THE BERWYN GROUP, INC.

Mortality Verification and Locator Services A SOC 2 Compliant Company

Date: March 26, 2015

National Technical Information Service
U.S. Department of Commerce

Submitted electronically via www.regulations.gov

Re: Request for Comments ("RFC") regarding the establishment by the National Technical Information Service ("NTIS") of the final proposed rules for the certification program for Persons who seek access to the Social Security Administration's Public Death Master File ("DMF")

This letter shall serve as a response by The Berwyn Group, Inc. ("Berwyn Group") to the RFC from the public regarding the establishment by the NTIS of final proposed rules for the certification program for Persons who seek access to the Social Security Administration's Public Death Master File (DMF) as required by Section 203 of the Bipartisan Budget Act of 2013 (Pub. L. No. 113-67) ("Act"). In its Request for Comments, the NTIS seeks responses to specific areas set forth in the RFC in order to provide the opportunity to participate in the rule making process.

In order to fully understand Berwyn Group's response to the RFC, it is helpful to understand how Berwyn Group uses the information contained in DMF, and to understand the functions Berwyn Group performs as a third party administrator on behalf of its customers that require it to have continual access to the DMF. Berwyn Group services a wide range of industries including, major corporations, banks, financial institutions, insurance companies, unions, public and municipal employee retirement systems, medical institutions and universities. Berwyn Group assists these clients by conducting regular mortality verification (death audits) and address verification (locator services) of clients' pension files, insured's, beneficiaries, annuitants as well as audits or analysis of any large data base that is utilized to send insurance claims payments, unclaimed property distributions, pension, IRA and 401(k) distributions, insurance policies, annual funding notices and other important benefits, pension and insurance documents to individuals.

These services are designed to:

- Prevent fraud by avoiding sending checks to retirees or beneficiaries who are deceased;
- Prevent Identity Theft by not sending important financial, pension and insurance documents to unintended recipients and beneficiaries;
- Identify insured's, annuitants or beneficiaries who are deceased, but have not filed a claim for proceeds;
- Correct inaccuracies in client files;

23215 Commerce Park Dr, Suite 215; Beachwood, OH 44122-5843
Tel: (216)765-8818 Fax: (216)765-8827 Email: felix@berwyngroup.com Website: www.berwyngroup.com

- Prevent paying medical premiums for retirees and/or spouses who are deceased;
- Improve plan financial viability by reducing erroneous payments;
- Locate beneficiaries of deceased retirees/term vested participants to ensure compliance with federal regulations;
- Satisfy auditors that client records are correct and in order; and
- Assist with compliance with a multitude of State and Federal laws regarding pension administration and unclaimed funds;

In order to conduct its business, Berwyn Group electronically compares client records against its proprietary Master Death Database comprised of millions of deceased individuals compiled from numerous sources over many years. Berwyn Group files are frequently updated and contain records from the Social Security Administration (SSA) DMF via NTIS, state and federal agencies, and its own proprietary death data. In order to perform these important functions, continued and regular access to the DMF is required. It is also important that Berwyn Group be lawfully permitted to disclose information contained in the DMF to its certified as well as to its non-certified client's in order to perform its services.

Berwyn Group routinely has access to "non-public personal information files." The information within these files is protected by the Gramm-Leach-Bliley Act ("GLBA"), 15 U.S.C. § 6801, et seq. and the Fair Credit Reporting Act, 15 U.S.C. § 1681 et seq. ("FCRA"), and for certain clients by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and the Health Information Technology for Economic and Clinical Health Act ("HITECH"). In addition to GLBA, FCRA, HIPAA and HITECH, Berwyn Group clients are regulated by a wide variety of federal and state laws including:

(i) Federal Trade Commission
(ii) Federal Deposit Insurance Act
(iii) Securities and Exchange Act of 1934
(iv) Federal Trade Commission Act
(v) Employee Retirement Insurance Securities Act of 1974 ("ERISA")
(vi) US Patriot Act
(vii) Bank Secrecy Act Customer Identification Program

Berwyn Group is currently certified to have access to the DMF under NTIS' Interim Rule pursuant to the Temporary Certification Program for Access to the Death Master File.

Access to the DMF is required by State Statutes regarding unclaimed funds in approximately twenty (20) states. In addition, certain states require the implementation of procedures to identify deceased individuals in their insurance pools (where claims have not been previously filed) and investigate and locate beneficiaries with respect to death benefits under these life insurance policies. For example, New York State Department of Financial Services Insurance Regulation 200, 11 NYCRR226 requires the implementation of procedures to investigate and locate beneficiaries with respect to death benefits under life insurance policies for unreported claims. In addition, numerous states have entered into agreements with insurance companies that require specified procedures to identify deceased policyholders on a proactive basis and to investigate and locate beneficiaries with respect to death benefits under life

insurance policies, annuities and other insurance products. A compliance agreement between thirty six (36) states and John Hancock Life Insurance Company requires access and use of the DMF. Berwyn Group assists many insurance companies (and our insurance company client list continues to grow) in complying with this and similar agreements.

