American Bar Association
Section of Science & Technology Law
750 North Lake Shore Drive
Chicago, Illinois 60611

Date: June 28, 2003

Director
Regulations and Forms Services Division
Bureau of Citizenship and Immigration Services
425 I Street NW., Room 4034
Washington, DC 20536

Re: American Bar Association, Section of Science and Technology Law, Comments for the Department of Homeland Security, Bureau of Citizenship & Immigration Services: "Electronic Signature on Applications and Petitions for Immigration and Naturalization Benefits; Interim Final Rule", CIS No. 2224-02

Dear Sir or Madam:

The Section of Science and Technology Law of the American Bar Association is pleased to submit the following comments in connection with the Secretary's public request for comments on "Electronic Signature on Applications and Petitions for Immigration and Naturalization Benefits; Interim Final Rule," Fed Reg. (Federal Register: April 29, 2003 (Volume 68, Number 82), located online at http://a257.g.akamaitech.net/7/257/2422/14mar20010800/edocket.access.gpo.gov/2003/03-10442.htm, reference CIS No. 2224-02.

These views are being presented on behalf of the Science and Technology Law Section only and have not been approved by the House of Delegates or the Board of Governors of the American Bar Association and should not be construed as representing the position of the Association.

A. Introduction

The Secretary's Federal Register Notice describes a signature process and a phased-in program specifically permitting immigration applicants and petitioners to sign electronically as a step towards fulfilling the mandates of the Government Paperwork Elimination Act (GPEA), and support for a feasibility study for online filing mandated by the Public Law 107-296.[1] Acknowledging that the "courts appear to recognize electronic signatures supported by appropriate authentication safeguards if the governing statute or rule specifically permits them," the rule was promulgated "to amend the regulations at 8 CFR 103.2(a)(2) to specifically permit applicants and petitioners to electronically sign their applications or petitions filed electronically with the BCIS."[2] A stated goal was for "the BCIS to accept electronically filed applications and petitions without diminishing the certification made under penalty of perjury by applicants and petitioners".

B. Electronic Signature Methodology

The Secretary described the process for signing electronically as follows:

---

[1] The Secretary noted that the GPEA provides that the Office of Management and Budget (OMB) must ensure that no later than 5 years from October 21, 1998, executive agencies provide for the option of electronic submission of information, when practicable, as a substitute for paper. The Secretary further observed that Section 461 of the Homeland Security Act of 2002 (effective January 24, 2003) provides that the Secretary of Homeland Security shall conduct a study of the feasibility of online filing.

[2] Sec. 103.2(as amended): Applications, petitions, and other documents.

(a) * * *

(2) Signature. An applicant or petitioner must sign his or her application or petition. However, a parent or legal guardian may sign for a person who is less than 14 years old. A legal guardian may sign for a mentally incompetent person. By signing the application or petition, the applicant or petitioner, or parent or guardian certifies under penalty of perjury that the application or petition, and all evidence submitted with it, either at the time of filing or thereafter, is true and correct. Unless otherwise specified in this chapter, an acceptable signature on an application or petition that is being filed with the BCIS is one that is either handwritten or, for applications or petitions filed electronically as permitted by the instructions to the form, in electronic format.

* * * * *

The interim rule was made effective May 29, 2003, and post-adoption comment only has been requested. "The DHS's implementation of this rule as an interim rule, with provisions for post-promulgation public comments, is based on the ``good cause'' exceptions found at 5 U.S.C. 553(b)(B)."

"The applicant or petitioner would … be required to select the 'Signature' block of his or her application or petition in order to submit it to the BCIS. The applicant or petitioner would receive a confirmation number electronically to acknowledge that the BCIS has accepted the application and electronic signature…[B]y selecting the 'Signature' block, the applicant or petitioner is certifying under penalty of perjury that the application or petition is true and correct." No provision was made for any cryptographic protection of the signatures either by the text of the regulation or the discussion of it contained in the request for comments, though the Secretary did not expressly preclude cryptographic protection either.

