



UNDER SECRETARY OF DEFENSE
5000 DEFENSE PENTAGON
WASHINGTON, DC 20301-5000

SEP 27 2023

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

SUBJECT: Use of Digital Signatures on Standard Form 312

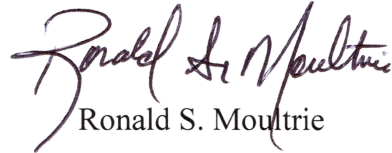
References: (a) Executive Order 13526, "Classified National Security Information," January 5, 2010
(b) 32 Code of Federal Regulations, Part 2001, June 28, 2010
(c) ISOO Notice 2022-01: "Digital Signatures on Standard Form (SF) 312, Classified Information Nondisclosure Agreement," May 9, 2022
(d) DoD Manual 5200.01, Volume 1, "DoD Information Security Program: Overview, Classification, and Declassification," February 24, 2012, as amended

The Information Security Oversight Office, as Executive Agent for references (a) and (b), issued updated guidance to Departments and Agencies on the use of digital signatures on Standard Form (SF) 312, "Classified Information Non-Disclosure Agreement" at reference (c). Based upon that guidance and in the interest of information security reform, Department of Defense (DoD) Components are authorized to accept digital signatures on all SF 312s as described in this memorandum.

DoD military, civilian, and contractor personnel may now sign SF 312s using a DoD-issued credential that is: (1) based on public key infrastructure (PKI) and (2) includes a reliable certificate authority (CA). This includes the common access card, DoD-approved derived credentials (e.g., Purebred), personal identity verification (PIV), or DoD-approved PIV-Interoperable (PIV-I) cards. In addition, DoD personnel may use digital signatures from DoD-sponsored External Certificate Authority PKIs, which are listed at <https://cyber.mil/eca/>, and DoD-approved external PKIs, which are listed at <https://cyber.mil/pki-pke/interoperability/>. DoD-approved external PKIs include certain federal personal PIV and industry PIV-I PKI credentials.

DoD components will reciprocally accept SF 312s containing digital or manual signatures, or a combination of both. Because of the authentication, consent, and integrity provided by the digital signature, the witness block does not require a signature if the user signs digitally. However, a digital or manual signature in the Acceptance block is still required.

This memorandum supersedes requirements in Enclosure 3, Section 12.b.(1) of reference (b) and will be incorporated into future policy reissuances. The point of contact for information security policy matters is Michael Russo, who may be reached at (703) 692-7836 or michael.c.russo14.civ@mail.mil.



Ronald S. Moultrie