In performing these functions, Berwyn Group is also required by law to make certain that the client companies and individuals for whom it works with, and with whom it shares information with, have a legal right to access this data. Many states have legislation governing standards for protection of personal information. For example, the Commonwealth of Massachusetts established requirements designed to adopt and implement the maximum feasible measures needed to ensure the security, confidentiality and integrity of Personal Information, as defined in MGL. c. 93H and MGL. c. 66A, including access to systems containing such information or data, and as implemented by 201 CMR 17.00. As a part of Berwyn Group's responsibilities under these statutes, it is required to document that it has made every reasonable effort to verify the permissible purpose, and permissible use.

Permissible purpose includes preventing fraud. Making certain that clients have the correct address information in its files for vested participants ensures that beneficiary checks are not cashed by unintended recipients. Berwyn Group also assists in preventing fraud by identifying deceased individuals, locating and contacting beneficiaries of deceased individuals, contacting vested participants, and updating records. Permissible use does not include using this data for marketing purposes, selling or transferring this data to organizations (either external or internal to the client company) for the purpose of marketing products, or using the data for employment purposes.

The area's that NTIS requested public comments are as follows:

1. ***"Limited Access DMF" Proposed Definition:*** NTIS is soliciting comments on its proposal to revise the definition of "Limited Access DMF" by adding a sentence that clarifies that an individual element of information (name, social security number, date of birth, or date of death) in the possession of a person whether or not certified but obtained through a source independent of the Limited Access DMF, will not be considered "DMF information" if the NTIS source information is replaced with the newly provided information.

Comment: The last part of the sentence, "*if the NTIS source information is replaced with the newly provided information"*, is confusing and unnecessary. What does that mean to replace the information? If the recipient has the information from another source, the concept of replacing it is confusing in the sense that such recipient does not know what or how to replace it. The end of the sentence should state: "will not be considered "DMF information" if the NTIS source information *is obtained from a source other than NTIS"*.

Unsolicited Comment: NTIS should endeavor to restore the complete DMF rather than the reduced limited version as currently provided.

2. ***Certifying Fraud Prevision/Business Purpose Interest:*** NTIS is soliciting comments on the specificity with which a Person should be required to provide as the basis for certifying its fraud prevention interest or business purpose. NTIS is also requesting comments on what types of materials NTIS should accept in support of a certification application to demonstrate that a party has legitimate business purpose or legitimate fraud prevention interest.

Comment: Berwyn Group recommends that NTIS develop a standardized Certification Form to be completed by the proposed certified and non-certified recipient of the DMF information. A Certified Person should have clear and concise guidelines for sharing DMF information with a non-certified Person. For example, a certified Person could satisfy its responsibilities for sharing DMF information with a non-certified Person by receiving an NTIS approved form. The form could include a check the box information section such as the following:

Is your company certified by NTIS to receive DMF information: ___yes: ___no

What is Industry is served by your company:_____
Provide NAICS and/or SIC code:_____
DUNS # (if available):_____

Is your company currently regulated by security and privacy provisions of other state or federal regulations? Please list all relevant regulations that apply._____

Functional Responsibilities: (Check the item that best describes your functional responsibility)

- □ Actuarial Services
- □ Auditor
- □ Governmental Pension Administration
- □ Human Resources Administration
- □ Health & Welfare Fund Administration

□ Insurance Administration
□ Investment Services Administration
□ Pension Administration
□ Other:_____

PART 2: PLEASE STATE THE PURPOSE OF DATA REQUEST:

□ Locate Missing Terminated Vested Participants
□ Locate Missing Pensioners.
□ Locate Missing Shareholders
□ Other purpose: _____
_____
_____

PART 3: ELIGIBILITY CHECKLIST:

SECTION A: GLBA ACCEPTABLE USES (CHECK ALL THAT APPLY - AT LEAST ONE MUST BE CHECKED)

The information that will be provided to your company may contain consumer identification information governed by GLBA. In accordance with GLBA, such information may only be used for the following purposes:

□ **Insurance purposes** including (a) account administration, (b) reporting, (c) fraud prevention, (d) premium payment processing, (e) claim processing and investigation, (f) benefit administration, or (g) research projects.