B. Forms Initially Selected for Electronic Filing

The Secretary did announce that the BCIS will begin deploying technology in fiscal year (FY) 2004 to enable electronic filing of all immigration and naturalization applications. The Secretary did not specifically mention any technology to be employed, and instead identified twelve of the highest volume petitions that BCIS had selected as practicable for electronic filing. These accounted for ninety to ninety-five percent of the total immigration workload annually[3] and from the list, he narrowed the initial choices to

[3] Form I-90, Application to Replace Permanent Resident Card;
Form I-129, Petition for Nonimmigrant Worker;
Form I-130, Immigrant Petition for Alien Relative;
Form I-131, Application for Travel Document;
Form I-140, Immigrant Petition for Alien Worker;
Form I-485, Application to Adjust Status;
Form I-539, Application to Extend/Change Status;
Form I-751, Petition to Remove Conditions on Residence;
Form I-765, Application for Employment Authorization;
Form I-821, Application for Temporary Protected Status;
Form N-400, Application for Naturalization; and
Form N-600/N-643, Application for Certificate of Citizenship.

two: BCIS Forms I-90 and I-765[4], discussed in more detail infra, which he stated have represented approximately thirty percent of the overall immigration workload annually.[5]

The Secretary identified Forms I-129, I-131, I-140, I-539 and I-821 as a second group of additional forms that would be electronically filed by the end of FY 2003.

The Secretary requested comment on the regulation as amended, the electronic signature program as described, and the specific selection of the two initial forms for implementation.

C. Discussion

1. The Regulation

The text of the regulation is intended to give the Secretary great latitude to experiment and design a system that implements electronic filing while at the same time being mindful of security and the stability of the immigration benefits process.[6] The terms of the regulation are very broad and only state that "an acceptable signature on an application or petition that is being filed with the BCIS is …, for applications or petitions filed electronically *as permitted by the instructions to the form*, in electronic format." (Emphasis added) Such instructions apparently have not yet been written to implement the details of electronic signatures. They presumably also will be consistent with the

[4] Forms for immigration and citizenship are available on the Internet from BCIS at http://www.immigration.gov/graphics/formsfee/forms/index.htm .

[5] The Secretary justified the selection of these two forms over the others on the grounds that they are relatively short and easy to complete and require little or no supporting documentation in paper that would have to accompany the forms; applications for renewals, replacements, or authorizations are easy to verify against existing data; and each form requires capture of a biometric (photograph, fingerprint, and signature) in connection with processing at a BCIS facility which will enable reliable verification of identity of a signer.

[6] One stated purpose is to "allow the BCIS to minimize disruptions to current business practices while it pursues the parallel strategy of integrating modern technology necessary to support *full implementation* of electronic filing for immigration and naturalization benefits." (Emphasis supplied)

discussion that is set forth in the request for comments of the Federal Register, though there appears to be no guarantee that they will be or any legal requirement for them to do so. The use of electronically filed forms or digital signatures should remain only one permissible filing method given the possible expense of electronic filing or authentication and the lack of access to technology of many applicants and petitioners.

B. The Signature Process

The request for comment narrows the scope of the electronic signature process somewhat, but also lacks sufficient specificity to understand thoroughly what is intended. Absent such details,[7] use of a Signature block should be appropriate to the formation of an electronic signature if an action by the signer is taken which logically associates the identity of a signer with the information contained in the form and an intention to be bound under oath. Such an action can be accomplished by a combination of keyboard input and mouse movements. Examples include clicking on a portion of a computer screen denominated as a signature block or typing a name into a signature block to create a signature and then clicking a submit button. Similar actions should also suffice.

The technology-neutral Federal E-Sign law does not forbid treating such computerized actions as a legal signature but it does not expressly mandate or authorize this result either; rather, such a signature is covered by the Uniform Electronic

[7]The federal E-Sign law precludes requiring a particular technology in relation to its records absent specific findings by an agency. "[A]gencies are given the authority to interpret §101(d) on retention of records by specifying standards to assure accuracy, record integrity and accessibility. The interpretive regulations may require specific formats or give special legal status or effect to the use of particular technologies if the requirement serves an important governmental objective and is substantially related to the achievement of that objective. This is limited, however, by a provision that the agency may not require use of a particular type of software or hardware in order to satisfy record-retention rules." P. Fry, "A Preliminary Analysis of Federal and State Electronic Commerce Laws,", http://www.bmck.com/ueta-esign.doc., p. 12. This requirement suggests that the vagueness of the regulation and the request for comments may have been deliberate. The Secretary may be reluctant to make such findings without first having gained practical experience with the two forms initially selected for electronic signatures.

