U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES

FOOD AND DRUG ADMINISTRATION

ELECTRONIC IDENTIFICATION/SIGNATURE WORKING GROUP

PROGRESS REPORT - FEBRUARY 24, 1992

(Reformated November, 1996)

ELECTRONIC IDENTIFICATION/SIGNATURE WORKING GROUP

PROGRESS REPORT - FEBRUARY 24, 1992

CONTENTS:

ELECTRONIC IDENTIFICATION/SIGNATURE WORKING GROUP

PROGRESS REPORT - FEBRUARY 24, 1992

EXECUTIVE SUMMARY:

This is the first report of the Electronic Identification/Signature Working Group, a sub unit of the Electronic Identification/Signature Task Force which was formed at the direction of the Office of the Commissioner to consider (1) issues attendant to electronic identification in the pharmaceutical industry, and (2) proposed standards for digital signatures. Preliminary research revealed that the issues, and regulations potentially affected, extend across center lines to virtually all parts of the agency. Electronic endorsements are considered within the context of electronic records.

We considered the issues as they relate to three types of electronic documents which may contain alternatives to conventional signatures: records maintained by the regulated industry, records submitted to the agency for review, and records prepared by the FDA itself. Also of interest is what other federal agencies are doing in this area; we found different approaches but similar concerns about legal acceptance and assurances of authenticity.

We identified seven key issues and determined the following:

1. Legal Acceptance - Legal acceptance of signature alternatives is vital. We have found no deterrents to admissibility of electronic records. However, concerns for authenticity assurances are prominent. We found Justice Department guidelines that could be useful.

2. Regulatory Acceptance - Agency centers have different degrees of acceptance for signature alternatives. The drug CGMP regulations do not permit such alternatives and would need codified changes to allow them. Prescription Drug Marketing Act regulations are still evolving but lean toward adoption of signatures recorded electronically, but not signature substitutes. Devices CGMPs vary but call for signatures on master records.

3. Enforcement Integrity - Our enforcement activities must not be hampered by signature alternatives. Inspectional problems have not yet surfaced but may be encountered in the future. Sufficient legal tools exist under Title 18 of the U.S. Code to pursue cases of electronic records falsification.

4. Validation/Reliability - Validation and reliability of signature alternative technologies are vital and the agency may need to issue guidance documents in this area in the future; computer system validation has been problematic in the pharmaceutical/medical device industries.

5. Security - Security of signature alternatives is vital, especially because electronic identification is more liable to undetected falsification than conventional signatures, a weakness recognized by the courts. We found security measures in federal guidelines that we may apply to industry.

6. Standards - While we recognize their utility, practical standards for electronic signatures have yet to be developed. The Digital Signature Standard proposed by the National Institute for Standards and Technology is not suitable for adoption by FDA at this time.

7. Freedom of Information - New administrative procedures and fees may need to be established to handle FOI requests (some submitted in electronic form) for electronic documents.

Our primary recommendations are federal register publication of an advanced notice of proposed rulemaking to gather the widest possible public comment on the myriad of complex issues attendant to electronic identification, and appropriate follow-up publication of regulations and guidance documents in order to accommodate electronic identification/signatures in a manner consistent with our regulatory responsibilities.

The group is continuing to gather information which will be provided in subsequent supplementary reports.

BACKGROUND:

The Electronic Identification/Signature Working Group was formed on November 26, 1991, from the Electronic Identification/Signature Task Force. The task force, made up of representatives from each agency unit, was created in response to industry correspondence to the Office of the Commissioner **[1]**, regarding electronic identification issues in the pharmaceutical industry, particularly within the Current Good Manufacturing Practice (CGMP) Regulations, and as a follow up to emerging federal standards on digital signatures **[2]**. By memo of November 12, 1991, Ms. Mary Jo Veverka, Office of the Commissioner, Senior Advisor for Management and Information (HF-20), requested Mr. William T. Lampkin, Director of the Division of Compliance Policy (HFC-230), to form an agency wide working group to determine what is needed for FDA to be able to accept electronic identification and to identify the attendant issues **[3]**. The overall task force was organized by Mr. Lampkin by his memo of November 20, 1991 **[4]**, and held its first meeting on November 26, 1991 and each major agency unit presented its preliminary thoughts and approach on the issues **[5]**.

It became clear from that preliminary meeting that the issues on electronic identification (electronic signatures) were complex, varied, encompassed far more than human and veterinary drug CGMPs, and potentially involved regulations managed by every center in the agency, especially if some reasonably uniform agency wide policies were to be applied to acceptance of substitutes for handwritten signatures. For example, a search was conducted for the words "signature", "signatures", "sign", or "signed" in the FDA-ON CD-ROM database to assess the scope of accepting electronic signatures in lieu of conventional signatures called for in various regulatory documents. That search found that one or more of the words occurred in 733 documents, including 384 occurrences in the Code of Federal Regulations (331 in 21 CFR in a total of 164 different sections [132 sections under FDA management and 32 sections under DEA management]), and 8 in the Food, Drug and Cosmetic Act **[6]**. Interestingly, the search did not disclose a definition of the word signature.

Mr. Lampkin thus appointed a sub group, the Electronic Identification/Signature Working Group, to address the issues from the various agency perspectives and to present its findings at a subsequent task force meeting.

WORKING GROUP COMPOSITION:

The Electronic Identification/Signature Working Group is composed of the following individuals:

Mr. Paul J. Motise, CDER, HFD-323, Chairperson
Mr. Martin Browning, ACRA/ORO, HFC-131, Vice Chairperson
Mr. Tom M. Chin, ACRA/OE, HFC-230
Mr. Seth Ray, OGC, GCF-1
Mr. Boyd Fogle, Jr. CBER, HFB-120
Ms. Jo Gulley, CVM, HFV-226
Ms. Christine Nelson, CDRH, HFZ-332[1]
Mr. David R. Hamrick, OMO, HFA-51
Mr. Len Valenti, CFSAN, HFF-310[2]

DEFINITION OF TERMS:

The working group believes it is necessary to distinguish and define the terms signature, electronic identification, electronic signature, and signatures recorded electronically. At this point we suggest the following:

Signature: A signature is the name of an individual, handwritten in script by that individual. The act of signing with a writing or marking instrument such as a pen, pencil, or stylus is preserved. However, the scripted name, while conventionally applied to paper, may also be applied to other devices which, like paper, capture the written name **(signatures recorded electronically)**. The act of signing serves as an intrinsic behavioral link to the signer.

Electronic Signature: An electronic signature is a non-handwritten unique means of identifying an individual, which has an intrinsic biometric or behavioral link to the individual which remains with the individual such that other persons cannot apply the electronic signature. Examples of electronic signatures include retinal scan systems, voice prints, and hand prints.

---

[1] Ms. Nelson replaced Mr. Byron Tart, the original CDRH representative, and was not present at the Nov. 26, 1991 meeting.

[2] Mr. Valenti replaced the original representative, Dr. Vir Anand, HFF-335, subsequent to the Nov. 26, 1991 meeting.

Electronic Identification: Electronic identification is a means of identification which lacks an intrinsic biometric or behavioral link to the person being identified. Uniqueness of the identification is predicated upon a system of administrative controls. Examples of electronic identification include passwords/identification codes, bar codes, and personal identification codes.

For purposes of this document we will term electronic identification and electronic signature as signature alternatives (SA's).

PRIMARY AND SECONDARY AREAS OF CONCERN:

At this point the working group perceives three primary and one secondary areas of general concern in the application of electronic identification (i.e. non-handwritten signatures/initials) and electronic signatures.

First, we are generally concerned about application of signature alternatives (SA's) in documents which our regulated industry must maintain as part of day to day operations, documents which are subject to FDA inspection. For example, such documents are required by the Current Good Manufacturing Practice (CGMP) regulations for human and veterinary drugs, medical devices, and biologics, and the Good Laboratory Practices regulations. Application of signature alternatives in the drug CGMP regulations is what precipitated this agency project. However, many other regulations, as disclosed by the FDA-ON CD-ROM search, also require firms to execute signatures in various production/control and investigative records.

Second, there is the area of official records submitted by the regulated industry to FDA for review and approval, usually as part of research or marketing applications. For example, the issue of acceptability of SA's has come up in connection with computerized new drug applications (CANDAs), abbreviated new drug applications, and food additive petitions. Generally, signatures on these documents provide certification of data or authentication of submitted records.

Third, there are FDA's own internal documents, some administrative, some regulatory, which are increasingly being subject to automation. For example, sample collection reports and analytical work sheets represent regulatory documents which might contain SAs instead of conventional signatures. Electronic mail, by its nature, does not accommodate conventional signatures and is ripe for some sort of alternative; this area will gain in significance as the agency expands its electronic communication to the regulated industry.

A secondary consideration of the working group is what other federal agencies are doing in the area of signature alternatives. Whereas we do not believe it necessary to

delay FDA decisions until other agencies have acted, and FDA would not be bound by the policies of other agencies, it is nonetheless useful to know how other agencies have approached or resolved the issues.

Although the group does not have routine liaison with other federal agencies, available information from direct phone contacts **[7]** and published articles indicates a variety of approaches and general sharing of the fundamental legal concerns we have, particularly about the absence of physical signatures in electronic records **[8][9]**. Experiences of other parts of the federal government have interesting parallels to FDA's programs, as follows:

The Internal Revenue Service believes that the current law does not allow it to accept a digital signature in place of a hand written signature. The IRS requires a paper trail and maintains both electronic and paper submissions until another method is developed.

The U.S. Customs Service reportedly allows Customs house brokers to access the Customs Service electronically in order to handle import transactions; 30 percent of all transactions are paperless and the captured data is used for tariff collection, and enforcement of trade laws and regulations for numerous agencies **[10]**. Thus, significant paperless electronic submissions are accepted by the regulating agency, whereas most transactions retain some paper records.

The Treasury Department has plans to allow banks to bid on U.S. Treasury securities electronically; system security is a concern, and bidders will have to furnish written verification of offers **[11]**; the critical nature of the electronic action apparently necessitates the security of paper verification.

The Interstate Commerce Commission permits rail carriers to file tariffs electronically but experienced a resource problem in not having sufficient computer equipment to read the electronic submissions; the problem was address when, under General Accounting Office guidance on the ethics of having industry provide the government with the needed equipment, rail carriers furnished the necessary hardware **[12]**. The group notes that an analogous situation exists in FDA where NDAs are filed electronically on optical disks and the agency lacks equipment to read those submissions.

The Federal Communications Commission is planning a system enabling electronic filing of applications for radio broadcasting licenses (the FCC reportedly receives more than one million applications each year) **[13]**. Here, it appears that high volumes of submissions drive the need to accept efficiencies attendant to electronic submissions.

The Department of Defense is looking to replace some paper inventory forms with

electronic records generated by "pen-based" computers, although the legal validity of signatures generated by such equipment is a concern **[14]**.

The Securities and Exchange Commission has an electronic data interchange system for electronic filing of critical registration and disclosure documents. Paper filings are not required. Participants need a Personal Identification Number for signing documents, as well as a password. Encryption of the signature or the data is not required.

The Department of Transportation established an electronic data interchange system in December of 1989 regarding international airfare information. The system was tested for nine months during which backup paper submissions were required. Currently, the system is being used without paper submissions. Passwords are assigned to each individual who requires access to the system. Airfares are approved or disapproved electronically. This system requires initials as well as passwords for certification and validation of data.

The General Accounting Office issued a December 13, 1991 "Decision" paper, stating that federal agencies could create valid contractual obligations, for purposes of 31 U.S.C. Section 1501, by using Electronic Data Interchange technologies, provided the technology used provides the same degree of assurance and certainty as traditional "paper and "ink" methods of contract formation **[15]**. This paper echoes the concerns for security, and notes the need to prevent fraudulent alteration of the terms of an electronic contract.

ISSUES:

We consider the following to be key issues in accepting signature alternatives:

I. LEGAL ACCEPTANCE:

It is vital that the agency conform to judicial acceptance and qualifications regarding signature alternatives. Any accepted alternative should be viewed by the courts as equivalent to conventional signatures. The alternatives should carry the same commitment, legal weight, and significance as conventional signatures. Furthermore, falsification of signature alternatives should be considered to be fraudulent to the same extent as is falsification of conventional signatures.

