SUBJECT: Cybersecurity Reciprocity

Reference: (a) DoD Instruction 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)," March 12, 2014

The DoD requires speed and agility in the delivery of warfighting capability to the field. It also must deliver secure solutions. Achieving this balance requires that scarce security resources be spent on due diligence and analysis, rather than redundant and unnecessary testing or bureaucratic documentation. As stated in Reference (a), it is DoD policy that "*The DoD RMF presumes acceptance of existing test and assessment results and authorization documentation*." Notwithstanding that this principle has been DoD policy and is set forth in the DoD Instruction in Reference (a), DoD components frequently do not evaluate the body of evidence, which is the basis for reciprocity, developed by other DoD Components in their prior authorization of a system or software to be deployed.

Reference (a), at Enclosure 5, provides details for the implementation of Cybersecurity Reciprocity. Effective immediately, in accordance with the Reference, Components will maximize reuse of assessment and authorization evidence developed by prior system authorization and deployments within sister DoD Components. Any such cybersecurity assessment, authorization and testing conducted by another component shall be evaluated before additional assessment or testing is undertaken. Assessments, authorizations, and tests by another DoD Component shall be presumed to have been correctly completed, and that assessment, authorization and testing, and the resultant test evidence, will be accepted by all DoD components as a basis for Assessment and Authorization. A DoD component may conduct additional testing to address unique conditions within the Component environment, as specified in Reference (a), but is not authorized to retest what another DoD Component has already tested. In the case where a component organization asserts that the assessment, authorization and testing completed by another component was performed incorrectly, or was deficient in some other manner, approval must be obtained from the DoD CIO prior to any additional assessment, authorization and testing.

Each component will make all cyber security authorization documentation available (via Enterprise Mission Assurance Support Service (eMASS) or other electronic means) to other components seeking to utilize reciprocity for that system or software.

Cybersecurity Reciprocity is the default for Assessment and Authorization of an IT system already deployed in the Department of Defense. Accordingly, any DoD Component undertaking an assessment and authorization effort will determine if the system being assessed has already been assessed, authorized and tested, and will proceed based upon existing assessment evidence.

My point of contact for this matter is Mr. Mitchell Komaroff at mitchell.komaroff.civ@mail.mil, (703) 697-3314. Additional information about reciprocity can be found on the Risk Management Framework Knowledge Service (https://rmfks.osd.mil).

HALVORSEN.TERRY.A.1034645953

Digitally signed by HALVORSEN.TERRY.A.1034645953
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OSD, cn=HALVORSEN.TERRY.A.1034645953
Date: 2016.10.18 15:41:05 -04'00'

Terry A. Halvorsen
DoD Chief Information Officer

Attachments:
None

DISTRIBUTION:
SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DEPUTY CHIEF MANAGEMENT OFFICER
CHIEFS OF THE MILITARY SERVICES
CHIEF OF NATIONAL GUARD BUREAU
COMMANDANT OF THE UNITED STATES COAST GUARD
COMMANDERS OF THE COMBATANT COMMANDS
CHIEF OF THE NATIONAL GUARD BUREAU
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, COST ASSESSMENT AND PROGRAM EVALUATION
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
ASSISTANT SECRETARY OF DEFENSE FOR LEGISLATIVE AFFAIRS
ASSISTANT TO THE SECRETARY OF DEFENSE FOR PUBLIC AFFAIRS
DIRECTOR, NET ASSESSMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES