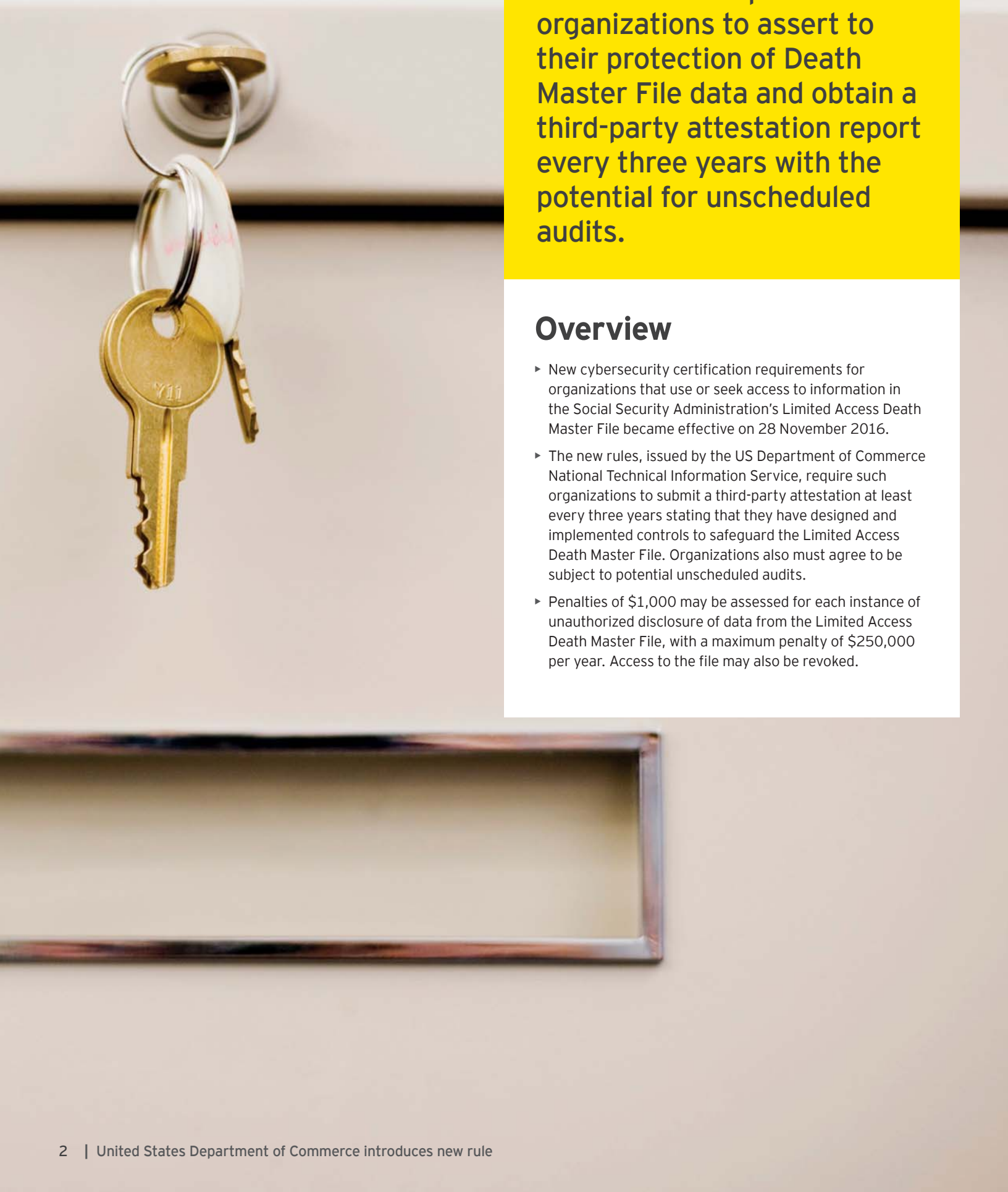
United States Department of Commerce introduces new rule

Organizations using the Limited Access Death Master File are required to obtain a third-party conformity attestation

EY
Building a better working world



The new rule requires organizations to assert to their protection of Death Master File data and obtain a third-party attestation report every three years with the potential for unscheduled audits.

Overview

- New cybersecurity certification requirements for organizations that use or seek access to information in the Social Security Administration's Limited Access Death Master File became effective on 28 November 2016.
- The new rules, issued by the US Department of Commerce National Technical Information Service, require such organizations to submit a third-party attestation at least every three years stating that they have designed and implemented controls to safeguard the Limited Access Death Master File. Organizations also must agree to be subject to potential unscheduled audits.
- Penalties of $1,000 may be assessed for each instance of unauthorized disclosure of data from the Limited Access Death Master File, with a maximum penalty of $250,000 per year. Access to the file may also be revoked.

Background

The US Department of Commerce (Commerce) National Technical Information Service (NTIS) published a rule (15 CFR Part 1110[1]) that became effective November 28, 2016, requiring organizations (Certified Persons) with current or requested new access to the Limited Access Death Master File (DMF) to submit a written third-party conformity attestation from an auditor (Accredited Conformity Assessment Body, or ACAB) that the organization has "information security systems, facilities, and procedures in place to protect the security of the Limited Access DMF."