In reviewing this issue, it may be useful to consider how signature alternatives may conform with three primary functions of the conventional "autographical" signature. First, the signature identifies the actor and shows the authority to act. The signature

alternatives defined above (electronic signatures and electronic identification) may meet this function where administrative controls link the signature alternative to an individual by (for example) cross references.

Second, the signature documents the terms of the action in a manner that is legally binding and cannot be repudiated. The group considers that author repudiation would be much more difficult for electronic signatures, than for electronic identification, as defined above. Although legal precedence has yet to be encountered, it is the opinion of the group that electronic signatures would likely be more legally binding, by virtue of their security and non-transferability, than electronic identification.

Third, the signature creates a record traceable during investigations and admissible in court. By administrative controls and cross references, it is possible that signature alternatives would provide record traceability, although some complexity may hamper that effort. The admissibility of such a record remains a question.

Mr. Seth Ray, the GC representative, has conducted a comprehensive legal search to see if there are court cases and decisions that would clarify the legal acceptance of signature alternatives. No such cases or decisions were disclosed.

Thus far, we have identified two documents published by the Justice Department, which shed some light on the subject. First, the document titled "Admissibility of Electronically Filed Federal Records As Evidence" **[16]**, which does not speak to signature alternatives, per se, does note that the courts recognize the use of computerized (electronic) business records. An important point made by the document is that computer printouts should be received as evidence of the transactions covered by computer input, once the reliability and trustworthiness of the information put into the computer have been established -- the group believes that for FDA purposes, this point emphasizes the importance of system validation. The document also discusses the importance of laying a proper foundation for records admissibility because electronic files are particularly susceptible to purposeful or accidental alteration, or incorrect processing. Proper control over creation and maintenance of electronic files is emphasized. (Thus, there is emphasis on system security and the apparent acknowledgement that computerized systems may be more prone to falsifications than paper systems.) It is interesting to note that the document's reference to signatures is within the context of "genuine" (conventional) signatures used to authenticate electronic records (pg. 9 of the reference). This document is of interest not only to FDA, but also to other regulatory agencies **[17]**.

The second Justice Department document, published in 1988, is titled "Basic Considerations in Investigating and Proving Computer-Related Federal Crimes **[18]**. The document notes that an American Bar Association survey included, as the most

significant types of computer crimes, use of computers to destroy or alter data, and defraud consumers, investors or users. Of relevance to this project is the identification of impersonation as a means of executing computer related crimes. The following excerpt (pg. 2-5 of the reference) regarding falsified identification would apply to "electronic identification", as defined above, but would be very difficult to apply to "signatures recorded electronically", or conventional signatures:

> "Impersonation is the process of one person assuming the identity of another. Physical access to computers or computer terminals and electronic access through terminals to a computer require positive identification of an authorized user. The verification of identification is based on some secret password; something the user is ...; and something the user possesses, such as a magnetic stripe card or metal key. Anybody with the right combination of identification characteristics can impersonate another person."

The working group considers that it would be easier for an individual to falsify a computerized endorsement/verification (such as might be applied to an electronic batch production record) by use of electronic identification than it would be by use of electronic signatures or conventional signatures.

The legal admissibility of electronic records is addressed by an industry paper which echoes the concerns that court acceptance of such records will hinge upon their trustworthiness as demonstrated by an audit trail, documented procedures, and program documentation **[19]**.

The legal admissibility of FDA's own electronic records is addressed (within the context of such records maintained by all federal agencies) in a document published January 30, 1991 by the General Services Administration titled "Federal Information Resources Management Regulation Bulletin B-1" **[20]** Judicial use of electronic records is covered on pages 5 and 6, where the following procedures are identified to enhance legal admissibility:

> 1. Documentation that similar records are created consistently by the same procedures and that standardized retrieval methods are used.
>
> 2. Substantiation that security procedures prevent unauthorized addition, modification, or deletion of records.
>
> 3. Identification of electronic storage media, maximum storage time limits, and National Archives and Records Administration (NARA) approved disposition methods.

The FIRM Bulletin also calls for the following security measures:

1. Assurance that only authorized personnel have access to electronic records.

2. Back up and recovery procedures to protect against information loss.

3. Employee training in the safeguard of sensitive or classified electronic records.

4. Minimized risk of unauthorized alteration or erasure of electronic records.

5. Assurance that electronic records security is included in computer systems security plans prepared pursuant to the Computer Security Act of 1987 (40 USC 759).

The legal status of FDA's own electronic records is further addressed in the PHS IRM Manual **[21]** which states that PHS components would be helped in substantiating the authenticity of such records by adhering to the following guidelines:

1. Appointing an administrator for each system who is

   - o identified by job title rather than name;

   - o a management level employee involved with some aspect of system operation, but who may also have other responsibilities with legal implications, such as control over release or expungement of data;

   - o sufficiently familiar with the entire system to be able to give testimony.

2. Documenting system hardware and software features by:

   - o listing all brands and models of equipment components;

   - o listing dates hardware was put into or removed from service;

   - o obtaining technical specification sheets for all equipment;

   - o keeping records of repair and maintenance;

   - o listing source code, flow charts, debugging procedures for custom-developed programs;

o maintaining record version numbers, upgrades, implementation dates for purchased software.

3. Documenting all record-creation procedures to show that records are being maintained electronically in the regular course of business (as opposed to having been created specifically for a specific court appearance) by maintaining:

o workflow diagrams and written procedures for all equipment operators;

o input verification and validation procedures;

o logbooks to record names of equipment operators on specific dates.

4. Documenting the administrative, technical, physical and procedural safeguards.

5. Auditing all aspects of system operation on a regular basis for compliance with established procedures, and documenting the audit findings, and the implementation of corrective actions.

The group believes that the above security and legal acceptance measures, in both federal documents, could be applied by appropriate guidance documents or regulations to electronic records maintained by the regulated industry and/or submitted to FDA.

II. REGULATORY ACCEPTANCE:

Acceptance of signature alternatives, at least as a means of identifying individuals in records produced by the regulated industry, is not uniform in the various regulations managed by the different centers. For example, as described in CDER's section of this report, the CGMP regulations for human and veterinary drugs contain some sections which explicitly require handwritten signatures, some which call for signatures or initials, and some which implicitly (and by agency experience, precedent and compliance program instructions) require signatures or initials without actually using the words signature or initials. (See also reference 6 for a listing of regulations which contain the words signature, signatures, sign or signed.) Likewise, as described in CDRH's section of this report, various records submitted to the agency are explicitly required to be signed; interestingly, 21 CFR 1005.25, regarding designation of a foreign manufacturer's U.S. agent, requires all signatures to "be in ink". On the other hand, CFSAN, within the context of the low acid canned food regulations, accepts computer encoded methods of endorsement where the regulations call for identification of employee actions.

The working group recognizes the practical need to accommodate the differences among the various centers. However, it would be preferable to attain whatever degree of uniformity we can in regulatory acceptance of signature alternatives. It may be desirable to adopt a multi-tiered approach to regulatory acceptance of signature alternatives, where those documents of the highest regulatory significance must be signed by conventional autographic signatures or electronic signatures, and documents of lesser importance could contain less secure signature alternatives.

III. ENFORCEMENT INTEGRITY:

It is the consensus of the working group that whatever approach the agency takes to signature alternatives, the integrity of our enforcement efforts should not be hampered. For example, we should still be able to obtain copies of electronic records which would be admissible evidence in regulatory actions. The importance and legal acceptance of any signature alternatives in those records must not dilute the agency's ability to document individual responsibility and affix that responsibility in court, as we have done historically with paper records and conventional signatures.

The group has found that there are no cases which clearly endorse signature alternatives. At the same, time there are no cases which would impede our approach to their qualified acceptance.

Having adequate legal recourse to pursue electronic records falsification is a prime concern. The group is of the opinion that existing statutory requirements should provide the agency with sufficient legal tools to obtain sanctions against wrong doers, even in the absence of specific federal forgery statutes. Specifically, the following sections of Title 18, U.S. Code may be useful:

> Section 1001 - Statements or Entries Generally; these federal fraud and false statement provisions prohibit making or using false documents under agency jurisdiction;
>
> Section 1343 - Fraud by Wire, Radio, or Television; the development of further case law is needed before FDA can charge wire fraud in relation to interstate electronic submissions to the agency (e.g., electronic NDAs) because of a need to show use of electronic communication in furtherance of a scheme to deprive an individual or entity of money or property; these provisions would not generally be applied in the case of electronic records maintained by a firm (e.g., batch production records).
>
> Section 371 - Conspiracy to Commit an Offense or to Defraud the United States; this section can be an effective enforcement tool in situations

where two or more persons agree to create or use false or fraudulent electronic identification/digital signatures in a matter within the agency's jurisdiction.

Section 1505 - Obstruction of Proceedings Before Departments, Agencies, and Committees; these provisions may be appropriate for incidents of false or fraudulent electronic identification/digital signatures that arise during FDA investigations or administrative proceedings.

Section 1030 - Fraud and Related Activity in Connection with Computers; it appears some provisions could be used to prosecute individuals or entities who "traffic" in computer passwords (or similar information through which a computer may be accessed without authorization) that may result in false or fraudulent electronic identification/digital signatures.

A more comprehensive discussion of these provisions is given in the General Counsel's comment section of this report.

IV. SECURITY:

It is vital that signature alternatives be secure. Whereas we recognize that any system can be corrupted and defeated by those intent on falsification, substitutes for conventional signatures should nonetheless be at least as secure as conventional signatures. Considering the ease with which some electronic identification methods can be falsified without leaving an audit trail, some signature alternatives may be inherently less secure and therefore should not be accepted by the agency. (For example, at this point, CDER is not accepting bar codes and user identification code systems (electronic identification) as signature substitutes, and is deferring action on electronic signatures, in the area of the Prescription Drug Marketing Act (PDMA) **[22]**. Electronic recording of signatures is being accepted in the proposal.

V. VALIDATION:

The reliability of signature alternatives must be validated. Inadequate or entirely lacking computer system validation has been a problem detected by our field investigators. Thus, validation would have to be a significant factor in acceptance of any signature alternatives. The agency may need to develop specific guidance on validation of signature alternative systems in the future.

VI. STANDARDS:

The agency's acceptance of signature alternatives would be facilitated if FDA could apply appropriate signature standards developed by other organizations. The recognition and adoption of public standards is consistent with the agency's regulatory approach (e.g., pharmaceutical compendial standards [United States Pharmacopeia/National Formulary] are recognized in the FD&C Act. Thus, the group reviewed with interest, the proposed NIST Digital Signature Standard. Whereas the working group recognizes the potential benefits of scientifically sound signature alternative standards, we find that the NIST Digital Signature Standard does not meet our needs because of it's password/id nature (vulnerable to misuse through being lost, stolen or shared, misuse that would not be detectable by examination of the signature itself), the fact that it may be an unreasonable and inflexible burden to place on industry and FDA at this time, and because of reports of its controversial nature **[23] [24]**. Most significant is a report that NIST's own advisory group, the Computer Security and Privacy Advisory Board, has gone on record as opposing the draft standard **[25]**.

By memo of February 20, 1992, the agency advised the Public Health Service that the proposed NIST standard is not a viable digital signature standard, currently, for the regulated industry or for FDA **[26]**.

VII. FREEDOM OF INFORMATION:

The agency receives the vast majority of freedom of information (FOI) requests in paper form, where paper documents in possession of the agency are furnished to requestors consistent with legal requirements. The agency has very limited experience with requests that are submitted electronically, where documents at issue are in electronic form, or where documents in electronic form are requested to be furnished in electronic form.

The working group believes that several matters need to be addressed in this area. For example, administrative fees for researching, purging (as needed), and copying electronic records may need to be established, fees which reflect costs that differ from those involved in handling conventional paper forms (e.g., will requestors provide FDA computer disks to capture the electronic documents or will FDA have to furnish the disks?).

