UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

October 23, 1995

MEMORANDUM TO: Lloyd Donnelly, Director
Financial Management Procurement and Administration Staff
Office of Nuclear Regulatory Research

FROM: Arnold E. Levin, Deputy Director
Office of Information Resources Management

SUBJECT: PROPOSED PILOT FOR THE USE OF DIGITAL SIGNATURES

The Office of Information Resources Management (IRM) is not responsible for determining the legality of your proposal for using electronically generated, digitized signatures for your Department of Energy (DOE) contract pilot under the Resource Information Management System (RIMS). We are, however, responsible for pointing out the technical pitfalls and issues related to any proposal for the generation of electronic signatures and for ensuring that any method for doing so fits within an overall agency framework for using digital signatures. The method you plan to use in your pilot is nothing more than replication of a signature electronically--not digital signaturing. As such, if that is determined to be legally permissible for the pilot, IRM has no objection to its use. Likewise, the replication of signatures electronically is not an agency standard issue as long as it isn't used in the same context as digital signatures.

As you are no doubt aware, IRM has been exploring Electronic Information Exchange (EIE) technology and the related legal and records issues for some months now from an agency-wide perspective. We are charged with developing a strategy to assist NRC management in deciding what business transactions make sense to convert from paper to electronic means. We hope that strategy will be available for review and comment at the end of this calendar year. Electronic (a.k.a., digital) signatures are one aspect of the EIE topic. Substituting some form of digital signature for the customary and accepted "autograph" is a particularly difficult issue, with many complicated areas of concern.

IRM has the responsibility to select and apply enabling hardware, software, systems, and procedures in a standard way for all agency needs. This is both a technology task for us and a computer security task. However, technology is not the limiting factor. We already know how to apply electronic signatures and to exchange information electronically. The limiting issues are related to business, legal acceptance, and records storage.

Business...what is the business case for using EIE? Is it cost effective? Can efficiencies in processes be shown that offset the costs and risks of the new approach? Just because we can do EIE does not mean we should.

Legal...which method of accomplishing electronic signatures is the acceptable equivalent to the hand written signature?

Records...what records retention, distribution, and retrieval requirements exist for paper and how would they be accommodated in the electronic world?

Your pilot involves replicating signatures electronically and transmitting their associated document via fax; however, many of the same concerns will apply and have to be resolved. In general, what will constitute an acceptable electronic signature will depend on the nature of the transaction. IRM cannot certify that the method you propose for your pilot will generate a signature that is technically certifiable as being authentic, tamper-proof, or non-forgeable. For instance, it would be a very simple matter for even relatively unsophisticated computer users to capture a signature from one of your electronically created documents and replicate it on other documents. Likewise, it would be easy to electronically manipulate the contents of your electronic document (change numbers, words, dates, etc.) and reprint it. In both cases, under your scheme, the "forgery"/alterations would be absolutely undetectable.

At the October 31, 1995, SIRMO/ITC meeting, Chuck Fitzgerald will be giving a briefing on our EIE strategy background, status, and future steps. This information will be a great help to you, OC, OGC and any others involved in your proposed RIMS pilot. IRM staff will also be at the November meeting you called on this topic.

cc: G. Cranford, IRM
W. Olmstead, OGC
B. Kildee, OGC
R. Scroggins, OC
P. Norry, ADM
E. Halman, ADM

Distribution:
IRM/DD r/f
SDIB r/f
SDIB s/f

DOCUMENT NAME: P:lloyd

To receive a copy of this document, indicate in the box: "C" = Copy without attachment/enclosure "E" = Copy with attachment/enclosure "N" = No copy

OFFICE	IRM/SDIB		IRM/DD							
NAME	CEFitzgerald	CEF	AELevin	AEL						
DATE	10/23/95		10/23/95							

OFFICIAL RECORD COPY

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

OCT 11 1995

MEMORANDUM TO: Jesse Funches, OC/DO
Edward Halman, ADM/DC
Moe Levin, IRM/DD/LSSA

FROM: Lloyd Donnelly, Director
FMPAS/RES

SUBJECT: DIGITAL SIGNATURES ON DOE CONTRACT PAPERWORK

For two years now, RES has been developing a capability to create and process DOE procurement packages electriconally within the Resource Information Management System (RIMS). At the outset, I obtained a legal ruling (attached) on the use of electronic signatures. The ruling was that such signatures are legally acceptable providing the system and its use of electronic signatures were acceptable to IRM, OC, and ADM.