Transactions Act ("UETA"), which has been adopted by many states, and is closely intertwined with E-Sign.[8]

The use of cryptography as a protective measure was omitted from the regulation. Though not required to create a legally binding signature, cryptography applied to the signed data in the signature process can increase the level of security of archived signed data, and there are many competing technologies that can be employed to achieve such a result. The added ease with which BCIS signature process can be extended to the bulk of other immigration forms, and the scalability of BCIS electronic signatures to other departments and agencies involving related visa issuance and citizenship decisions such as the Department of State and the Labor Department strongly suggest a role for cryptography, coupled with appropriate trust relationships.

Three basic types of cryptographic models ought to be considered. The first of these is a digital signature created by a digital certificate that has been issued to a signer by a trusted certification authority within a public key infrastructure or PKI. The technology is well understood and is offered commercially by a number of vendors. It is touted by its proponents as secure and reliable. Using PKI, a relying party can positively determine the identity of a signer, and detect any changes introduced to a document after the signature was affixed. However, critics claim that a PKI is expensive, inconvenient

---

[8] "E-Sign [itself] contains no provisions dealing with the attribution of electronic records or signatures. Frequently the issue in a dispute is not whether or not a record, paper or electronic, has been signed, but instead the issue is whose signature appears. For example, whether or not the name Patricia B. Fry appears on a record, I cannot be bound to that record if the name was not placed by me, ratified by me, or inserted by someone acting on my authority. UETA §9 states explicitly that an electronic record or signature is to be attributed to a person if it was the act of the person. This fact can be established by any relevant evidence, including by showing that some sort of technology or password was used which helps to establish who attached the signature. Section 9 also clarifies that the effect of a record or signature on the person to whom it is attributed is to be determined from the context and surrounding circumstances at the time of the creation, execution or adoption of the record. Fry, op. cit. supra, note 7 at p. 4.

for end users, administratively difficult to set up and maintain, and dependent upon identification procedures during digital certificate issuance that are generally unsuited to the kind of rigorous security required by a governmental department like Homeland Security, which is responsible for national security in times of heightened terrorist threats. Even if PKI were a preferred choice of the Secretary, he would be required by law to justify the technology specification, consistently with E-Sign.

In the request for comments, the Secretary did allude to the experience of the courts in electronic filing. Generally with few exceptions courts have abandoned or rejected the use of PKI digital certificates as impractical and unsuitable. In March 2003, two membership organizations of state court administrators, the Conference of State Court Administrators and the National Association for Court Management Joint Technology Committee, acting in concert with the National Center for State Courts approved the "Standards for Electronic Filing Processes"("the Standards"). [9] The Standards do not propose the use of PKI for court filings. Instead they recommend authentication of a filer by unspecified means, coupled with generating and saving a message digest of the filed document using a standard SHA-1 hashing algorithm specified by the US Government standard, FIPS-180. No further digital signature encryption is recommended. Without such additional encryption, it is not possible using cryptography to determine the identity of a signer. Verification of a signer's identity is unspecified by the Standards, and presumably is achieved through database records of a signer's identity that were created at the time of signature. Such records, if properly

---

[9] Available online at http://www.ncsconline.org/D_Tech/Standards/Standards.htm#ElectronicFilingProcesses .

reflective of identity at the time of signature and securely stored afterwards, could suffice to support electronic signatures, but this solution is fraught with difficulties, as discussed below.

It is true that the resulting message digest of a signed document enables automatic detection of any changes to a filed document. Given the ease with which electronic data can otherwise be altered without detection, the method recommended by the Standards is arguably an improvement over no cryptography at all. If a change is made to a document, a new message digest will no longer match the original one that was generated, even if the change is immaterial to the document's content, such as the removal of a duplicate white space from a line or paragraph. By comparing message digests, authenticity of a document version can be determined.

The method adopted by the Standards for electronic signatures has been criticized as an inadequate half-measure that fails to create document security properly.

> [T]he hash or message digest[10] can be generated by anyone through use of the hashing algorithm, which unlike encryption keys, is available generally to anyone. … The intentionally free availability of hashing resources creates a possibility of an intruder replacing a genuine hash in the database with another one of his or her making, thus tricking the system into believing a judge signed an order other than the one originally submitted.
>
> Such an attack requires an ability to break-in to the network and database to effectuate the substitution.
>
> There is a recent case documented of such an actual break-in and alteration of court records in Riverside, CA, which led to the conviction of two consultants. They pled guilty and were sentenced to nine years apiece. [11]

---

[10] The terms "message digest" and "hash" are synonymous terms that refer to the digest that results from application of a hashing algorithm like SHA-1 to a document.