Where electronic documents must be purged of non-disclosable information it is vital that the electronic form of document storage permit such deletions. This may not be possible where documents collected by the agency are in an electronic form that requires special equipment to replicate and alter.

The electronic form of documents may also permit some efficiencies, however. For instance, administrative overhead involved in processing individual FOI requests for previously released electronic documents may be reduced if such documents are placed into an electronic database accessible by the general public; automation could, in theory, manage access fees and tracking. A multi-agency task force is reportedly working on a draft model policy to address the basic concept of public access to federal electronic records; security is a major concern **[27]**. At any rate, the group foresees opportunities for creative uses of such a project and suggests that agency FOI managers consider planning for such a program.

ADDITIONAL COMMENTS FROM MEMBERS OF THE WORKING GROUP:

THE OFFICE OF THE GENERAL COUNSEL:

(By Seth Ray, GCF-1)

As you are aware, FDA regulated industries are developing electronic identification/digital signature computer systems for use in a variety of applications that directly affect several agency responsibilities (e.g., "paperless" drug manufacturing and control systems, remote data entry of clinical trial data, pen-based computer grid pad systems for use in drug sample distribution, computer assisted new drug applications, etc.) The agency is concerned that some of these systems are inappropriate signature substitutes and lack the security and legal acceptance of conventional handwritten signatures. More importantly, fraudulent use of such alternatives might not be viewed in the same manner as fraudulent conventional signatures, thereby frustrating our enforcement responsibilities and resulting in increased instances of records falsification. This section discusses the statutory provisions that are available to support enforcement action in cases of false or fraudulent electronic identification/digital signatures.

We are aware of only two federal court decisions which pertain to electronic identification systems. Computer Identics Corp. v. Southern Pacific Co., 756 F.2d 200 (1st Cir. 1985) (an action under the Sherman Antitrust Act, 15 U.S.C. § 1, alleging a conspiracy to restrain trade in a computerized system for automatically identifying railroad cars (ACI)); Sylvania Electric Products v. Brainerd, 369 F. Supp. 468 (D. Mass. 1974) (a patent infringement/validity action involving ACI).

Although there are no reported cases in which the federal government has taken legal action against individuals/entities for making or using false or fraudulent electronic identification/digital signatures, in many respects, the laws that will bear upon these cases in the "electronic world," are the same as those that have applied in the "paper world." Although there is no general federal forgery statute,[3] there are a number of

[3] The federal forgery statutes only pertain to government obligations or securities, foreign obligations or securities, foreign bank notes, coins, bars, bonds and obligations of certain lending agencies, contractors' bonds, bids, public records, contracts, deeds, powers of attorney, writings pertaining to customs matters, letters patent, military discharge certificates
or official passes, money orders, postage and revenue stamps, postage meter stamps,

statutes to draw on in dealing with crimes involving computers. Following is a summary of these criminal statutes and their application to cases involving false or fraudulent electronic identification/digital signatures:

18 U.S.C. § 1001 - Statements or Entries Generally

In a very sweeping criminal statute, federal law proscribes the making of any false, fictitious, or fraudulent statements or representations in connection with federal government affairs.

Title 18, U.S.C. § 1001, provides that:

> Whoever, in any matter within the jurisdiction of any department or agency of the United States knowingly and willfully falsifies, conceals or covers up by any trick, scheme, or device a material fact, or makes any false, fictitious or fraudulent statements or representations, or makes or uses any false writing or document knowing the same to contain any false, fictitious or fraudulent statement or entry, shall be fined not more than $10,000 or imprisoned not more than five years, or both.

Title 18, U.S.C. § 1001, technically describes three separate offenses concerning any matter within the jurisdiction of a department or agency of the United States:

a. Falsifying, concealing, or covering up a material fact by any trick, scheme, or device.

b. Making false, fictitious, or fraudulent statements or representations.

c. Making or using any false writing or document.

The above acts are criminal if there is an affirmative response to each of the following questions:

a. Was the act material?

---

postal cards, postmarking stamps, seals of courts, signatures of judges or court officers, seals of departments or agencies, ship's papers, government transportation requests, and endorsements on Treasury checks, bonds, or government securities. 18 U.S.C. §§ 471-513.

b. Was the act within the jurisdiction of a department or agency of the United States?

c. Was the act done knowingly and willfully?

The federal courts have interpreted 18 U.S.C. § 1001 broadly. The discussion which follows is primarily limited to offenses involving false statements or representations, and false writings or documents.

The false statement may be written or oral, sworn or unsworn, voluntary or required by law, signed or unsigned. Title 18, U.S.C. § 1001 does not require that the false statement be made directly to the federal government. United States v. Uni Oil Co., 646 F.2d 946 (5th Cir. 1981), cert. denied, 455 U.S. 908 (1982). False statements warranting prosecution may be made in at least three ways:

a. Directly to a federal agency.

b. To a private person or institution which implements federal programs.

c. To one's self, as false statements in business records which may be subject to federal government inspection.

A false statement is a "matter within the jurisdiction" of a federal agency if:

a. The agency had the power to act on the statement. United States v. DiFonzo, 603 F.2d 1260 (7th Cir. 1979);

b. There is an "intended" relationship between the act and the federal government. United States v. Stanford, 589 F.2d 285 (7th Cir. 1978); or

c. The act was calculated to induce government action. United States v. Barbato, 471 F.2d 918 (1st Cir. 1973).

The courts have held that 18 U.S.C. § 1001 does not require:

a. Any financial or property loss to the federal government. United States v. Richmond, 700 F.2d 1183 (8th Cir. 1983).

b. Any favorable agency action. Brandow v. United States, 268 F.2d 559 (9th Cir. 1959).

c. Reliance by the government on the false statement or document. United States v. Lichtenstein, 610 F.2d 1272 (5th Cir. 1980).

d. Proof of the defendant's knowledge of federal agency jurisdiction. United States v. Yermian, 468 U.S. 63 (1984).

To commit an act "knowingly" as used in § 1001 requires only that the defendant acted with knowledge, United States v. Mekjian, 505 F.2d 1320 (5th Cir. 1975), and not because of mistake, accident, or some other innocent reason. An act is done "willfully" if the defendant acted "deliberately and with knowledge." Id. at 1324.

The word "material" is not used in the statute with respect to false statements and false documents, but only in the first clause regarding a trick, scheme, or device. This has generated a conflict between the circuit courts of appeal as to whether proof of materiality is required when a false statement or document is charged. The Second Circuit Court of Appeals requires proof of materiality only for the first clause of the statute. United States v. Rinaldi, 393 F.2d 97 (2d Cir.) cert. denied, 393 U.S. 913 (1965). However, the majority and better view is that the element of materiality pervades the entire statute. See, e.g., United States v. Adler, 623 F.2d 1287 (8th Cir. 1980); United States v. Lichtenstein, 610 F.2d 1272 (5th Cir. 1980). As a practical matter, because a false statement or document must be a meaningful one to have a convincing case, the sensible solution is to allege and prove materiality. The test for determining the materiality of the falsification is whether the falsification had a natural tendency to influence, or was capable of influencing the agency or department. United States v. East, 416 F.2d 351 (9th Cir. 1969).

False or fraudulent handwritten signatures, by themselves, can form the basis for criminal prosecution under 18 U.S.C. § 1001. See, e.g., United States v. Corsino, 812 F.2d 26 (1st Cir. 1987) (conviction under 18 U.S.C. § 1001 affirmed; false signatures of supposed recipients of funds under Department of Housing and Urban Development home rehabilitation grant were material even if not specifically required by the agency); United States v. Cole, 469 F.2d 640 (9th Cir. 1972) (conviction under 18 U.S.C. § 1001 affirmed against a civilian employee at a military installation who forged a signature on a requisition form); Gilbert v. United States, 359 F.2d 285 (9th Cir. 1966) (conviction under 18 U.S.C. § 1001 affirmed against an accountant who forged his clients' endorsements on their federal income tax refund checks).

We are aware of only one reported case brought under 18 U.S.C. § 1001, in which false information was furnished to the government electronically. The defendant in United States v. Blair, 886 F.2d 477 (1st Cir. 1989), was found guilty of broadcasting false radio distress signals to naval aircraft in violation of 18 U.S.C. § 1001. The court

of appeals affirmed the conviction.

Despite the paucity of cases involving false electronic statements or representations under 18 U.S.C. § 1001, this law is so broadly worded and expansively interpreted by the courts, it should cover almost any false or fraudulent electronic dealings with the government. Clearly, a false or fraudulent handwritten signature (on paper) constitutes a false statement/representation and a false writing for purposes of § 1001. Similarly, a convincing argument can be made that a false or fraudulent electronic identification/digital signature is a false representation and causes the making of a false writing (a computer printout), to support a prosecution under § 1001.

The issue of "materiality" (previously discussed) may present a problem for some false or fraudulent electronic identification/digital signature cases. An argument can be made that a false electronic signature in a submission to the agency (e.g., NDA, ANDA, etc.) or in records that are maintained by regulated industry (e.g., "paperless" drug manufacturing systems), is not material. In other words, it should not matter to the agency who signs a submission or record, as long as it is signed by someone associated with the firm. However, we do not believe that this argument is particularly persuasive in light of the test for materiality previously discussed and the importance of credible recordkeeping and submissions to the agency's mission.

Title 18, U.S.C. § 1001 is by far the most useful statute for prosecuting cases of false or fraudulent electronic identification/digital signatures that arise in matters within the agency's jurisdiction.

18 U.S.C. § 1343 - Fraud by Wire, Radio, or Television

The wire fraud statute, 18 U.S.C. § 1343, provides in part that:

> Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, shall be fined not more than $1,000 or imprisoned not more than five years, or both.

To establish a violation of 18 U.S.C. § 1343, the following elements must be proved beyond a reasonable doubt:

a. The devising of a scheme and artifice to defraud, and

b. A transmittal in interstate or foreign commerce by means of wire, radio, or television of writings, signs, signals, pictures or sounds for the purpose of executing the scheme and artifice to defraud.

Inasmuch as the statute requires a transmission in interstate or foreign commerce, an intrastate transmission does not constitute an offense. Boruff v. United States, 310 F.2d 918 (5th Cir. 1962). Each use of the interstate instrumentality (wire, radio, or television) constitutes a separate offense. United States v. Calvert, 523 F.2d 895 (8th Cir. 1975).

In 1987, the United States Supreme Court decided a case that significantly affects the extent to which the wire fraud statute can be used to prosecute a wide variety of fraudulent schemes. This decision, McNally v. United States, 107 S.Ct. 2875 (1987) (a public corruption prosecution under the mail fraud statute, 18 U.S.C. § 1341) rejected the notion that a scheme to defraud can be premised upon the loss of intangible rights, and held that 18 U.S.C. § 1341 only reaches schemes which result in the deprivation of money or property. According to the Court, the mail fraud statute's reference to "any scheme or artifice to defraud," or "for obtaining money or property by means of false or fraudulent pretenses, representations, or promises," (the wire fraud statute contains identical language) should not be read disjunctively; rather the words "to defraud" refer to "wronging one in his property rights ...." Id. at 2880-81. The McNally rule has been extended to wire fraud prosecutions under 18 U.S.C. § 1343. Carpenter v. United States, 108 S.Ct. 316 (1987); United States v. Gimbel, 830 F.2d 621, (7th Cir. 1987) (a scheme which concealed information from the Treasury Department did not deprive the Department of money or property). Thus, a proper charge under the wire fraud statute must allege that the defendant used wire, radio, or television communication in furtherance of a scheme to deprive an individual or entity of money or property.

Until the circuit courts begin to focus on the proof required to show pecuniary harm, the McNally decision may preclude FDA from utilizing § 1343 against firms/individuals that electronically transmit false or fraudulent electronic identification/digital signatures in interstate or foreign commerce to the agency (e.g., electronically submitted fraudulent NDA's from applicants outside Maryland). The interstate or foreign commerce requirement makes § 1343 inapplicable to false or fraudulent electronic identification/digital signatures that are transmitted within a facility (e.g., digital signatures used in "paperless" drug manufacturing systems).

