Report No. 2008-02

Options for Verifying the EIN or Otherwise Authenticating the Employer in the E-Verify Program

This paper reflects the consensus recommendations provided by the Data Privacy and Integrity Advisory Committee to the Secretary and the Chief Privacy Officer of the Department of Homeland Security (DHS). The Committee's charter under the Federal Advisory Committee Act is to provide advice on programmatic, policy, operational, administrative, and technological issues relevant to DHS that affect individual privacy, data integrity and other privacy related issues.

The Committee deliberated on and adopted these recommendations during a public meeting on December 3, 2008, in Arlington, VA.

On September 15, 2008 the DHS Privacy Office requested that the Data Privacy and Integrity Advisory Committee (DPIAC) provide guidance on options for achieving the goal of "verifying the EIN or otherwise authenticating the employer" in the E-Verify application. A number of serious privacy and security risks associated with the current E-Verify identification and authentication policies and processes were discussed in public testimony in recent meetings of the DPIAC. Addressing these risks has been made much more urgent by the expanding use of the system, including state mandates and the recent federal rule requiring certain government contractors to use it.

The Privacy Office's letter to the DPIAC states that the Verification Division within Citizenship and Immigration Services has established an E-Verify Employer Registration Business Process Reengineering (BPR) program which will design "a secure, easy to use, and configurable employer E-Verify registration process" and that the DPIAC's guidance will be considered by the BPR Identity Assurance Design team. The design team will establish guidelines that "clearly define the sufficient level of assurance across three major areas: an organization's identity, an individual registrant's identity, and the

relationship between the organization and the individual (e.g. that the person registering for E-Verify is authorized to enroll the company)."

In its letter to the DPIAC, the Privacy Office has noted that the "collection and validation of particular pieces of data are fundamental toward establishing identity. The Employer Identification Number (EIN), if validated, can be instrumental in verifying the identity of an organization. However, validating the EIN through the Internal Revenue Service (IRS) database is challenging due to the legislative constraints on the use of the data. In particular, IRS Code section 6103 (Internal Revenue Code § 6103) prohibits sharing and disclosure of tax return data (interpreted to include the EIN); consequently Verification needs guidance on alternate ways to achieve this goal of verifying the EIN or otherwise authenticating the employer."

In response to the request from the DHS Privacy Office, the DPIAC formed a subcommittee to address these questions, and has held teleconference meetings with representatives of the Identity Assurance Design Team and the Social Security Administration (which is a participant in the E-Verify program) to gather additional information.

The DPIAC notes that the process for assessing the security risks and appropriate risk management controls for applications is vital, and is well documented in NIST special publications, Federal Information Processing Standards, and OMB guidance.

The DPIAC recommends that the BPR Identity Assurance Design Team be expanded to include both a security professional familiar with these standards and requirements as well as a member of the Verification Division Privacy Office to ensure that these guidance documents are considered and addressed as appropriate.

Key NIST guidance includes:

• FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*;

• FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*;

• NIST Special Publication 800-30, *Guide for Conducting Risk Assessments*;

• NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*;

• NIST Special Publication 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*; and

• NIST Special Publication 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*.

The DPIAC also notes that OMB M-04-04, E-Authentication Guidance for Federal Agencies, dated December 16, 2003, requires agencies to establish appropriate risk-based assurance levels for authentication. This memorandum (which references the NIST security guidance noted above) addresses the question of the trade-off between increasing ease of use of an application and implementing necessary security controls:

> *Easing identity credential assurance level requirements may increase the size of the enabled customer pool, but agencies must ensure that this does not corrupt the system's choice of the appropriate assurance level*.

The Committee is concerned that inadequate assurance controls pose significant personal privacy risks. If unauthorized users are able to obtain access to the system to identify combinations of names and SSNs that pass verification, this would represent a major security weakness, compromising personal privacy and frustrating E-Verify's ability to achieve its program goals. The information matches will be far less useful in establishing legitimate employment eligibility.

In this context, the DPIAC offers a number of basic recommendations and options related to the questions posed by the DHS Privacy Office to the Committee.

1. Assess security and privacy risks using NIST and OMB guidance and evaluate, select and implement controls appropriate to that risk. This is a fundamental starting point for the BPR team. Because the Social Security Administration's Social Security Number Verification Service (SSNVS) and E-Verify provide the same information to employers in response to the same queries, they must provide comparable levels of controls. At present, they do not.

2. Explore options for establishing an employer identification and authentication system modeled on that used by the Social Security Administration for SSNVS. The SSA system uses (among other controls) an out-of-band mailing of an access code to employers filing for access to the system and uses tax records to link the user of the system to the employer for whom he or she is working in order to ensure that the user is authorized to access the system. If this is the best means of identification and authentication, DHS should recommend narrowly focused legislative changes to allow it to verify that an EIN is valid, active, and associated with the requestor.

3. Identify and authenticate all individual users of E-Verify. This does not appear to be addressed today in the present registration process. Understanding who is accessing the system, along with whom they are authorized to represent, requires a chain of trust which is the result of verifying and authenticating their identities. A new registration method should be considered which would involve the creation of an identification scheme for employers (or third party agents) and their employees registering as authorized users of E-Verify. This could be completely disconnected from EIN matching for authentication purposes. Such a DHS-managed employer identification scheme would need to ensure authenticated initial registration and enrollment along with ensuring day to day authenticated access to E-Verify.

4. Explore with legal counsel in DHS, IRS and the Social Security Administration options whereby employers may give permission for the use of their EIN for E-Verify purposes that would be consistent with Internal Revenue Code § 6103. For example, when registering to use an improved E-Verify authentication system, employers may give explicit permission for the use of their information as part of the authentication process.

5. Develop alternative registration and authentication methods that will reflect the existing levels of trust associated with types of employers or third-party service providers. This would enable better risk management. For example, the registration and identification processes for large employers or large third party providers who have existing relationships with DHS (or SSA) might differ from processes put into place for small employers. Such an approach could potentially improve risk management by tailoring risk controls according to categories of employers or third parties.

6. Consider the use of commercial information sources to verify the identity of employers registering to access the system and establish agreements and processes with employers authorizing specific employees or third party providers to use E-Verify on their behalf. Any such use of commercial information sources should be consistent with the DPIAC's prior guidance on the use of commercial data.

7. Implement audits and take steps to penalize and publicize fraudulent uses of the E-Verify system.

Finally, the Committee notes that adequate privacy and security controls will require an investment in the E-Verify program. These investments need to be reflected in future budgets. The DPIAC looks forward to further dialogue on other privacy and data integrity aspects of the E-Verify program.