□ **Fraud detection and prevention** including, but not limited to: pension, investment account and benefits administration – for the purpose of locating missing vested participants to ensure that checks and confidential information are sent to the correct individuals so that there are no losses and unintentional consequences as a result of confidential information and monies being utilized by wrongful recipients.

□ **Other Purpose:**

Each Person would be required to submit the form. The form must include a certification and confidentiality provision.

3. ***Accredited Certification Bodies Attestation:*** NTIS is soliciting comments on implementing Accredited Certification Bodies to conduct periodic scheduled and unscheduled audits of certified Persons on behalf of NTIS. NTIS requests comments on the proposal to accept attestations by private sector, third party, Accredited Certification Bodies under the rule.

Comment: NTIS should develop criteria to accredit and certify organizations to conduct audits. A shared assessment tool that is widely used for information security related risks can be used. However, if a certified entity has already invested in completing such an assessment, and/or if a certified Person has already been audited by an accredited third party (such as an independent audit firm that is accredited to conduct such audits), an independent auditor opinion letter, attestation or copy of the report should be deemed adequate evidence. The cost implication of periodic scheduled and unscheduled audits of certified Persons on behalf of NTIS should be taken into consideration. These audits can be cost prohibitive to many entities and having certified Persons repeat audits by an independent audit firm representing NTIS will cause undue financial burden.

4. ***Accreditations Encompassing the Information and Security Requirements:*** NTIS is soliciting comments on its proposal of requiring the Accredited Certification Body attest that the scope of its accreditation encompasses the information safeguarding and security requirements.

Comment: The goal is to insure that the recipient of DMF information has systems, facilities and procedures in place to protect personal data and to deter fraud. In addition to the ISO/IEC 270006-2001, the American Institute of Certified Public Accountants have guidelines for conducting audits to test the suitability of the design and operating effectiveness of controls to meet the criteria for the security, availability, processing integrity and privacy principals. For example, SOC 2 engagements use predefined criteria in *Trust Services Principals, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy (*AICPA Technical Practice Aids) as well as the requirements and guidance in AT Section 101, *Attest Engagements, of SSAEs (*AICPA, *Professional Standards, vol.1).* A Type 2 report includes a description of the test performed by the auditor and the results of those tests. SOC 2 reports specifically address one or more of the following key elements.

Security-The system is protected against unauthorized access (both physical and logical).

Availability- The system is available for operation and use as committed or agreed.

Processing integrity- The system processing is complete, accurate, timely and authorized.

Confidentiality- Information designated as confidential is protected as committed or agreed.

Privacy- Personal information is collected, used, retained, disclosed and disposed of in conformity with the commitments in the entity's privacy notice, and with criteria set forth in Generally Accepted Privacy Principles ("GAPP") issued by the AICPA.

A Person who undergoes an audit by an independent CPA firm who issues a satisfactory AICPA Service Organization Control Report, ("SOC") Type 2 Audit Report should be deemed to satisfy Sec. 1110.102(a)(2) and 1110.502(b) and be exempt from further audit by the NTIS or its designee. At most, if a Person submits an accredited audit, the audit directed by NTIS should be limited to a review of such Person's independent accredited audit. In the event the NTIS audit discloses a deficiency in such Persons accredited audit, the NTIS directed audit should be limited to the deficiency discovered. A CPA firm accredited to conduct such audits should automatically be accredited to attest that the scope of its accreditation encompasses the information safeguarding and security requirements. The rules should include a reference to the AICPA being an approved Accredited Certification Body in section 1110.5.

5. ***Approaches to Safeguarding Information:*** NTIS is soliciting comments on relevant suitable approaches for safeguarding information contained in the DMF.

Comment: No additional comment.

6. ***Three-year Frequency of Assessments:*** NTIS is soliciting comments on its proposal that the limitation of three years is appropriate as to the frequency for assessments addressing the controls set forth in the Limited Access DMF Certification Program.

Comment: Three years is an appropriate time period. The rules should also specify that an independent attestation only be required one time within a three year time period.

7. ***Interpretation of Section 203(b):*** NTIS is soliciting comments on its interpretation of Section 203(b) as requiring persons to certify that they have systems, facilities, and procedures in place that are "similar to" those required by section 6103(p)(4) of the IRC in order to become a certified Person.

Comment: Certified Persons should submit documentation of compliance. Such documentation could include an SOC 2, ISO/ Report. Documentation could also include a security policy and manual applicable to the handling of DMF information that demonstrates that they have systems, facilities, and procedures in place that are "similar to" those required by section 6103(p)(4) of the IRC. Non-certified recipients of DMF information should be required to sign a form certifying the following:

(i) Such Person meets the requirements of paragraphs (a)(1) through (3) of Section 1110.102;

(ii) Such Person has a legitimate fraud prevention interest or a legitimate business purpose pursuant to a law, governmental rule, regulation, or fiduciary duty;

(iii) Such Person shall not further disclose the information to any person other than a person who meets the requirements of paragraphs (a)(1) through (3) of this Section 1110.102.