18 U.S.C. § 1505 - Obstruction of Proceedings Before Departments, Agencies, and Committees

Title 18, U.S.C. § 1505, provides in part that:

> Whoever corruptly, or by threats or force, or by any threatening letter or communication influences, obstructs, or impedes or endeavors to influence, obstruct, or impede the due and proper administration of the law under which any pending proceeding is being had before any department or agency of the United States ... shall be fined not more than $5,000 or imprisoned not more than five years, or both.

To establish a violation of 18 U.S.C. § 1505, the following elements must be proved beyond a reasonable doubt:

a. Corruptly, or by threats, force, threatening letter or communication

b. Influences, obstructs, or impedes or endeavors to influence, obstruct or impede

c. A pending proceeding before any federal department or agency

The greatest difficulty in applying this statute to cases of false or fraudulent electronic identification/digital signatures, is the requirement that the obstruction must be material to a pending proceeding. The "pending proceeding" rule has been the focus of many reported decisions concerning 18 U.S.C. § 1505.

Some courts have applied the "pending proceeding" requirement loosely. In United States v. Fruchtman, 421 F.2d 1019 (6th Cir.), cert. denied, 400 U.S. 849 (1970), the court of appeals held that "'proceeding' is a term of broad scope, encompassing both the investigative and adjudicative functions of a department or agency." Id. at 1021. The court concluded that the submission of falsified documents to the attorney in charge of a Federal Trade Commission investigation during the investigation was a 18 U.S.C. § 1505 offense. A similar ruling was handed down by the Tenth Circuit Court of Appeals in a case involving an investigation by the U.S. Customs Service of the defendants' practice of importing firearms. United States v. Browning, Inc., 572 F.2d 720 (10th Cir.), cert. denied, 439 U.S. 822 (1978). The court in Browning held that the "pending proceeding" requirement was satisfied where a defendant advised a firearms exporter to lie to federal investigators while the Customs Service was undertaking "an initial or preliminary evaluation ... which was a prelude to a criminal investigation." Id. at 724.

Other cases, however, establish a stricter "pending proceeding" requirement, one that calls for a formal act. In United States v. Batten, 226 F. Supp. 492 (D.D.C. 1964), aff'd mem., No. 18610 (D.C. Cir. Oct. 15, 1964), cert. denied, 380 U.S. 912 (1965), the § 1505 offense concerned the subornation of perjury before a Securities

and Exchange Commission (SEC) hearing that was part of an investigation instituted by formal order of the SEC. The court held that an investigation directed by a formal order of the SEC, at which a designated officer takes testimony under oath, is a pending proceeding. Id. at 494. Moreover, several district courts have concluded that § 1505 prosecutions must be limited to actions which relate to the rulemaking or adjudicative powers vested in an agency by law. See, e.g., United States v. Higgins, 511 F. Supp. 453 (W.D. Ky. 1981) (FBI investigation is not a pending proceeding).

Accordingly, criminal prosecutions under 18 U.S.C. § 1505, may be appropriate for incidents of false or fraudulent electronic identification/digital signatures that arise during FDA investigations or administrative proceedings.

18 U.S.C. § 371 - Conspiracy to Commit an Offense or to Defraud the United States

If two or more persons are involved in the creation or use of false or fraudulent electronic identification/digital signatures, they may be guilty of conspiracy.

The general conspiracy statute, 18 U.S.C. § 371, contains two alternative offenses: (1) conspiracy to commit an offense against the United States, and (2) conspiracy to defraud the United States. The statute provides as follows:

> If two or more persons conspire either to commit any offense against the United States, or to defraud the United States, or any agency thereof in any manner or for any purpose, and one or more of such persons do any act to effect the object of the conspiracy, each shall be ....

To establish a violation of 18 U.S.C. § 371, the following elements must be proved beyond a reasonable doubt:

a. An agreement by two or more persons.

b. To commit an offense against the United States, or to defraud the United States.

c. An overt act committed by one of the conspirators in furtherance of the agreement (the overt act need not itself be a crime)

If the offense, the commission of which is the object of the conspiracy, is a misdemeanor only, the punishment for such conspiracy shall not exceed the maximum punishment provided for the object offense. The maximum penalty for all other conspiracies is a fine and/or imprisonment for not more than five years.

In proving an agreement, it is not necessary to prove by direct evidence that there was a formal agreement or that the parties to the agreement stated in writing, or in words, what the agreement was or how it was to be effected. It is sufficient to show by circumstantial evidence that there was a mutual understanding to accomplish an unlawful purpose or to accomplish a lawful purpose by unlawful means. American Tobacco Co. v. United States, 328 U.S. 781 (1946); United States v. Heck, 499 F.2d 778 (9th Cir. 1974), cert. denied, 419 U.S. 1088 (1974). A corporation is a person under the law, and therefore a corporation can be indicted and tried as a conspirator. United States v. Socony-Vacuum Oil Co., 310 U.S. 150 (1940). It is also well established that a conspiracy to commit an offense against the United States is a separate and distinct offense from the substantive criminal violation. United States v. Pacheco, 489 F.2d 554 (5th Cir.), cert. denied, 421 U.S. 909 (1975).

The second prong of the general conspiracy statute, a conspiracy "to defraud the United States, or any agency thereof in any manner or for any purpose," is very broadly stated. There is no requirement that the fraud comprise conduct that could be held unlawful under some other statute or rule. United States v. Winkle, 587 F.2d 705 (5th Cir.), cert. denied, 444 U.S. 827 (1979). The crime of conspiracy to defraud the United States includes acts that "interfere with or obstruct one of its lawful governmental functions by deceit, craft or trickery." Hammerschmidt v. United States, 265 U.S. 182 (1924). Proof that the United States has been defrauded does not require any showing of pecuniary or proprietary loss. Id.

In situations where two or more persons agree to create or use false or fraudulent electronic identification/digital signatures in a matter within the agency's jurisdiction, prosecution under either prong of 18 U.S.C. § 371 (conspiracy to commit an offense against the United States, e.g., conspiracy to commit 18 U.S.C. § 1001, or conspiracy to defraud the United States, e.g., to impede, impair, obstruct, or defeat the lawful functions of FDA) is an effective enforcement tool.

The United States Code also contains several provisions which explicitly address computer-based fraud, theft, and vandalism. These statutes are relatively new, and as a result, very few prosecutions have been brought under these provisions. Title 18, U.S.C. Sections 1029 and 1030, could be used as the basis for enforcement action in certain cases involving false or fraudulent electronic identification/digital signatures.

18 U.S.C. § 1029 - Fraud and Related Activity in Connection with Access Devices

Title 18, U.S.C. § 1029(a), makes it a crime (felony) to:

(1) Knowingly and with intent to defraud produce, use, or traffic in one or

more counterfeit access devices;

(2) Knowingly and with intent to defraud traffic in or use one or more unauthorized access devices during any one-year period, and by such conduct obtain anything of value aggregating $1,000 or more during that period;

(3) Knowingly and with intent to defraud possess fifteen or more devices which are counterfeit or unauthorized access devices; or

(4) Knowingly, and with intent to defraud, produce, traffic in, have control or custody of, or possess device-making equipment;

and thereby affect interstate or foreign commerce.

This statute also prohibits attempts and conspiracies to commit any of the offenses enumerated in subsection (a) above.

On their face, subsections (a)(1), (a)(3), and (a)(4) of this statute, appear to be potential bases for enforcement action against individuals who use counterfeit and/or unauthorized access devices (cards, codes, account numbers, etc.) to create false or fraudulent electronic identification/digital signatures. However, after reviewing the definitions section of the statute [18 U.S.C. § 1029(e)], the reported prosecutions brought pursuant to this statute, and the pertinent legislative history, it appears that this statute was primarily intended to proscribe fraud involving credit cards and other financial access devices.

All of the prohibitions in § 1029(a)(1)-(4) pertain to counterfeit or unauthorized access devices. The term "access device" is defined in 18 U.S.C. § 1029(e) as any "card, plate, code, account number, or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value or that can be used to initiate a transfer of funds .... " (emphasis added). Therefore, to bring a prosecution under this statute, the government must be able to prove beyond a reasonable doubt, that a means of account access can be used to obtain money, goods, services, or any other thing of value. This burden would be difficult to meet in most, if not all, false or fraudulent electronic identification/digital signature cases the agency might confront.

There are several reported prosecutions brought pursuant to this statute. All of these cases pertain to either the unauthorized use of credit cards, credit card account numbers, credit card drafts, or long distance telephone access codes. One case in particular, United States v. McNutt, 908 F.2d 561 (10th Cir. 1990), specifically addresses the scope of § 1029. The defendant/appellant in McNutt was convicted of

conspiracy to traffic in counterfeit access devices (satellite television descramblers) in violation of 18 U.S.C. § 1029. On appeal, the defendant/appellant argued that § 1029 is not applicable to satellite television descramblers, that is, satellite television descramblers are not "access devices". The court of appeals agreed, after consulting the legislative history of § 1029.

> In enacting § 1029, 'Congress was focused upon the fraudulent use of [access] devices in connection with credit transactions ....' (quoting United States v. Blackmon, 839 F.2d 900, 913-914 (2d Cir. 1988)). Congress sought to address 'the growing problem in counterfeit credit cards and unauthorized use of account numbers or access codes to banking system accounts ....' (quoting H.R. Rep. 894, 98th Cong., 2d Sess., reprinted in 1984 U.S. Code Cong. & Admin. News 3182, 3689.) Congress sought to include in its definition of access devices 'credit cards, debit cards, account numbers and combinations of these and other methods of obtaining goods and services.' (Id. at 3705).

McNutt, 908 F.2d at 563.

By reason of the foregoing, we would not recommend that enforcement actions involving the unauthorized use of access devices to create false or fraudulent electronic identification/digital signatures, be initiated on the basis of § 1029.

18 U.S.C. § 1030 - Fraud and Related Activity in Connection with Computers

Title 18, U.S.C. §§ 1030(a)(1)-(5), makes it a crime to access or attempt to access without authorization: classified information in a computer (computer espionage), computer records of a financial institution, computer credit information of a consumer reporting agency, and government/"Federal interest computers." This statute also prohibits trafficking in computer passwords.

Title 18, U.S.C. § 1030(a)(6), provides criminal penalties (misdemeanor and felony) for anyone who:

> Knowingly and with intent to defraud traffics (as defined in § 1029) in any password or similar information through which a computer may be accessed without authorization, if-
>
> (A) such trafficking affects interstate or foreign commerce; or
>
> (B) such computer is used by or for the Government of the United States

To establish a violation of 18 U.S.C. § 1030(a)(6), the following elements must be proved beyond a reasonable doubt:

a. Knowingly

b. With intent to defraud

c. Traffics (or attempts to traffic)

d. In any password or similar information through which a computer may be accessed without authorization.

e. If-

(1) such trafficking affects interstate or foreign commerce; or

(2) such computer is used by or for the Government of the United States

The penalty for first offense violations of 18 U.S.C. § 1030(a)(6) (including attempts) is a fine and/or imprisonment for not more than one year. The penalty for subsequent offenses is a fine and/or imprisonment for not more than ten years.

The term "traffic," as defined in 18 U.S.C. § 1029(e)(5), means to "transfer, or otherwise dispose of, to another, or obtain control of with intent to transfer or dispose of." Title 18, U.S.C. § 1030(e)(1) defines the term "computer" as an:

> electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device.

We have found only three reported decisions that resulted from criminal prosecutions brought under § 1030. United States v. Morris, 928 F.2d 504 (2d Cir. 1991); United States v. Morris, 728 F. Supp. 95 (N.D.N.Y. 1990); United States v. Hagen, 711 F. Supp. 879 (S.D.Tex. 1989). The two Morris decisions involve charges under subsection (a)(5) of the statute (intentionally accessing a "Federal interest computer" without authorization). The defendant in Hagen was convicted (before a magistrate) of violating subsection (a)(6)(A), but his appeal to the district court (cited above) only addressed the propriety of his sentence.