[11] From: http://www.sans.org/newsletters/newsbites/vol5_6.php; some of the details of how the attacks were made and discovered are discussed at http://www.sachitechcops.com/news1115.htm:

"According to investigators, Brandon Wilson and William Grace cracked into the county's court computer system 72 times, altering Wilson's records and those of four other people to make it appear that their cases had been closed.

….

> An attacker may be able to find a back door into the network at any vulnerable point and work backwards into the systems to reach the databases. The security issues are likely to increase dramatically as the infrastructure develops and matures.[12]

By eliminating the encryption key that converts a hash into a digital signature, so the argument runs, an essential security feature is eliminated under the approach taken by the Standards, equivalent to "throwing the baby out with the bath water." Even official comments to the FIPS 180 standard, found at http://www.itl.nist.gov/fipspubs/fip180-1.htm make clear that "SHA-1 is designed primarily as a basis for digital signature creation and verification, and the use of SHA-1 as a substitute for digital signatures is not an intended use.[13]" Because the approach taken by the Standards arguably does attempt to substitute a message digest for a digital signature, so the argument continues, it is a contrarian use of the technology.

A third approach midway between a full-blown PKI and the SHA-1 method of the Standards, which blends advantages of each of them, consists of a Digital Signature Service (DSS), operated at a server, which affixes digital signatures on behalf of requestors who are properly authenticated to the server. The key or keys used to sign by the DSS can be each supported by a digital certificate from a certificate authority operating a PKI. The advantage of a digital signature service over the SHA-1 system recommended by the Standards has been articulated as follows:

"Charges included possession of illegal drugs and weapons, failure to appear in court, driving under the influence, and manufacturing and importing weapons. Officials say Wilson changed the records to show that the charges had been dismissed."

[12] See J. Messing, Security of Court Orders, http://lists.oasis-open.org/archives/legalxml-courtfiling/200305/msg00014.html.

[13] Ibid.

> Not only is the hash extracted and saved, but the hash is encrypted with a private asymmetric key. (An encrypted hash is the digital signature itself).
>
> An added advantage is that an encrypted hash is much harder to forge than a hash itself because one generally lacks the private encryption key, which unlike the hashing algorithm, is not freely available but is unique, guarded and hidden. [14]

With a DSS, it is possible for a server with a single key to sign on behalf of many requestors. Thus, a DSS with a single key, and a single certificate, allows many signers to sign documents through a sharing of the signature key. With a DSS, it should be possible in the BCIS electronic signing process to capture a message digest of a submitted electronic document and to encrypt it, creating a digital signature that is specific to the signed document. This gives needed cryptographic protection against subsequent modifications to the document and provides additional protection against an accidental or intentional destruction of the filed records.[15] With backup and encryption, the contents of an authentic filing, even though it is in electronic form and not tangible, can be established scientifically.

Such a digital signing process has been in use at the Arizona Court of Appeals, Division Two, http://www.apltwo.ct.state.az.us since September 2001. Each submitted pleading as well as all of the issued judgments are signed by the court server on behalf of the attorneys and judges. Since the method does not require digital certificates of filers or judges, the inconveniences and expense of digital certificates associated with a PKI are avoided, [16] but the private key that is used to sign all of them is linked to a digital

---

[14] Ibid.

[15] In April 2002, an incident in the California Service Center of the BCIS was reported where contract personnel allegedly destroyed filed and pending paper immigration documents without authorization. See http://www.visaus.com/02-2003update.html; http://www.testmagic.com/forum/topic.asp?TOPIC_ID=534.

[16] With a DSS, however, digital certificates can optionally be supported as a means of authenticating signers.

certificate from a commercial certificate authority and thus is part of a PKI. “A DSS thus avoids having to have end users each obtain, master, and use their own encryption keys and digital certificates, while still using digital signatures for security.” Through an additional of layer of encryption, with a DSS, signer authentication can be bound to the document itself creating a self-contained, secure document, without also requiring the use of digital certificates by signers of the DSS. This solution creates signature data redundancy securely and thus reduces dependency upon database records and network vulnerabilities which an attacker could discover and use in the forging or modifying electronic signature data at a central repository of records.

