ITS NEWS

WINTER 1992
Vol. 8, No.1
NUREG/BR-0056

Information Technology
Services Support Center
and Training Laboratory

U.S. Nuclear
Regulatory
Commission

Office of Information
Resources Management

Office of Personnel

The Threat Is Always Present

By Emily Robinson, IRM

What threat?

The threat of computer virus infection on your diskettes or in your microcomputer.

The threat of computer virus infection that may damage your memos, your spreadsheets, your briefings, your valuable work products! It may also damage your system software and your standard software packages, i.e., IBM PC-DOS, dBASE III.

The threat of computer virus infection that was perpetrated maliciously at first, but is often introduced inadvertently as people share software, send diskettes to one another, or take information from unchecked sources (some reputable bulletin boards and computer services are already scanning for viruses, because of the worldwide epidemic).

Remember the mainframe era? Even then, your information was at risk from other users. Everyone worked on terminals connected to the central computer system, and programming errors could destroy a user's data. All the security features and integrity management were then the responsibility of the mainframe operating system and its administrators. The user didn't have to worry about such things.

Now we're in the personal computer (PC) era and the situation has changed considerably. Five years ago the first recorded PC virus appeared, and the most common ones (Jerusalem and Stoned), are now 3 years old and show no signs of going away in this country or abroad.

Your computer hasn't been infected yet? Lucky you!! But watch out, this threat can occur when you least expect it. Surely you know someone who has experienced a computer virus and wondered how all this could have happened.

It happened because the most common microcomputer operating system, IBM's PC-DOS, has limited built-in integrity check and protection. DOS will happily attempt to execute anything presented to it, and the common viruses activate when an infected file is executed. Those integrity management programs that exist now have been layered on top of DOS and owe their success to the relatively unsophisticated nature of the virus attacks. Already there is an increase in boot-sector viruses (the part of DOS that starts up your computer) and partition-table infections (the part of DOS that assigns your file to tracks, a diskette or a hard disk). Recent discoveries in Europe indicate that much more innovative attacks are coming. Integrity software tools face an uphill development battle because

(Continued on Page 2, "Threat")

("Threat" Continued from page 1)

commercial pressures urge them to be as widely useful as possible while the user community want them to maintain compatibility with all IBM PC-DOS versions.[1]

Local area network (LAN) architecture is relatively new, by comparison, and has been developed with features for possible implementation of stronger security and virus control. However, these features are not always used because of system response degradation. LANs connected to other LANs, through gateways and bridges, permit other opportunities for viruses to travel.

You, the user, have a defense shield. It is called virus detection software. Presuming your stand-alone PC or network system is virus free, the prime infection source is a diskette that carries a virus. For your own protection, the safety of your work, and in consideration of people who share the network with you, please get a virus checking software package and check every diskette that you receive. To be sure that a boot-sector virus is not hiding in your system, boot up from a known virus-free, original, write-protected DOS disk, and then use the virus detection software. The NRC has a site license for IBM VIRSCAN and you can get the latest version by calling Dara Gordon on 492-9974 or FTS 492-9974.

The NRC has established self-service disk-scanning centers in the following locations:

ITS Center, Phillips Building Penthouse

ITS Center, OWFN 3 C8/10

You are encouraged to check any and all disks received from an outside source before using them.

Recently IRM conducted two virus seminars, one on November 7th, with James Vavrina, U.S. Army as speaker; and another on December 2nd, National Computer Security Day, with Jim Polk, National Institutes of Standards and Technology, as speaker. More than 40 staff members signed up to obtain virus checking software. **Did you?** ■

The virus seminars were videotaped. The Cliff Stohl video "The KGB, The Computer and Me" is also available. You may borrow these tapes by calling Emily Robinson on 504-3490 or FTS 964-3490.

"Computers Under Attack" by Peter Denning, Addison Wesley, 1990. A much-quoted book now available in the NRC Library.

[1]"There Will Always Be a Threat," *Information Security Product NEWS*, May/June 1991.

Disposal of Classified and Sensitive Unclassified Paper Waste

By Wayne G. Burnside, ADM

The Nuclear Regulatory Commission (NRC) uses one method for the collection and destruction of classified and sensitive unclassified paper waste, and another method for non-paper media (e.g., computer diskettes, ribbons, and microfiche). Receptacles for the collection of classified and sensitive unclassified paper waste have been placed in numerous locations throughout all Headquarters buildings. Do not place non-paper media in these receptacles.

The Division of Security (SEC) collects the paper waste each Wednesday for transport to a facility where it is destroyed and recycled. Non-paper media are collected by request. When a sufficient quantity is accumulated by SEC, it is then transported to a facility where it is destroyed.

Employees who have non-paper media to dispose of should contact SEC's Facilities Security Branch on 492-4122 or FTS 492-4122. ■

THE ISSUE AT HAND

* * * * *

ITS NEWS CREDITS

The ITS NEWS is a quarterly publication providing information of interest to users of computer technology at the NRC. It is produced by the staff of the NRC Information Technology Services Support Center and Training Laboratory in conjunction with the NRC's Office of Personnel.

We welcome questions and comments and articles.
Please contact the ITS staff by:

Phone: 492-8309
Mail or in Person: MNBB-7602

Ina Schwartz, IRM/TTSB
Executive Editor

Graduate School/USDA
Publication Coordination

Alvin Blunt, IRM/TTSB
Design Consultation

Illustrations and Concepts by NRC Automated Graphics Section

Contributors to regular items are: M. Holmes, C. Madison, E. Robinson, P. Smith, C. Merrill.