The U.S. Attorney's Manual notes that subsection (a)(6) was designed to proscribe the conduct associated with private bulletin boards used by hackers to display passwords. See USAM 9-48.116 (Oct. 1988). However, we could not find support for this proposition in the legislative history.

It appears that § 1030(a)(6)(A) could be used to prosecute individuals or entities who "traffic" in computer passwords (or similar information through which a computer may be accessed without authorization) that may result in false or fraudulent electronic identification/digital signatures.

CENTER FOR DRUG EVALUATION AND RESEARCH:

(By Paul J. Motise, HFD-323)

(1) Regulatory Acceptance:

(a) The CGMP regulations for human and veterinary drugs (21 CFR 210 and 211) do not anticipate nor permit signature alternatives. Requirements for conventional signatures are explicit, implicit and set by precedent (to the extent that use of conventional signatures is current practice as encountered by field investigators). Some sections of the regulations call for endorsements by full signature; some call for initials or signatures **[28]**. It is vital that individual endorsements be accurate, secure, in a form that cannot be refuted by the author, legally binding, and in a form that permits subsequent investigations.

(b) The Prescription Drug Marketing Act (PDMA) calls for signatures of physicians when they request and receive samples of drug products. The PDMA implementing regulations, as currently being developed, will accept signatures recorded electronically but not such signature alternatives as electronic identification (e.g., id codes); consideration of electronic signatures (e.g., retinal scans) is being deferred **[22]**. It should be noted that at this point the draft federal register notice stating this approach has not yet been circulated for agency clearance. CDER has been active in obtaining technical information on signature systems from various system developers and end users.

(c) The Institutional Review Board (21 CFR 56) regulations call for signatures relating to clinical investigations. We received an inquiry from the University of Wisconsin, asking if electronic signatures may be used. Our reply acknowledged that the entire issue of automated data systems is being reviewed by the agency. The inquiry itself demonstrates the technological advancements that are being made and their application to FDA regulations.

(2) Industry Communication:

(a) Communication with the Pharmaceutical Manufacturers Association (PMA) disclosed the keen interest that the association has in the subject of electronic identification. We discussed the subject at a 5/91 meeting **[29]**. In a 11/25/91 letter to FDA, PMA furnished several discussion papers **[30]**. In a 12/5/91 response to that letter, the agency made it clear that the CGMP regulations do not anticipate, nor permit use of electronic or surrogate signatures or initials

[31]. We anticipate continued discussions with PMA.

(b) Communication with the Parenteral Drug Association (PDA) disclosed the interest that the association has in the subject of electronic identification. We received an informal request from PDA to form a joint PDA/FDA task force to address the issues of electronic signatures within CGMPs. We declined the invitation as inappropriate but established a line of communication. Some segments of the industry are anticipating, it was learned, receiving official FDA correspondence, including FD 483's, by FAX or other electronic means.

(c) Burroughs Wellcome Co. met with CDER representatives on July 18, 1991 regarding their plans to construct a highly automated production facility that would implement paperless production records; we advised the firm of existing requirements and the prospects for revising the regulations to accommodate electronic signatures **[32]** The firm also submitted a Citizen's Petition on electronic identification **[33]**. The 10/18/91 petition requested the agency to clarify CGMP requirements as to when full handwritten signatures are required, and to permit electronic identification in lieu of such signatures. The center will issue an interim reply to the petition, in line with the 12/5/91 letter to PMA.

(3) Systems Evaluation by WEAC:

CDER has suggested that the Winchester Engineering and Analytical Center (WEAC) become involved in the electronic identification project. By memo of 11/1/91 to the Division of Field Sciences, CDER suggested that WEAC undertake a field research project of evaluating electronic signature technologies by examining loaned vendor samples **[34]**. The examinations would identify potential problem areas/weaknesses as well as positive attributes, based on non-destructive testing, with a view toward codification of key performance features (not specific systems). Results of testing would be available to all agency units. WEAC/Field Sciences has not yet formally responded, although WEAC Section Supervisor Robert Mazzaferro, HFR-NE-480 has, by phone, acknowledged receipt of the suggestion and expressed some interest in the project. We are forwarding technical information from system vendors to WEAC as it becomes available.

(4) CDER Electronic Documents:

a. Electronic Laboratory Records: Our Division of Drug Analysis at St. Louis purchases material by electronic sign off on a system secured by two levels of passwords and optical disk recordation. However, it should be noted that the ultimate purchase order is still executed conventionally when the division's administrative officer signs a paper form. Furthermore, that unit is developing electronic collection reports and work sheets **[35]**.

b. Electronic Mail to the Industry. CDER has recently extended its internal ALLINONE electronic mail system to permit electronic mail exchange with outside FDA parties via MCI mail and BITNET. The multitude of concerns expressed by CDER personnel about this move, concerns which include issues about legal acceptance of unsigned correspondence, have caused CDER project managers to limit the expansion to a pilot project, and to reverse an earlier decision to publicize the program via a federal register notice **[36][37][38][39]**. In addition, the ALLINONE electronic mail system has a fax interface, such that correspondence which lacks a physical signature may be transmitted as a fax. Our experience in this area is limited and electronic faxes have generally been restricted to answering routine incoming inquiries in fax form **[40]** In one case a German correspondent balked at receiving an unsigned FAX document (one generated by electronic mail) forwarded in response to an inquiry on ethylene oxide **[41]**; the author was asked to sign a paper copy of the fax as a method of verification, and did so; the incident raises the issue of how other countries (including those with which we have memoranda of understanding) are viewing electronic signatures.

(5) Submissions to the Agency:

About 10% of new drug application submissions are in electronic form, currently. The center's goal is to have 100% of all applications in electronic form (no paper at all) by 1995. For now, however, duplicate paper submissions are still required for computerized applications. The paper version is the archive copy. Some submissions are made on optical disk; because the agency lacks optical disk readers, firms which submit such electronic forms must loan the agency the equipment necessary to read the submissions. At this point, the center is not prepared to go to court and rely upon electronic signatures contained in computerized submissions. Our scientific review divisions lack standard operating procedures to verify electronic submissions against paper versions, although some reviewers may, in fact, be conducting such audits. Some electronic submissions include applicant provided search engine programming to allow keyword searches and statistical reviews.

The agency has recently been awarded Presidential Priority Status for our program of automating the new drug review process **[42][43]**. We expect that this support will result in availability of additional funding.

(6) Validation/Reliability:

CDER agrees that signature alternatives need to be validated, and that reliability is vital. Specific guidance in this area can be prepared in the future, as needed. The CDER/CDRH Guidelines On the General Principles of Process Validation may be of use in a general approach to validating signature systems.

(7) Security:

CDER agrees that a high degree of security is needed for signature alternatives and has proposed general security measures as part of the PDMA implementation regulations (draft now being developed).

(8) Enforcement Integrity:

We have not yet been made aware of instances in which inspections have been hampered because production records were in electronic form. However, certain fraud investigations may be somewhat hampered by the lack of physical evidence that paper and ink records afford. For example, stacks of paper records may reveal important impressions that were made when top sheets of paper were written by hand. Furthermore, physical samples of ink used to sign a document may be analyzed in a laboratory and dated as to time of manufacture, thus providing, in some instances, a key indicator of post action falsifications. Paper may also reveal evidence of erasures.

CENTER FOR VETERINARY MEDICINE:

(By Jo Gulley, HFV-226)

It is rather apparent that the issue of electronic communications, including electronic submissions, signatures, signature surrogates, documents, mail, etc., has to be specifically addressed by the agency. The proposed federal standard for electronic identification has made this matter urgent. CVM is of the general impression that the issues of electronic processing and technology as it impacts on documents and records required by law to be generated/maintained by industry also must be addressed. CVM cannot agree, however, on the proposed federal Digital Signature Standard as it currently exists. We do not believe that the NIST Draft DSS should be adopted by the agency because its security and performance are the subject of considerable controversy and because implementation of said standard would likely be too costly and burdensome to both the FDA and industry.

CVM is in agreement with the definitions proposed by the work group; CVM is also in agreement with the work group's recommended goals thus far, which are 1) to come to an agreement on the acceptance of signature alternatives for the agency on a multi-center basis, 2) render a publication in the Federal Register providing an advanced notice of the proposed rule-making plans of the agency to consider whether or not to develop regulations addressing signature alternatives (allowing a 90 day comment period) and 3) if indicated by the comments, develop codification of general signature alternatives acceptance provisions for publication in the Code of Federal Regulations.

The anticipated uses (applications) for electronic submissions to the agency specifically relating to CVM (i.e., documents/records that lend themselves to the possibility of using electronic signatures/identification in the future/or would be directly impacted upon due to electronic submissions, signatures, identification and signature substitutes) are as follows:

Data in support of New Animal Drug Application (NADA) approvals (including supplemental applications), Food Additive Petitions (FAP's), Investigational Food Additive Petitions (IFAP's), Investigational New Animal Drug Applications (INAD's), Drug Experience Reports (DER's), Adverse Drug Reactions Reports (ADR's), Medicated Feed Applications (MFA's), Notice of Drug Shipments, Final Dispositions, Veterinary Master Files (VMF's), Facsimile transmissions and communications, Direct data (information) exchange, Batch/production records from inspections, Clinical trials (Efficacy data, Target Animal Safety trials), Experimental data, Laboratory data, correspondence, and letters.

CVM has reviewed the work group's findings and offers the following responses to several key points:

(1) Regulatory Acceptance:

CVM agrees that:

(a) The CGMP regulations (21 CFR 211) do not permit signature alternatives. There are requirements for conventional signatures in this section of the regulations.

(b) The proposed changes to the CGMP regulations (21 CFR 225 & 226) should address the issue of electronic submissions and signature alternatives.

(c) The NADA rewrite may have to be revisited to see if any specifics will have to be amended to implement electronic signature alternatives.

(2) Issues of computer validation/electronic signatures within CGMPs.

CVM has been developing some guidelines to be followed by field investigators in reviewing validation information on computer systems used in the manufacture of medicated feeds. Section 225.102(b)(1) of the Current Good Manufacturing Practice Regulations for medicated feeds requires that each Master Record File shall be prepared, checked, dated, and signed or initialed by a qualified person. Questions have been raised asking what are acceptable ways of complying with this requirement when the "person" preparing, checking, and dating master formulation is, in fact, not a human being, but an automated piece of equipment, such as a computer system. CVM recognized that it was possible that a computerized system could achieve the same or a higher degree of assurance as would be provided by a person if the process used to create and transmit this sequence of events was properly controlled and adequately validated.

Guidelines have been developed on what constitutes an acceptable means of complying with the identification and approval requirements of 21 CFR 225.102(b)(1). CVM has stressed validation of computerized systems and has stated such validation data for on-site processes must be available for on-site review.

(3) Industry Inquiries:

Some industry inquiries have been received pertaining to signature/initials being added by a computer on mandatory records needed to be generated and maintained by industry. For instance, an inquiry was received requesting clarification/criteria of

CGMP regulation interpretation as to when full handwritten signatures are required, and to permit electronic identification in lieu of such signatures. Specifically, there were questions regarding the interpretation of § 225.102 (b)(2)(i), which requires "...a written endorsement in the form of a signature or initials by a responsible individual" on batch production records. The requestor wanted to know if computer generated initials or name could be used in place of handwritten initials or signature. Another instance involved validation of computer hardware and software; the requestor was soliciting information on available computer validation guidelines for the feed industry. Additionally, another requestor wanted to discuss the plans of some members in the feed manufacturing industry to hire his firm for the development of an industry standard that will use bar codes for data collection purposes. This requestor wanted to know just what requirements FDA had for the feed and drug industries concerning data collection. Specifically, he was concerned with formulations in which the computer would control everything and scanners would be used to "read" information on drug ingredients from the micro ingredient bins. CVM will address these issues.

(4) FDA Electronic Documents - It is foreseeable that Analytical Worksheets, Collection Reports, Establishment Inspection Reports, List of Observations will all be electronically created and maintained in the future.

Other Electronic documents - Electronic NADA data submissions are already being received. Some MFA's being received are computer generated but are still hand signed. The emphasis at this time is that someone still has to sign a paper form of the document. CVM agrees that the agency must consider electronic mail systems, including electronic correspondence with other countries and we must consider how these countries are viewing electronic signatures, etc.