The Digital Signature Services (DSS) Technical Committee (TC) of the Organization for the Advancement of Structured Information Standards (OASIS), http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=dss, is in the process of formulating open standards for digitally signing and validating XML documents and binary files that can be embedded into XML documents using a DSS. When this work is completed, sometime in 2003 according to current estimates, a number of interoperable DSS products and services should become available on the market, possibly in time for the full blown electronic filing of immigration and citizenship applications and petitions envisioned by the Secretary in 2004. With encryption and digital signatures, the electronic filings will have enhanced security, which is one goal of the Secretary as expressed in the request for comments.

While the Science & Technology Law Section does not specifically endorse or recommend any particular method or solution, it does recommend to the Secretary that

additional consideration be given by supplementary regulation or the form instructions, to the use of encryption technologies for document security purposes.

C. Authentication and Trust Issues

In the request for comments, the Secretary noted that signers will be authenticated by trusted BCIS employees at a support center. The employees will check identity credentials before a signature is allowed to take place. The signer's immigration history will also be available to the employee. Further, the employee will capture one or more biometric identifiers during the application processing, which will also be useful as a record of authentication. The Science & Technology Law Section agrees that the Secretary has described a satisfactory method of signer authentication. It further suggests that information collected during authentication can be used to further enhance the usefulness of the electronic signing system through very simple yet effective means.

First, this identity information should be considered as a secure basis for the issuance of a digital identifier by the BCIS to an applicant or petitioner, for use in subsequent signatures in addition to the one-time signature affixed during the visit to the BCIS facility. Such a digital identifier could be a username and password, alone or in combination with the captured biometric data or an issued digital certificate. With the digital ID, the holder could theoretically sign subsequent documents electronically, even remotely over the Internet using a digital certificate or trusted DSS or other electronic signing method without a need to appear each time in person at a BCIS facility. This could result in considerable cost savings to the BCIS, provided that the risks of digital ID compromise by a signer are properly identified and steps are taken to manage the

likelihood of such an occurrence at or below a level deemed to be acceptable to the Secretary.

Second, it is also possible for the BCIS to allow attorneys who help to prepare documents on behalf of clients, voluntarily to become responsible for authenticating their clients as signers as well. Attorneys who help applicants and petitioners fill out immigration and citizenship forms are already required to file a special notice of appearance on a form G-28. With regard to the other immigration forms that they help to prepare on behalf of clients, they are also required to declare that the information contained on the form is true and correct to the best of their knowledge. This system of trusting attorneys with the document content could be extended to include signer identity as well. An attorney is able access client's identity credentials and past records at the time of signing in an attorney's presence. An authenticating attorney is thus able in ways that are similar to a BCIS employee to confirm identity during signing. Issuing a digital identifier securely to an attorney who voluntarily enrolls with the BCIS for this purpose will enable the participating attorneys who file G-28 notices of appearance to authenticate their clients to the BCIS for signature purposes using a DSS or a private key and a digital certificate issued by a certificate authority. It may be preferable to issue such a digital ID to participating attorneys than to their immigrant clients directly because disciplinary actions against errant attorneys should be an effective deterrent, while devious applicants may feel they have little or nothing to lose if they fail to act responsibly. Under this line of reasoning, an applicant will sign electronically, as described generally in the Secretary's request for comments by, for example, typing his or her name into a form in the attorney's presence, and clicking a submit button, followed by the signer's attorney

countersigning with an encryption device and affixing a digital signature to confirm the client's identity as the signer to the BCIS. The trust relationship between the BCIS and the attorney will be inherited by the client's signature through attorney's cryptographic countersignature on the submitted form. At the same time, the scope of the attorney's duties in connection with electronic documents should not be expanded beyond those in connection with paper filings. Rather, to the extent that attorney preparers of paper filing presently undertake only a limited duty of investigation, no greater duty should be imposed on those attorneys countersigning electronic forms. In this regard, limiting language similar to that already contained in the preparer's signature block on paper forms should appear on electronic forms and/or in the language of the rule itself. In addition, any attorney's participation in the digital signature process should be on a wholly voluntary basis.