A certified Person should be permitted to rely upon a certification of a non-certified Person, and should have clear guidelines for sharing MDF information with non-certified Persons.

8. ***LADMF Certification Program Publication 100:*** NTIS is soliciting comments on the security guideline document it developed setting out safeguard approaches adapted to the provisions of Section 203.

Comment: Publication 100 should specifically state that a Certified Person who adheres to the guidelines set forth in Publication 100 is not required to comply with I.R.S. Publication 1075.

9. ***"Safe Harbor" Rule:*** NTIS is soliciting comments on the proposed rule allowing another certified Person to disclose Limited Access DMF to other certified Persons and not imposing a penalty under Section 1110.200(a)(1)(i)-(iii) where the receiving party turns out not to be certified Person.

Comment: An additional safe harbor should be developed so that a certified recipient of DMF information can lawfully disclose DMF information to a Person who is not certified, provided that such non-certified Person executes a certification form containing the items set forth in the comment to #7 above. This is critically important to certified Persons who provide important

fraud prevention, record-keeping, regulatory compliance and related services to customer organizations who do not subscribe (and hence not certified) independently to obtain SSA's DMF.

Section 1110.200 Imposition of penalty, should be modified to include the following:

> (d) Disclosure to a Non-certified Person. Provided a certified Person obtains a certification from a Non-certified Person in compliance with Section 1110.102, no penalty shall be imposed under paragraphs (a)(i) through(iii) of this section on a certified Person who discloses, to a Non-certified Person, DMF information of any deceased individual at any time during the three calendar-year period beginning on the date of the individual's death, where the sole basis for imposition of penalty on such certified Person is that such Non-certified Person has been determined to be subject to penalty under this part.

10. ***Section 1110.102(a)(1) Audits:*** NTIS is soliciting comments on its proposal allowing NTIS to conduct unscheduled audits regarding Section 1110.102(a)(1) at its discretion.

Comment: NTIS should only be permitted to conduct an audit for good cause. As stated in #4 above, a Person who undergoes an audit by an independent CPA firm or similar, who issues a satisfactory AICPA Service Organization Control Report, ("SOC") Type 2 Audit Report, or a similar ISO/IEC Report should be deemed to satisfy Sec. 1110.102(a)(2) and 1110.502(b) and be exempt from further audit by the NTIS or its designee. At most, if a Person submits an accredited audit, the audit directed by NTIS should be limited to a review of such Person's independent accredited audit. In the event the NTIS audit discloses a deficiency in such Persons accredited audit, the NTIS directed audit should be limited to the deficiency discovered.

11. ***Auditing Costs:*** NTIS is soliciting comments requiring audited persons to be directly responsible to the Accredited Certification Body for any charges and/or audit fees.

Comment: The audited Person should not be responsible for the cost of an audit that exceeds $3,000.00 in any three (3) year period. Certified Persons may have spent large sums, time and effort to obtain a SOC 2 audit or similar ISO/IEC audit. The audited Person would have no control over the cost of an NTIS audit, which such audited Person may or may not be able to pay. A limit on the cost of the audit is appropriate in light of the fact that the certified Person has no control over the time, scope or frequency of an audit. In similar governmental audit circumstances such as an IRS audit, the audited Person does not reimburse the IRS for the cost of an audit.

12. ***Independent Attestation:*** NTIS is soliciting comments on its proposed rule requiring the Accredited Certification Body performing the attestation be independent of the Person, and requiring it itself be accredited by a recognized accreditation body.

Comment: See response to #4 above.

13. ***Attesting to ISO/IEC Standard 27006-2011:*** NTIS is soliciting comments on its proposed rule requiring the Accredited Certification Body attest that it is accredited to ISO/IEC Standard 27006-2011 Requirements for bodies providing audit and certification of information security management systems or to another recognized standard for bodies providing audit and certification of information security and management systems.

Comment: See response to #4 above.

14. ***Impacted Entities:*** NTIS is soliciting comments on the different types and sizes of entities affected by the proposed rule as well as a description of the types of impacts that this rule will have on those entities.

Comment: All entities should be treated the same under the Rule. The size of the organization should not control the evaluation or certification process.

23215 Commerce Park Dr, Suite 215; Beachwood, OH 44122-5843
Tel: (216)765-8818 Fax: (216)765-8827 Email: felix@berwyngroup.com Website: www.berwyngroup.com