(5) Validation/Reliability - CVM agrees that signature alternatives need to be validated. Specific guidance must be prepared before any implementation can be done. Validation requirements should provide a means of documenting and assuring the movement and authenticity of data from the point of collection to the receipt of the document by CVM.

(6) Security - CVM agrees that a high degree of security is needed for signature alternatives; general security measures must be carefully proposed and vigorously implemented.

(7) Enforcement Integrity - We have not received any information or have knowledge of any specific instances in which inspections have been hampered because production or batch records were in electronic form. We are aware, however, of some instances where refusals have been encountered as a result of a request to review software documentation for computer produced production and batch records. We, too, agree that certain investigations may be somewhat hampered by the lack of

physical evidence that paper and ink records afford and that careful consideration must be given in this area.

(8) Standards. CVM acknowledges that standards for electronic signatures may be useful but cannot agree with accepting the proposed federal Digital Signature Standard as it currently exists.

(9) Freedom of Information. CVM is unaware of any specific FOI requests for releasable documents in electronic form. CVM is of the opinion that we can expect additional requests for a wide variety of electronic records in the future as well as requests on how the agency determined the validation issues pertaining to the authenticity of the electronic documents. We feel SOPs will have to be prepared to deal with unique problems pertaining to FOI requests as well as validation issues in general.

OFFICE OF THE COMMISSIONER

OFFICE OF INFORMATION RESOURCES MANAGEMENT

(By David R. Hamrick, HFA-51)

The Office of the Commissioner (OC) does not collect data from the public which, by law, must be certified by a representative of the organization submitting the data. However, OC does receive requests for information, distributes responses to requests and performs internal processing of information where the use of a digital signature may improve the agency's effectiveness and efficiency.

All staff offices under the Deputy Commissioner for External Affairs, the Executive Secretariat, and OLA receive many paper requests for information. As we progress into the 90's, a shift to electronic media can be expected. A methodology for handling a digital signature will facilitate this process.

Computer generated form letters which require an original signature are used today to respond to many requests for information. Automating the signatures would shorten the processing of these letters. For example, responses to Freedom of Information (FOI) and Docket Management Systems inquiries could be improved by using an automated signature process.

Finally, internal routing of paperwork for approvals could be expedited by automation. Establishing the capability to use a digital signature will help facilitate this process.

CENTER FOR DEVICES AND RADIOLOGICAL HEALTH:

(By Christine Nelson, HFZ-332)

The following five areas are discussed in this report:

- Requirements for signatures;
- Proposed amendments to regulations which would require signatures;
- Implied signature requirements;
- Information received electronically; and
- Information stored electronically.

CDRH REQUIREMENTS FOR SIGNATURES

The following are sections of the FDA/CDRH regulations which have signature requirements. Where there are quotation marks, I have quoted subsections of the regulation. Where there are no quotation marks, I have paraphrased the regulation.

SUBCHAPTER H MEDICAL DEVICES

PART 800 GENERAL

Subpart C Administrative Practices and Procedures

800.55 Administrative detention.

800.55(a) "This section sets forth the procedures for detention of medical devices intended for human use believed to be adulterated or misbranded. . .

800.55(d) "The **detention order** shall be issued in writing, in the form of a detention notice, **signed by the authorized FDA representative** who has reason to believe that the devices are adulterated or misbranded, . . ."

PART 801 LABELING

Subpart E Other Exemptions

801.150 Medical devices; processing, labeling, or repacking.

801.150(a) Devices, which are shipped or otherwise delivered into interstate commerce for processing, labeling, and repacking at an establishment other than the one where they were originally processed or packed, shall be exempt from compliance with labeling and packaging requirements, provided there is a **written agreement, signed by the person who introduced the shipment into interstate commerce AND is the operator of the establishment where the device is to be processed, labeled, or repacked. If the person who introduced the shipment into interstate commerce is different from the operator of the establishment where the device is to processed, labeled, or repacked, both persons must sign the agreement**. The agreement must contain specifications for processing, labeling, or repacking to insure, if the specifications are followed, that the device will not be adulterated or misbranded.

801.150(e) The Food and Drug Administration will initiate no regulatory action against a device as misbranded or adulterated when a nonsterile device is labeled sterile and is introduced into or in interstate commerce for shipment to a contract sterilizer, provided all the following conditions are met: there is in effect a **written agreement** which is **signed by the person authorizing such shipment and the operator or person in charge of the establishment receiving the devices for sterilization**. The agreement must contain instructions, procedures, and specifications to assure that the device will be brought into full compliance with the Federal Food, Drug, and Cosmetic Act.

Subpart H Special Requirements for Specific Devices

801.420 Hearing aid devices; professional and patient labeling.

801.420(c)(3) "Federal law restricts the sale of hearing aids to those individuals who have obtained a medical evaluation from a licensed physician. . . . **a fully informed adult may sign a waiver statement** declining medical evaluation for religious or personal beliefs that preclude consultation with a physician. . ."

801.421 Hearing aid devices; conditions for sale.

801.421(a)(2)(iii) The hearing aid dispenser shall not sell a hearing aid unless (1) the prospective user has presented a **written statement signed by a licensed physician** stating that

the patient's hearing loss has been medically evaluated and the patient may be considered a candidate for a hearing aid, or (2) the **prospective user has signed a waiver of medical evaluation**. This section provides wording for a waiver of medical evaluation.

PART 808 EXEMPTIONS FROM FEDERAL PREEMPTION OF STATE AND LOCAL MEDICAL DEVICE REQUIREMENTS

Subpart B Exemption Procedures

808.20 Application.

808.20(b) An **application for exemption from preemption** shall be in the form of a letter **signed by an individual who is authorized to request the exemption on behalf of the State or political subdivision.**

PART 812 INVESTIGATIONAL DEVICE EXEMPTIONS

Subpart B Application and Administrative Action

812.20 Application.

812.20(a)(3) **Applications for Investigational Device Exemptions (IDE) shall be signed by the sponsor**.

812.20(b)(4) The application must include a list of the names and addresses of all **investigators who have signed the agreement entered into by the investigators.**

Subpart C Responsibilities of Sponsors

812.43 Selecting investigators and monitors.

812.43(c) In selecting investigators, sponsors shall obtain a **signed agreement from each participating investigator** which includes information such as the investigator's curriculum vitae; a statement of the investigator's relevant experience; an explanation of any of the investigator's research which was terminated; and a statement of the investigator's commitment to conduct the investigation.

812.46 Monitoring investigations.

812.46(a) A sponsor shall secure compliance or discontinue shipments of the device if an **investigator** does not comply with the **signed agreement**, the investigational plan, applicable FDA regulations, etc.

Subpart E Responsibilities of Investigators

812.100 General responsibilities of investigators.

812.100 An **investigator** is responsible for ensuring that an investigation is conducted according to the **signed agreement**.

812.110 Specific responsibilities of investigators.

812.110(b) An **investigator** shall conduct an investigation in accordance with the **signed agreement** with the sponsor.

Subpart G Records and Reports

812.140 Records.

812.140(b) A sponsor shall maintain certain records including **signed investigator agreements.**

PART 813 INVESTIGATIONAL EXEMPTIONS FOR INTRAOCULAR LENSES

Subpart B Applications for Exemptions for Investigational Studies Involving Human Subjects

813.20 Application.

813.20(a) "The sponsor of an investigational study shall submit to the Food and Drug Administration a completed **application for an investigational device exemption** that has been **signed by the sponsor or an authorized representative of the sponsor.**"

813.20(b) "An application for an investigational device exemption for an intraocular lens shall include the following information: . . ."

813.20(b)(11) "**A copy of the agreement signed by investigators who will be participating . . .**"

813.39 Supplemental applications and submissions concerning applications.

813.39(c) "The sponsor shall submit to the FDA the **signed statements required under 813.43(b) for any additional investigators** and, as required by 813.42(d), the **statement signed by the chairman of any institutional review committee that is added to an investigational study after submission of an application for an investigational device exemption under 813.20(b).**"

Subpart C Sponsor Responsibilities in Investigational Studies of Intraocular Lenses.

813.42 Review of the investigational study by the Food and Drug Administration and the institutional review committee

813.42(d) "The sponsor shall obtain from the institutional review committee a **statement, signed by the chairman,** that the committee has approved the investigational plan and has reviewed the report of prior investigations of the lens and that the committee will monitor the investigation in accordance with Subpart D of this part."

813.43 Selection of investigators.

813.43(b) The sponsor shall obtain from each **investigator who will participate in the investigational study a signed agreement for submission to the Food and Drug Administration** that includes a statement of the investigator's education and experience . . ., an agreement to comply with the investigational plan and requirements . . ., an agreement that any use of the lens involving human subjects be under the investigator's supervision . . ., a statement as to whether any investigational study or other research by such investigator has been discontinued on the order of a sponsor . . ., and the name of any other investigator who will participate in the investigator's supervision and responsible to him . . .

813.45 Control over the intraocular lens.

813.45(a) "The sponsor shall permit the lens to be shipped only to **investigators** who have **signed statements under 813.43(b).**"

Subpart E Investigator Responsibilities in Investigational Studies of Intraocular Lenses

813.107 Control over intraocular lenses.

813.107(a) "An investigator shall only permit the lens to be used for administration to, or use involving, subjects who are under his personal supervision or under the supervision of another investigator who is responsible to him and who is named by the **investigator** in his **signed statement undertaking the obligations of an investigator under 813.43(b).**"

PART 814 PREMARKET APPROVAL OF MEDICAL DEVICES

Subpart B Premarket Approval application (PMA)

814.20 Application.

814.20(a) **Applications for Premarket Approval (PMA)** shall be **signed by the applicant or an authorized representative**. If the applicant does not reside in the U.S., the PMA shall be countersigned by an authorized representative residing or maintaining a place of business in the U.S. and shall identify the representative's name and address.

Subpart C FDA Action on a PMA

814.44 Procedures for review of a PMA.

814.44(b) "The advisory committee shall a submit a report to FDA which includes the committee's recommendation and the basis for such recommendation on the PMA. . . . The advisory committee report and recommendation may be in the form of a **meeting transcript signed by the chairperson of the committee.**"

PART 820 GOOD MANUFACTURING PRACTICE FOR MEDICAL DEVICES: GENERAL

Subpart G Packaging and Labeling Control

820.121 Critical devices, device labeling.

820.121(b) "The **signature of the individual who proofreads**

the labels and other labeling for critical devices and the date of the proofreading **shall be recorded**." The record of proofreading of labeling, including the signature and date, becomes part of device history record.

Subpart I Device Evaluation.

820.161 Critical devices, finished device inspection.

820.161 A **designated individual shall authorize, by signature, the release of the device for distribution** after checking acceptance records and test results and assuring that the device history record is complete. The authorization to release the device for distribution becomes part of device history record.

Subpart J Records

820.181 Device master record.

820.181 The **device master record** shall be prepared, dated, and **signed by designated individual**. Any **changes** in device master record shall be **authorized** in writing **by signature of designated individual**.

820.185 Critical devices, device history record.

820.185(a)(2) The **device history record for critical devices** shall include the record of acceptance of critical components, including the acceptance date and **signature of the recipient**.

SUBCHAPTER J RADIOLOGICAL HEALTH

PART 1002 RECORDS AND REPORTS

Subpart A General Provisions

1002.7 Submission of data and reports.

1002.7 "**All submissions** such as reports, test data, product descriptions, and other information required by this part, or voluntarily submitted to the Director, Center for Devices and Radiological Health, . . . shall be **signed by the person making the submission.**"

PART 1005 IMPORTATION OF ELECTRONIC PRODUCTS

Subpart C Bonding and Compliance Procedures

1005.25 Service of process on manufacturers.

1005.25(a) and (b) "Every manufacturer of electronic products, prior to offering such product for importation into the United States, shall **designate a permanent resident of the United States as the manufacturer's agent** upon whom service of all processes, notices, orders, decisions, and requirements may be made for and on behalf of the manufacturer . . . The designation shall be addressed to the Center for Devices and Radiological Health . . . all **signatures** shall be in ink."