Over the past several months, we have had discussions at Financial Manager's Council meetings on the use and various forms of electronic signatures. I also gave the Council demonstrations of RIMS, its content, and how it would be used to produce procurement paperwork. At one meeting it was decided that RIMS and one other project in OC be used as pilots for the use of electronic signatures.

To date I have received nothing but positive endorsement of what we are trying to do within RIMS. Therefore, absent any objection, I plan to implement the electronic signature pilot here in RES for the issuance of DOE procurement paperwork. The pilot will start November 1, 1995, and will consist of replacing the ink signatures on the DOE work order (NRC Form 173) for the Funds Certifying Official and the Issuing Authority with digital signatures. The digital signatures will be imprinted to the Form 173 using a laser printer. The signatures will be created from the appropriate person's own signature by electronically scanning their signatures and storing them as graphic image files within RIMS. These signatures can only be transferred from the database to the electronic version of the Form 173 when the person having the issuing or certifying authority has indicated approval within RIMS. The ability to give these approvals is restricted first by a unique RIMS password and then by limiting access to the approval screens (through RIMS software) to only those individuals having the authority to make such approvaals.

There are several advantages to the above use of electronic signatures and electronic processing. They are:

- Errors are reduced and duplicate data entry is eliminated since much of the information to be input to the forms is done automatically from the existing RIMS database;

OCT 11 1995

- Efficiency is increased by allowing electronic paperwork to be processed through as many as seven processing steps without sending paper copies to these processing points;

- Productivity is increased by allowing paper copies to be generated from a high speed laser printer (versus copy machines);

- Productivity is increased by allowing procurement packages to be FAXED to DOE laboratories/field officies from a PC-based FAX modem;

- Electronic storage and recall of DOE procurement packages (complete with signatures) is possible. (Note: A paper copy will be maintained as part of the official project management file.)

- Status checking is facilitated since anyone in RES can query RIMS, at any point in the paperwork processing cycle, to check on procurement package processing status.

I believe these advantages support moving forward with the pilot at this point in time. I will keep all interested parties informed on the progress of the pilot effort.

Attachment: As stated

cc: B. Kildee, OGC
A. Lipuma, OIG

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

September 2, 1993

MEMORANDUM FOR: Lloyd Donnelly, Director
Financial Management Procurement
and Administration Staff

FROM: Brian Kildee, Attorney
Office of the General Counsel

SUBJECT: ELECTRONIC SIGNATURES

Your May 21, 1993, memorandum advises that RES is designing and will soon be implementing the Research Information Management System, or RIMS, an automated information system which will be used to facilitate project management and financial management within RES. A portion of RIMS will be used to process DOE work orders and Requests for Procurement Action (RFPAs). You advise that RES would like to use electronic signatures to approve these actions and to certify funds under this automated system and you ask if this is legally permissible.

As I understand it, RIMS will encompass those responsibilities assigned to Allotment Financial Managers in the draft Handbook for NRC Management Directive 4.2. Specifically, the system will permit specified RES staff members to process administrative forms as necessary documentation, approvals and funding certifications are obtained. The final RES document conveying these approvals and funding certifications outside of RES, to DCPM in one case and DOE in the other, will be in paper format. The only visible difference envisioned between current RFPAs and DOE work orders and the same documents under RES's automated system will be a notation in the appropriate blocks of electronic signature, rather than hand signature.

As noted, RES will use RIMS to control two categories of nonexpenditure transactions, i.e., the allotment of funds to contracts and DOE work orders. In the case of contracts, RES will use the system to certify the availability of allotted funds for particular work, but not to obligate funds. DCPM will continue to obligate contract funds separately at time of award. In the case of DOE work orders, the RIMS certification will be the last NRC step needed to obligate funds. As is the case now, DOE's subsequent signature accepting the work order will create the obligation which OC records when it receives the work order.

RES plans to safeguard RIMS by requiring, in addition to the usual password to log on the NRC system, a second password to log on to RIMS. The system will limit each individual's ability to edit and view data in accordance with the needs of his or her

assigned function. For example, certifying officers, who are at the office level, will not be able to modify the dollar amounts, which will be entered at the division level. Some individuals will have edit capability and others will be limited to a read-only capability. The system will allow only those RES officials whose signatures are needed to authorize work and certify funds to have access to those fields that cause the system to print "signed by" and that individual's name in the appropriate signature block on the form.