The DMF is a Social Security Administration database that contains names, social security numbers, and dates of birth and death for US citizens who have died from 1936 to the present. Organizations generally obtain a full download of the DMF file each month and incorporate the file into their systems/environment.

DMF data has many purposes, but is commonly used by organizations to help prevent fraud and validate certain financial transactions (e.g., to stop payment of annuities or retirement benefits upon death, validate death claims, and research unclaimed property). In the insurance sector, many states are enacting laws requiring life insurers to check the DMF against current life insurance policies to help prevent insurers from failing to pay out to beneficiaries upon death. The National Association of Insurance Commissioners (NAIC) is currently working on an unclaimed benefits model law that would require similar procedures.

Currently, more than 550 organizations have access to the DMF, and most have had such access for several years. Under the previous rule, organizations wanting access paid a nominal fee to Commerce and self-certified every three years that adequate procedures were in place for protecting the DMF.

Key aspects of the new NTIS Rule, in addition to the third-party conformity attestation every three years, include:

- Access must be recertified by the organization annually (rather than every three years).
- Certified users must agree to both scheduled and unscheduled audits. Unscheduled audits are anticipated to be uncommon and would generally be conducted by NTIS or the ACAB at the request of NTIS.
- Penalties for using DMF information in a manner not intended by the law are $1,000 per unauthorized disclosure with a maximum penalty of $250,000 per year.
- A process exists for appealing denials or revocations of certification.

Third-party attestation requirements

Under the NTIS Rule, an ACAB is defined as an independent third party that is accredited by an accreditation body under nationally or internationally recognized criteria (e.g., American Institute of Certified Public Accountants (AICPA) or International Organization for Standardization (ISO)). Under the rule, as organizations' three year renewal periods occur, an ACAB must conduct a third-party assessment against a security framework to confirm an organization's information security systems, facilities, and procedures are in place to protect the security of the DMF. Acceptable security frameworks cited by Commerce NTIS include, but are not limited to, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53,[2] the NIST Framework for Improving Critical Infrastructure Cybersecurity, and the ISO 27000 series of publications.

If an organization has not adopted a formal security framework as a suitable criterion for an attestation, NTIS has created the Limited Access Death Master File (Limited Access DMF) Certification Program Publication 100[3] (Publication 100). Publication 100 is a subset of controls largely based upon NIST SP 800-53 and allows for third-party attestation against criteria, as defined in its sections (4) Information Secure Storage; (5) Restricting Access to Limited Access DMF Information; (6) Disposing of Limited Access DMF Information; and (7) Information Security.

Although Commerce will make all decisions regarding interpretation of and adherence to the NTIS Rule, organizations may comply through having an examination engagement conducted under the AICPA attestation standards. The examination report can take different forms, including being at a point-in-time over management's assertion that the controls over the DMF were designed and implemented in accordance with either the criteria of a security framework or Commerce Publication 100 sections 4–7.

Commerce NTIS is aware that security assessments and/or audits are routinely performed and is permitting organizations to leverage the procedures conducted by an ACAB to support the third-party attestation requirement provided the controls assessed also specifically protect the DMF. Organizations already obtaining a Service Organization Control 2 (SOC 2) examination report or an ISO 27001 certification may be best positioned for such synergies and could consider using their existing independent auditor as their ACAB.

Given the importance of maintaining continued access to the DMF for many organizations, consider **pre-assessments** to permit satisfactory remediation of control deficiencies, if any, prior to the formal attestation and access renewal.

Upon completion of the attestation by the ACAB, Commerce NTIS requires the ACAB Systems Safeguards Attestation Form be completed to collect information on the attestation by the ACAB conducted within three years prior to the date of the access renewal. Such collection activities include specific requirements of the NTIS Rule, which the ACAB must certify are satisfied, and the collection of specific information by the ACAB, such as the assessment date of the third-party attestation and the standard(s) applied to the attestation engagement. The *ACAB Systems Safeguards Attestation Form* does not currently provide for listing control deviations identified by the ACAB over safeguarding the DMF within the Assessment Results section. The examination report could be attached to the ACAB Systems Safeguards Attestation Form and submitted by the ACAB.

We encourage organizations that are required to comply with the new NTIS Rule to determine when they must renew their certification and identify synergies between controls being assessed in their existing audits/attestations and those required for compliance by Commerce.

We recommend that organizations that have not already formally adopted a security control framework (e.g., NIST SP 800-53, ISO 27001) consider applying the framework suggested by Publication 100 as it is a smaller subset of controls as compared with a full control framework, such as NIST SP 800-53.

Organizations may consider having a pre-assessment performed by a third party to identify potential control deficiencies relevant to the DMF in order to take remediation actions prior to the formal attestation and DMF access renewal depending upon their renewal deadline.

Endnotes:

[1] The final rule is listed on the Federal Register at https://www.federalregister.gov/documents/2016/06/01/2016-12479/certification-program-for-access-to-the-death-master-file.
[2] (SP) 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations,* NIST, April 2013.
[3] Publication 100, June 2016, http://www.ntis.gov/assets/pdf/NTIS-DMFsecurityGuidelinesv14.pdf.

SCORE no. 01035-171US

1702-2202869

ED None