prior to March 28, 2016 and at all times thereafter.

[FR Doc. 2022–06669 Filed 3–28–22; 8:45 am]

BILLING CODE 0099–10–D

DEPARTMENT OF THE TREASURY

Internal Revenue Service

26 CFR Part 1

Income Taxes

CFR Correction

This rule is being published by the Office of the Federal Register to correct an editorial or technical error that appeared in the most recent annual revision of the Code of Federal Regulations.

■ In Title 26 of the Code of Federal Regulations, Part 1 (§§ 1.301 to 1.400), revised as of April 1, 2021, in § 1.358–6, revise paragraph (f)(1) and revise the first sentence of paragraph (f)(3) to read as follows:

§ 1.358–6 Stock basis in certain triangular reorganizations.

* * * * *

(f) * * *

(1) *General rule.* Except as otherwise provided in this paragraph (f), this section applies to triangular reorganizations occurring on or after December 23, 1994.

* * * * *

(3) *Triangular G reorganization and special rule for triangular reorganizations involving members of a consolidated group.* Paragraph (e)(1) of this section shall apply to triangular reorganizations occurring on or after September 17, 2008. * * *

* * * * *

[FR Doc. 2022–06668 Filed 3–28–22; 8:45 am]

BILLING CODE 0099–10–D

NATIONAL ARCHIVES AND RECORDS ADMINISTRATION

Information Security Oversight Office

32 CFR Part 2001

[FDMS No. NARA–22–0002; NARA–2022–021]

RIN 3095–AC06

Classified National Security Information

AGENCY: Information Security Oversight Office (ISOO), National Archives and Records Administration (NARA).

ACTION: Direct final rule.

SUMMARY: We are revising our Classified National Security Information regulation to permit digital signatures that meet certain requirements on the Standard Form (SF) 312, which is the non-disclosure agreement required prior to accessing classified information. Due to agency needs during the COVID–19 pandemic and remote work situations, combined with developments in digital signatures since a regulatory prohibition on electronic signatures was implemented in 2010, it is both urgent and appropriate to make this administrative change at this time.

DATES: This rule is effective on May 9, 2022, unless we receive adverse comments by April 28, 2022 that warrant revising or rescinding this rulemaking.

ADDRESSES: You may submit comments, identified by RIN 3095–AC06, by the following method:

• *Federal eRulemaking Portal: https://www.regulations.gov.* Search for RIN 3095–AC06 and follow the site's instructions for submitting comments.

We may publish any comments we receive without changes, including any personal information you include.

During the COVID–19 pandemic and remote work situation we cannot accept comments my mail or delivery because we do not have staff in the office.

FOR FURTHER INFORMATION CONTACT: Kimberly Keravuori, Regulatory and External Policy Program Manager, by email at *regulation_comments@nara.gov,* or by telephone at 301.837.3151.

SUPPLEMENTARY INFORMATION: These regulations were last revised in 2010. At that time, these regulations included a prohibition against signing the Standard Form (SF) 312 electronically, due to concerns about integrity and legal enforceability of any form of electronic signature (e-signature) at the time. In the decade-plus since then, encryption and other measures for e-signatures have advanced and they are now regularly encouraged or required and deemed legally enforceable. In addition, Federal agencies are required to digitize services and forms and accelerate the use of e-signatures as much as possible (*see, e.g.,* 2018 21st Century Integrated Digital Experience Act (21st Century IDEA), 44 U.S.C. 3501 note).

Since the COVID–19 pandemic began in March 2020, numerous Federal agencies have had to engage in remote work to varying degrees and have had difficulty bringing new workers onboard who require access to classified information, due to the requirement for handwritten signatures on the SF 312. It has been placing employees at risk of spreading the virus, as well as creating logistical and other difficulties. Multiple agencies have been consistently requesting the ability to allow e-signatures as a result, and the need became critical and urgent once the COVID–19 pandemic extended much longer than originally anticipated.

The advances in technical ability to ensure valid e-signatures, and legal acceptance of such signatures, is clearly the way of the future and necessary to support a modernized classified national security information system. However, the timing to make this change is more urgent now because of COVID–19 related health risks.

Under laws such as the Government Paperwork Elimination Act (GPEA), 44 U.S.C. 3504 note, the Uniform Electronic Transactions Act (UETA), a model act since adopted by 47 states and the District of Columbia (the remaining three states have comparable laws), and the Electronic Signatures in Global and National Commerce Act (ESIGN), 15 U.S.C. 7001, *et seq.,* an e-signature has the same legal weight as a handwritten signature and cannot be considered invalid simply due to being electronic. The laws establish criteria for valid e-signatures, along the following lines: Intent to sign, consent to do business electronically, association of the signature with the record, attribution to the person signing, and a record of the digital transactions. The United States practices an open-technology approach, meaning there's no law requiring use of a specific signing technology for an e-signature to be legally binding, as long as it meets the criteria.

However, for the purpose of e-signatures on the SF 312, ISOO has established certain requirements agencies must meet if they wish to allow such signatures. We require that agencies use digital signatures (rather than other forms of e-signature) on the SF 312 because digital signatures provide the requisite level of security and authenticity appropriate for these agreements. Digital signatures are a specific signature technology type of e-signature that allows users to sign documents and authenticate the signer. Digital signatures are based on a standard, accepted format, called public key infrastructure (PKI), to provide the highest levels of security and universal acceptance through use of a mathematical algorithm and other features. The mathematical algorithm acts like a cipher and encrypts the data matching the signed document. The resulting encrypted data is the digital signature, which is also marked with the