As a general matter, federal computer systems must comply with the requirements of the Computer Security Act of 1987, 40 U.S.C. § 759, note, which requires that each agency prepare computer security plans "commensurate with the risk and magnitude of the harm resulting from the loss, misuse or unauthorized access to or modification to the information contained in such system." Appendix III to OMB Circular A-130 implementing this statute requires security specifications for new systems, design reviews to assure proposed designs meet approved security specifications, certification that the system meets all applicable regulations, and periodic recertifications.

Within NRC, IRM has primary responsibility for determining whether RIMS satisfies the standards of the Computer Security Act of 1987 and Appendix III to OMB Circular A-130. This determination is primarily a question of informed technical judgment, balancing the degree and magnitude of risk against administrative costs. IRM can draw upon technical standards and guidelines for the security of federal computer systems developed by The National Institute of Science and Technology under 15 U.S.C. § 278-g-3 when making this determination.

Because RIMS is a financial system, it must also satisfy any special requirements imposed on such systems. The federal entity with primary responsibility for establishing standards for financial systems is the GAO, which coordinates such standards with Treasury and the Office of Management and Budget. To date, GAO has not issued guidance on the question of electronic signatures for nonexpenditure transactions. The GAO has approved the use of electronic technologies to process vouchers for payments, including the certifying function. See Subchapter 7.4 of the GAO Policy and Procedure Manual, May, 1993. This manual requires that the certifying officer's electronic signature be (1) unique to the certifying officer, (2) capable of verification, and (3) under the sole control of the certifying official when such signatures are used to certify vouchers. As noted earlier, the RIMS system will not be used to certify vouchers or for other expenditure transactions. However, electronic signatures which satisfy GAO's security requirements for expenditure transactions are clearly adequate for nonexpenditure transactions, given the reduced risk associated with nonexpenditure transactions.

Title 2 of the GAO Policy and Procedures Manual establishes accounting standards for financial systems which RIMS must follow. Appendix II to that title, "Internal Control Standards" defines the standards of control required for accounting systems. These standards cover a range of topics, including execution authority, separation of functions and access limitations. While these broadly stated standards cover automated systems, they do not contain specific guidance on automated systems. Appendix III to this title, "Accounting Systems Standard," does provide specific guidance for automated systems, including transaction processing and production control (pg. 2-7), system security and protection (pg. 2-11), and authorization or access control (pg.2-17). Together, these two appendices provide comprehensive guidance on GAO's requirements for financial systems.

If RES wishes to pursue this matter, it should ask OC to review and approve the entire RIMS system, including its proposed method of signature, in light of applicable federal standards for financial systems. When conducting this review, OC should determine whether it is necessary to impose the more rigorous electronic signature requirements associated with expenditure transactions on a system such as RIMS which does not involve expenditure transactions. RES should also contact IRM and verify that RIMS conforms with the general security requirements for federal computer systems.

Further, Exhibit VI-3 of the handbook for draft NRC Management Directive 4.2 imposes general requirements on certifying the availability of funds for both Financial Certifying Officers (FCOs) in OC and Allotment Financial Managers (AFMs) in the program offices. One requirement is that the FCO and AFM "must sign and date the certification in ink." Since the draft NRC Management Directive 4.2 requires that certifying officers sign by hand, it would be inappropriate to include electronic signature capabilities in RIMS at this juncture. Therefore, RES must also obtain OC's approval to deviate from the NRC requirement that documents certifying the availability of funds be signed in ink.

Finally, the signatures on RFPAs and DOE work orders evidence things other than funds certification, such as showing that the work itself is authorized by an appropriate agency official. For this reason, the use of electronic signatures on these documents should be coordinated in advance with DCPM and other interested offices.

In summary, electronic signatures are legally permissible and certifying officers may use such to certify the availability of funds under the conditions and subject to the approvals noted above.

Brian Kildee, Attorney
Office of the General Counsel

cc: T. Hagan, DCPM
B. Shelton, IRM
C. Miller, OC
R. Rokowsky, OC
C. Turner, OC
J. Dorfman, OC
D. Hassell, OGC