PART 1020 PERFORMANCE STANDARDS/IONIZING RADIATION EMITTING PRODUCTS

All references to "sign" which appear in this part refer to signs of ions, not signing as in writing one's signature.

PROPOSED CHANGES TO REGULATIONS REGARDING SIGNATURE REQUIREMENTS

MEDICAL DEVICE REPORTING

Current Medical Device Reporting (MDR) requirements do not include signature requirements. However, the proposed amendments described below include signature requirements.

PART 803 MEDICAL DEVICE REPORTING

Subpart B Reports and Records

803.26 **Manufacturers** shall submit a **signed baseline report for each model family for which they have had reports**, which includes distribution and failure analysis information.

803.28 **User facilities, distributors, and manufacturers** shall submit a **signed report for each reportable incident** of which they become aware.

803.30 Each **manufacturer** shall submit an annual certification of the number of MDR reports filed or, if none were submitted, that none were supposed to be submitted. A **signed certification that the information in the report is correct** shall be included.

CDRH "IMPLIED" SIGNATURE REQUIREMENTS

Although there are no specific requirements for signatures in the regulations, CDRH will not process certain requests from the regulated industry without signatures.

EXPORT REQUESTS

FD & C Act There are no specific requirements for signatures in "Export Sec. 801(e) Requests" of the FD & C Act Section 801(e), however the Regulatory Guidance Branch will not process **requests for permission to export** unless the request is signed.

ESTABLISHMENT REGISTRATION

807.22 This section requires:

(1) first registration of a device establishment by submission of an Initial Registration of Device Establishments form (FD-2891),
(2) subsequent annual registration by submission of a Registration of Device Establishment form (FD-2891a), and
(3) initial listing of devices and subsequent updating on a Medical Device Listing form (FD-2892).

Although there is no signature requirement, the Registration and Listing Branch does not consider a **registration form** to be valid unless it is signed.

807.40 Foreign manufacturers or foreign exporters wishing to distribute a foreign-made medical device in the U.S. must submit a completed **Medical Device Listing form** (FD-2892). Although there is no signature requirement, the Registration and Listing Branch does not consider a form to be valid unless it is signed.

PREMARKET NOTIFICATION SUBMISSION (510(k))

807.87(j) This section is being added to the existing requirement that registered establishments submit notification of intent to begin introduction or delivery for introduction into interstate commerce for commercial distribution of a device intended

for human use which meets certain specified criteria. The new section will require a **statement certifying the correctness and accuracy of the information** submitted. Although a signature is not specifically required, the Office of Device Evaluation will expect to see a signature on the certification.

INFORMATION RECEIVED ELECTRONICALLY FROM THE REGULATED INDUSTRY

MEDICAL DEVICE REPORTING

The Division of Product Surveillance (DPS) in the Office of Compliance and Surveillance (OCS) is working on an agreement to receive information electronically from at least one firm submitting reports under the Medical Device Reporting requirements. DPS will rely on a signed transmittal letter for the legally binding signature. DPS is working on an approach that will not require a transmittal letter when the firm directly submits reports to a CDRH PC based bulletin board.

In complying with the revised MDR regulation, signatures would be maintained in the firm's complaint files.

DPS anticipates instances in which it will be necessary to take legal action based on false and misleading information submitted by firms and/or user facilities. We do not know how the courts will respond to an electronic signature.

No other offices in CDRH are accepting electronic submissions which require signatures at this time.

ELECTRONIC STORAGE OF DOCUMENTS

For the past year and a half, CDRH has been scanning and storing closed 510(k) documents and reports submitted under the Medical Device Reporting (MDR) regulations in the Center's optical imaging system. Beginning in early February, closed Premarket Approval (PMA) applications are being scanned for storage.

CENTER FOR BIOLOGICS EVALUATION AND RESEARCH

(By Boyd Fogle Jr., HFB-120)

1. REGULATORY ACCEPTANCE

CBER's regulatory authority for biological products is obtained from the Public Health Service Act (42 USC 262) and the Federal Food, Drug, and Cosmetic (FD&C) Act. The legal identity of biological products (including licensed products and products not subject to licensure) are either drugs or devices as defined by the FD&C Act. As a result, biological products defined as drugs must be manufactured in conformance with applicable provisions of the CGMP's for finished pharmaceuticals (21 CFR 211). Biological products defined as devices are generally subject to applicable provisions of the CGMP's for medical devices (21 CFR 820, et seq.), but there are particular references in the regulations to the drug CGMP's for certain in vitro biologics.

Since requirements for identification of persons performing significant steps in manufacturing or reviews and release decisions are drawn from CGMP authorities for both drugs and devices, whatever policy is developed and adopted by CDER or CDRH would have a direct impact on CBER.

There are also separate CGMP requirements at 21 CFR, Part 600 that apply to the manufacture of blood and blood components and Source Plasma (See 21 CFR, Parts 606 and 640). A review of the blood and blood components CGMP's and additional standards revealed that only twice is there a requirement for a full signature. All other requirements request only the identity of the person(s) performing work. A summary of our review follows these comments. Note that in references for 21 CFR, Part 610 (General Biological Products Standards), there are many cross references to specific drug CGMP's (21 CFR 211's) for records requirements. These facts illustrate the need for a uniform policy.

We have observed a significant increase in the use of computer systems in blood establishments over the past two to three years. As a result, CBER has issued two memorandum to the blood industry. In addition, CBER recently (January 1992) conducted a workshop on quality assurance in blood establishments, and a portion of the workshop was devoted to use and validation of computer systems. The systems currently in use provide for electronic identification, and CBER has accepted these systems provided that the systems have been properly validated, provide for adequate security, and provide an audit trail to indicate when corrections to critical information has been made and by whom.

2. ENFORCEMENT INTEGRITY AND LEGAL ACCEPTANCE

Recordkeeping systems used in the manufacture of biological products whether manual or computerized must be accurate and provide sufficient detail to describe significant steps in manufacturing and identify the person responsible for work performed. Inaccurate entries in required records whether maintained manually or by computer system would be evaluated as violations of the FD&C Act, Section 501 (a)(2)(B). If investigations revealed that material false statements had been made to conceal facts or impede and obstruct FDA inspections, violations of Title 18, United States Code, Section 371 (Conspiracy), 1001 (False Statements), and 1505 (Obstruction) would also be evaluated.

3. VALIDATION/RELIABILITY

CBER would require that systems using a form of electronic identification to meet a CGMP requirement or other signature alternatives be properly validated to ensure reliability and have adequate security to prevent unauthorized entry and use. The agency guidelines on general principles of process validation, inspection of computer systems, and guides for software development have also been applied to manufacturers of biological products. We believe that more detailed and specific guidance should be developed by the agency concerning systems that include electronic identification for work performed and review/release decisions. CBER has been working with CDRH to develop more detailed guidance to the blood banking and plasma industry relating to computer system validation. These facts also illustrate the need for an agency wide policy.

4. SECURITY

Any form of computer system used in manufacturing operations must provide for adequate security. CBER would expect the same level of assurance with a computer system as would be provided for in non-computerized control systems.

5. STANDARDS

CBER agrees that it would be premature to accept the NIST Digital Signature Standard recognizing the reports of much opposition to the draft standard with respect to its security and performance. In addition, the proposed standard may not be practical for adoption by the industry due to cost and due to efforts which may be far along in development of systems without recognition of the proposed NIST standard. It would, therefore, be more appropriate for the agency to adopt a more flexible standard that

would accommodate all manufacturers and provide for acceptance of more than one standard system. CBER also agrees with the proposal of the task group for establishment of standard terms and definitions for use in the development of a agency wide policy.

6. FREEDOM OF INFORMATION

CBER agrees with the task group consensus concerns relating to FOI functions.

Formal submissions to CBER include: Establishment and Product License Applications and Amendments, IND's, IDE's, NDA's, 510(k)'s, Manufacturing Protocols for Lot Release, Export Requests, etc.

CBER is in agreement with the task group recommendations for: 1) an agency wide policy that could be adopted by all Centers; 2) publication in the Federal Register of an advanced notice of rulemaking which would solicit comments from the affected industry and providing current information to the agency concerning current practice in the industry, and 3) as appropriate, revise CGMP's or develop additional, specific standards.

Review of Biologics Regulations Re: Signature Requirements
Prepared by: HFB-120

<u>Electronic Identification:</u>

600.10(a) Responsible Head

600.12 Records

(a) ...such records shall be legible and indelible, shall identify the person immediately responsible,...

600.14 Reporting of Errors

601.3 License Forms
(a) Establishment License

(b) Product License

601.12 Changes to be Reported

"Important proposed changes in location, equipment, management and responsible personnel ...

shall be reported ... by the manufacturer... not less than 30 days in advance of the time such changes are extended to be made."

601.21 Product Under Development
Reference to Sec 505(i) and 21 CFR, Part 312.

PART 606:

606.110 "Physician had certified in writing ...

606.160 Records

(a)(i) "(...all records shall be legible and indelible, and shall identify the person performing the work ...

Donor Records
(b)(1)(vi) Blood collection, including identification of the phlebotomist.

(b)(2) Processing Records
(v) Labeling, including initials of person(s) responsible.
(b)(3) Storage & Distribution Records
(iii)
Storage temperature, including initialed temperature recorder charts
(v)
Emergency Release of Blood, including signature of requesting physician obtained before or after release.
(b)(2) General Records
(ii)
Responsible personnel

PART 607 Establishment Registration and Product Listing for Manufacturers of Human Blood and Blood Products

607.7 Re: submission of Registration Forms

607.22(b) In lieu of Form FD-2830, tapes for computer input may be submitted if equivalent in all elements of information as specified in Form FD-2830. All formats for such use will require initial review and approval by the Office of Compliance, Center for Biologics Evaluation and Research, Food and Drug Administration."

PART 610 General Biological Products Standards

610.12 Purity

610.13 Purity
(a)(2) Records
Ref. 21..188 (Batch Production and Control Records)
[211.188(b)(11) "identification of the persons performing and directly supervising on checking each significant step in the operation."

Ref. 211.194 - Laboratory Records
211.194(a)(7) - The initials or signature of the person who performs each test and the date(s) the tests were performed

(8) The initials or signature of a second person showing that the original records have been reviewed for accuracy, completeness, and compliance with established standards.

610.18 Cultures
(d) Records
Ref. 211.188 (Batch Production * Central Records)
Ref. 211.194 (Laboratory Records)

PART 620 Additional Standards for Bacterial Products Samples & Protocols

PART 630 Additional Standards for Viral Vaccines

Samples & Protocols

610.12 Sterility
(h) Records - Ref. 211.167 (Special Testing Requirements)
211.194 (Laboratory Records)

PART 640 Additional Standards for Human Blood and Blood Products.

640.65 Plasmapheresis
(b) Procedures - specific requirements
(2)(i) re: accumulated lab data (4 mo. sample)
"The review shall be signed by the reviewing physician."

(2)(ii)"Provided, ..., the donor's file contains a signed statement from a physician or clinic establishing that treatment for syphilis has been initialed..."

PART 650: Additional Standards for Diagnostic Substances for Dermal Tests

Protocols & Samples

PART 660: Additional Standards for Diagnostic Substances for Laboratory Tests

Protocols & Samples

PART 680: Additional Standards for Miscellaneous Product

680.1-3 Allergenic Products
680.2 Manufacture of Allergenic Products

(f) Records.

re: source material 211.188
(Batch Product Control Records)

680.3 Tests
(a) Identity
(b) Safety
(c) Sterility
(d) Reserved
(e) Potency
(f) Records
"The records related to the testing requirement of this section shall be prepared and maintained as required by 211.165, 211.167, 211.188, and 211.94 of this chapter"

680.20-26 Blood Group Substances

600.23(b) Sterility
600.23(c) Pyrogens - ref. 610.13(b)

FINDINGS OF THE WORKING GROUP:

At this point the working group finds that:

1. It is necessary to distinguish and define such terms as signature, electronic signature, and electronic identification. There is a key difference between electronic signatures and signatures recorded electronically.