Such "inherited trust" is an old and time-honored tradition in Anglo American law. Examples of "inherited trust" in paper and ink transactions include notarizations of documents transferring deeds by notaries public and authentications by court clerks regarding signed orders of a Court. Use of "inherited trust" for immigration documents could enable a rapid roll-out and wide range use of electronic signatures for a broad group of immigration and citizenship forms listed by the Secretary. Using such a system, two extremely important and widely used forms: one for family based permanent residency (form I-130) and another for adjustment of status (form I-485) could be quickly signature-enabled. Immigration and citizenship forms are generally obtainable as fill-in Acrobat forms over the Internet from the BCIS website. Paper versions are traditionally signed by the applicant or petitioner in an attorney's office, without a visit to a BCIS

support office. Any of these could be submitted electronically from an attorney's office over the Internet to the BCIS without a need for a signer to visit to a BCIS facility if electronic signatures based upon an attorney's authentication and encrypted counter-signature were allowed to serve as valid electronic signatures for immigration signing purposes.

With regard to BCIS forms that are used for visa processing at a US Consulate, such as the I-130 form for family based permanent residency and the I-140 form for employment based permanent residency, encrypted signatures based upon "inherited trust" could enable rapid processing by other US government agencies, including the National Visa Center and US consulates abroad, following initial BCIS approvals. Encrypted signatures from attorneys could be remotely verified by such other agencies, whether generated by a PKI digital certificate or a DSS, using recognized encryption verification procedures, thus accelerating the processing times and further increasing the benefits of the Paperwork Reduction Act. Without endorsing any encryption product or method, the Science & Technology Law Section recommends that the Secretary give consideration to "inherited trust" encrypted signatures from attorneys who have filed G-28 forms with the BCIS and have voluntarily agreed to provide such client authentications as part of the Secretary's program to use electronic signatures.

D. Initial Form Selections

The Secretary picked as candidates for the first electronic signatures the form I-90, which is used to replace expired or lost permanent resident cards, and the form I-765, which enables employment of petitioners and beneficiaries during immigration processing. The Science & Technology Law Section believes that the Secretary's

selection of these two forms is suitable as a beginning step towards comprehensive electronic filing. Neither form initiates a process to obtain immigration benefits. The form I-90 only applies to permanent resident applications that have been approved in the past. Therefore, the risk that a benefit will be erroneously conferred upon an applicant or beneficiary through an error generated by using the technology is reduced for this form, since the basis for initial issuance already was conferred using paper. Similarly, the form I-765 for work authorization can only be approved in conjunction with another request for another, more substantive immigration benefit, such as permanent residency. Here too, the risk of conferring an important immigration or citizenship right erroneously through an error the use of the technology is diminished by the Secretary's choice of forms. Since the benefit of work authorization is collateral to a paper-filed form, it can be rescinded in the event of error without interfering with the principal immigration benefit processing.

In both cases, trips to an immigration sub-office or support center are invariably required to confer the immigration benefit, during which photographs are checked or taken and fingerprints are also generally taken.

In both cases, rapid delivery of the immigration card is important to the applicant or beneficiary. For replacement permanent resident cards, quick servicing minimizes personal disruptions that can be occasioned by the absence or unavailability of important immigration papers in the possession of alien; while in the case of the employment authorization, severe economic consequences are minimized by rapid servicing of applications. The alien is allowed to work legally while the application for the principal immigration benefit is processed.

However, as described above, these two immigration forms are somewhat different from many of the other forms that the Secretary has targeted for rapid conversion to electronic signatures, which do involve procedures for awarding substantive immigration benefits, such as the I-140 (permanent residency for foreign workers); the N-400 (naturalization) and the I-129 (non-immigrant visas for foreign workers). Because these forms raise other, more serious security issues and potential consequences to both the BCIS and the alien in the event of errors, the Science & Technology Section recommends to the Secretary that at least one more additional form be added to the list of forms to be electronically signed initially, which will include a substantive immigration benefit. Lessons learned from the experience of processing such a form electronically will be immediately useful to the other forms the Secretary has stated an intention to begin processing electronically by the end of 2003.

E. Conclusion

Consistently with the comments set forth in this response to the request for comments, the Science & Technology Law Section believes the Secretary has stated a persuasive case for electronic filing of immigration applications in the request for comments, and has taken a useful first step in proposing to begin electronically filing of immigration forms I-90 and I-765.

Sincerely,

John Messing
Chairman, Electronic Filing Committee