2. To accommodate signature alternatives some existing regulations, including the drug CGMP regulations, will need to be changed. Guidance and policy documents could not be used to effectively change the requirements and meaning of signature contained in those regulations.

3. On the legal acceptance issue, we have not found any specific legal deterrents to the admissibility of electronic records. However, the admissibility of such records hinges on the trustworthiness of the records, as demonstrated by administrative controls, adequate security measures, and system validation. Electronic signatures, per se, are not addressed in the references we have encountered thus far.

4. On the issue of enforcement integrity, electronic records pose a greater opportunity for undetected falsifications and the agency stands to lose the benefits attendant to physical evidence existing in paper documents. However, existing Title 18 provisions of the U.S. Code should furnish the agency with sufficient tools to pursue cases of electronic fraud. Additional investigative tools and training may be needed in the future as the agency encounters more documents in electronic form.

5. There are legitimate differences in the degree of acceptance of signature alternatives among the various centers. Regulations within a given center may also differ in accepting various levels of signature alternatives. However, such differences should not prevent the agency from approaching the matter on a multi-center basis.

6. Security, validation, system reliability and the agency's enforcement integrity must all be preserved by whatever signature substitutes are eventually accepted.

7. Whereas the group does not seek to evaluate specific technologies, but rather to develop appropriate policy on an agency wide basis, we would benefit from receipt of additional information on electronic record management and signature alternatives from the regulated industry and from technology developers and vendors.

8. The NIST DDS draft document does not present a viable signature standard, at this time, for the regulated industry or for FDA.

RECOMMENDATIONS:

The working group recommends:

1. The publication in the Federal Register, of an advance notice of proposed rulemaking. The notice would:

a. Announce that FDA is considering whether or not to develop regulations that would accept certain signature alternatives in documents required to be maintained by the regulated industry, under existing regulations, and documents submitted to the agency for review and approval. The agency's own electronic documents, with attendant signature substitutes, would also be addressed (e.g., acceptance as official, electronic correspondence which lack autographical signatures).

b. Describe the seven key issues, as mentioned in this report.

c. Invite comments from all interested parties and would welcome presentations to the working group by such parties. (We have already received offers to hear such presentations from system vendors and the pharmaceutical industry.)

d. Identify the working group as the primary agency contact for further information. The working group would receive and evaluate the comments.

e. Allow a comment period of 90 days.

f. Incorporate this report by reference. The report and referenced documents should be made part of the administrative file that is maintained by the Dockets Management Branch.

2. Codification of general signature alternative acceptance provisions, should that be indicated by comments to the above Federal Register notice. In order to cover as many different commodities and centers as possible, it is the recommendation of the working group that such codification be established in a single regulation in the CFR. (Perhaps one of the currently reserved subparts (C and D) of Part I, General Enforcement Regulations, would be appropriate. Differences among the centers, and regulations within the management of each center,

may be accommodated by a multi-tiered approach, with the closest analogs to conventional autographical signatures being linked to the most significant regulatory/legal documents.

3. Consideration by agency FOI program managers of how the agency can fill requests for electronic documents, where requests themselves may take electronic or paper form, and in cases where electronic media may or may not be furnished by the requestors.

4. Development of specific training for field investigators on collection and handling of electronic records.

5. Evaluation by the Winchester Engineering and Analytical Center of electronic identification systems, made available by vendors on a loan basis, where such evaluation is executed by non-destructive testing to identify various features and weaknesses that might be addressed in implementing regulatory/policy documents issued by the agency.

6. Continuation of current regulatory and policy requirements and interpretations of "signature" and endorsement requirements until changes that may result from this project are implemented. The group believes it would not be prudent to adopt alternate interim policies until the issues addressed in this report have been fully resolved.

7. Continuation of the working group, as an agency wide entity to address the issues and develop and coordinate appropriate regulatory and policy documents. We anticipate a cessation of the group upon final codification of appropriate regulations and publication of ancillary policy documents.

ADDITIONAL INFORMATION:

The working group is in the process of gathering additional information from other federal agencies, system vendors, and FDA personnel. That information will be furnished in supplementary reports.

Paul J. Motise
Chairperson and
Center for Drug Evaluation and Research Representative

Martin Browning
Vice Chairperson, and
Office of Regional
Operations Representative

Tom M. Chin
Office of Enforcement

Boyd Fogle, Jr.
Center for Biologics
Evaluation and Research

Jo Gulley
Center for Veterinary
Medicine

Christine Nelson
Center for Devices and
Radiological Health

David Hamrick
Office of Information
Resources Management

Seth Ray,
Office of General Counsel

Len Valenti
Center for Foods and
Applied Nutrition

P. MOTISE
2/24/92
DOC ID ESIGRPT1.PJM

REFERENCES:

1. Letter from Kenneth G. Chapman, Director Quality Assurance Audit, Pfizer, Inc., Groton, CT, 8/23/91, to Ms. Mary Jo Veverka, Deputy Commissioner for Management & Policy.

2. Federal Information Processing Standards Publication (Draft), August 19, 1991, "Specifications for a DIGITAL SIGNATURE STANDARD (DSS)", published by the National Institute for Standards and Technology (NIST).

3. Memo, 11/12/91, from Mary Jo Veverka, Senior Advisor for Management and Information (HF-20) Subject: Proposed Electronic Identification Standard, to Bill Lampkin, Bob Lake, Paul Vogel, Fred Hooten, Tom Bozzo, George Mitchell, Tom Reddin, Margaret Porter, and Don Sauer.

4. Memo, 11/20/91, from William T. Lampkin, Director, Division of Compliance Policy (HFC-230), Subject: Electronic Identification - Digital Signature Working Group.

5. Memorandum of Meeting, 11/26/91, Subject: Electronic Identification - Digital Signature Working Group.

6. Search conducted 10/15/91 on CDER's VAX CD-ROM system, FDA_ON CD-ROM, a commercial program under copyright by Quantum Access, Inc., Houston, Texas. (Search conducted by Paul Motise.)

7. Memo, 2/14/92, from Deputy Director, Office of Information Resources Management (HFA-51) to Director, Division of Compliance Policy (HFC-230), Subject: Electronic or Digital Signature Usage by Other Government Agencies.

8. Government Computer News, 9/16/91, pg. 60, "No Signature on Paper? No Problem, Official Says", by Karen D. Schwartz.

9. Memo, 1/29/92, from David R. Hamrick (HFA-51) to William T. Lampkin (HFC-230), Subject: Status of Investigation of Other Agencies Handling of Digital Signature.

10. Government Computer News, 1/6/92, pg. 37, "Customs Imports Arrive Faster With EDI", by Karen D. Schwartz.

11. Federal Computer Week, 9/16/91, pg. 4, "Treasury Plans Automated Securities System", by Richard A. Danca.

12. Government Computer News, 9/2/91, pg. 88, "Rail Carriers Provide PCs to File Electronic Tariffs", by Kevin Power.

13. Government Computer News, 9/16/91, pg. 3, "FCC Considering Electronic Filing In Upgrade Plans", by James M. Smith.

14. Federal Computer Week, 11/4/91, pg. 23, "Pen-Based PCs Slice Through Navy Paperwork", by Carolyn Duffy Marsan.

15. Decision paper, 12/13/91, Comptroller General of the United States, Washington, D.C., File: B-245714, Matter of: National Institute of Standards and Technology--Use of Electronic Data Interchange Technology to Create Valid Obligations.

16. United States Department of Justice, Justice Management Division - Systems Policy Staff, "Admissibility of Electronically Filed Federal Records As Evidence", October 1990.

17. Federal Computer Week, 11/4/91, "DOJ Issues Guide for Records Managers", by Ann M. Mercier.

18. U.S. Department of Justice, 11/88, "Basic Considerations in Investigating and Proving Computer-Related Federal Crimes, available from the Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. 20402.

19. Reprint of "The Legal Status of Optical Disk and Electronic Imaging Systems", by Donald S. Skupsky, pp. 439-442, from Legal Requirements for Business Records, Copyright 1989 by Information Requirements Clearinghouse, Denver, CO. (Reproduction authorized by the author by letter of 2/14/92).

20. FIRM BULLETIN B-1, 1/30/91, TO: Heads of Federal Agencies, SUBJECT: Electronic records management, from General Services Administration.

21. PHS IRM Manual, Chapter 11, PHS Transmittal 91, page 21-22, and Exhibit 11-C.

22. Memo, 12/4/91, from Richard L. Arkin, Regulatory Counsel, HFD-362, Subject: Background information for the PDMA (electronic signature) meeting, with attached excerpts from proposed Federal Register notice.

23. Article by Mitch Ratcliffe, MACWEEK, 12/10/91, Vol 5 No 42 "Trapdoor unhinges DSS security".

24. Article by Richard A. Danca, Federal Computer Week, September 2, 1991, pg 3, "NIST Signature Standard Whips Up Storm of Controversy From Industry".

25. Government Computer News, 12/23/91, pg. 1, "Board Finds NIST's DSS Unacceptable", by Darryl K. Taft.

26. Memo, 2/20/92, from Director, Office of Information Resources Management/FDA to Director, Office of Organization and Management Systems/PHS, Subject: NIST's Proposed Digital Signature Standard

27. Federal Computer Week, 12/2/91, pg. 53, "Group Seeks Public Access to Federal Records.

28. Excerpts from the CGMP regulations, Sections 211.186, 211.182, 211.194, 211.110, 211.115, 211.188, and 211.192, DOC GMPPARTS.WP, P. Motise 11/22/91.

29. Memo of meeting, 5/15/91, PMA/FDA, Subject: Computerized Drug Processing; Electronic Signatures and Automated Alternatives to Human Actions, Paul J. Motise.

30. Letter, 11/25/91, from Thomas X. White/PMA to Daniel L. Michels/FDA regarding implementation of electronic identification within the CGMP regulations.

31. Letter, 12/5/91, from Sammie R. Young/FDA to Thomas X. White/PMA, responding to Mr. White's 11/25/91 letter.

32. Memorandum of Meeting, July 19, 1991, Burroughs Wellcome Co./FDA, Subject: Electronic Signatures/Electronic Records, by Paul J. Motise.

33. Citizens Petition, 10/18/91, from Burroughs Wellcome Co., Greenville, NC 27835-1887, by signature of Donald A. Knight, Director, Division of Drug Regulatory Affairs.

34. Memo, 11/1/91, from Chief Compendial Operations Branch, HFD-335, to Richard A. Baldwin, Director, Division of Field Sciences, Subject: ORO Research.

35. Interoffice Memorandum, 12/17/91, from Thomas Layloff, HFH-300, to Paul Motise, HFD-323, Subject: Re: Electronic Signatures - Your Views Requested.

36. Interoffice Memorandum, 1/29/92, from Dave Moss, HFD-070, to Paul Motise, et. al. (CDER ADP Focal Points), Subject: MCImail - An Update.

37. Interoffice Memorandum, 1/24/92, from Dave Moss, HFD-170, to Daniel Michels, et. al, Subject: RE: MCI Mail.

38. Interoffice Memorandum, 1/12/92, from Dave Moss, HFD-070, to Paul Motise et. al, Subject: RE: MCI MAIL -- ISSUES.

39. Interoffice Memorandum, 1/9/92, from Paul Motise, HFD-323 to Dave Moss et. al, Subject: MCI MAIL -- ISSUES.

40. For example, Interoffice Memorandum (FAX copy), 11/14/91, from Paul J. Motise, HFD-323, to Pharmaceutical Engineering and Design Limited/Mr. John Wilson, Surrey, England, Subject: Tungsten Carbide Bearings, Fax Inquiry.

41. Interoffice Memorandum (Fax copy), 11/19/91, from Paul Motise, HFD-323, to Mr. Al Lavender, Arthur A. Checchi, Inc., Wash., D.C., Subject: Fax Inquiry RE: ETO.

42. Federal Computer Week, 2/3/92, pg. 1, "Drug Approval System Wins Presidential Priority Status", by Kevin M. Baerson.

43. Government Computer News, 2/3/92, pg. 1, "Bush seeks big boost for priority systems", by Kevin Power.