Loose Bits Sink Ships

By Kathleen M. Padgett

(This article is reprinted, with the author's permission, from the Los Alamos National Laboratory, Security System Bulletin, Vol. 6, No. 1 (1991), p. 5.)

Computers have become such a common part of our daily routine that we hardly notice them. Our lack of awareness, coupled with an ingenuous attitude toward the importance of the information computers contain, can lead us to sink our own ship and the ships of others as well.

Several months ago, the following headline appeared in the newspaper: "Britain's Gulf War Plans Lost in Theft--Computer Taken from Car in London." The officer who had custody of the computer had casually left it on the back seat of an unlocked car, and the computer was stolen.

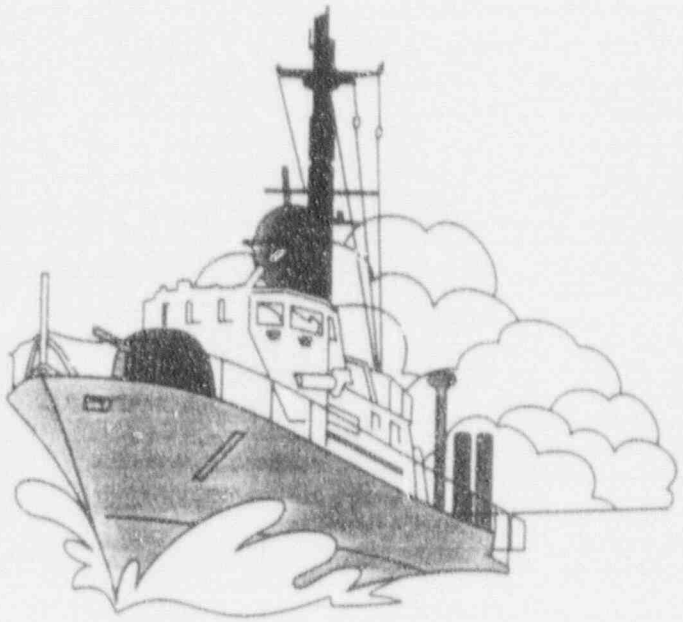
At one national laboratory, a graduate student who was doing leading-edge research for his doctorate left for a holiday without securing his computer or data files. The student's notes and research were stolen from the computer by his advising professor, who published them under his own name.

Data does not always have to be classified for its loss, damage, or theft to have a catastrophic effect. In the academic area, researchers are often touchingly naive when it comes to protecting their data. Being out of the commercial main stream, they do not realize the value that research can have. The private sector fully realizes its value. Many companies protect research and development data at a level commensurate with Top Secret.

Consumers are also naive about data protection. Virtually no one gives their ATM receipt or social security number a second thought, yet to a thief armed with this information, a consumer's private banking data is an open book. Bank clerks have been known to make a duplicate ATM card for someone without even requesting positive identification first. All this individual had to know was the account number. Private and federal investigators; people with connections into the banking, lending, or investigative professions; and disgruntled employees working in those fields can get consumer information from loosely protected data bases. For a nominal fee, through a private investigator, FDIC and FSLIC account activity records are available on the individual bank account level, showing all balances and banking activity for that particular account. These reports are for sale to investigators by company employees. It has been estimated that as much as 90 percent of computer fraud is perpetrated by employees.

In the credit information field, credit bureaus and other credit reporting agencies are also noticeably lax with consumer information, so lax that an illegal industry has come into existence. For a fee, the consumer can get his/her credit report cleaned up, have a sterling credit report substituted, or get "confidential" information on others from the credit databases. In some cases of revenge, bad credit reports have been generated for former spouses or others perceived to be enemies. Within the last two years, a juvenile hacker entered the files of a major national credit reporting agency, copied out account numbers, and published them on a computer network bulletin board. One of the major bank credit cards has just announced that it will set up a charge approval system that will transmit over a radio network. No mention was made of data protection.

Virtually all computer data are sensitive from some perspective. Individuals need to be aware of data sensitivity or value and should not distribute information thoughtlessly. In the case of information that may be classified, individuals must take the initiative immediately to [indicate] the level of the information, not casually mention a week later, "Oh, by the way, that data is classified." Such incidents cost hundreds of dollars in recovery time and effort. We must all learn to practice responsible computing every day. Remember, loose bits CAN sink ships! ■



Software Quality Innovations

By Mark E. Stella, ACRS

This article briefly describes some of the issues associated with the increasing use of software-dependent systems in safety-related applications at nuclear power plants.

Software Engineering

In much the same way as a hardware component is developed from a concept to reality, a specific article of software can be created through the application of a systematic engineering process. Software engineering is the term used to describe this systematic process, which encompasses the definition of the required functions of the software, the logical design of the software, its coding (or programming), and testing to prove its integrity and suitability for use in a larger system that includes both software and hardware.

Because the use of digital technology is increasing throughout our society, it becomes ever more important to ensure the integrity of the software used in these systems. The Software Engineering Institute is dedicated to the dissemination of technology and methods that will enhance the quality of the software used in all types of applications.

The Software Engineering Institute

The Software Engineering Institute (SEI) is a unit of the Carnegie Mellon University (CMU). It is a federally funded research and development center that is sponsored by the Department of Defense, (DOD) through the Defense Advanced Research Projects Agency (DARPA). The SEI mission is to provide leadership in advancing the state-of-the-practice of software engineering, with a goal to improve the quality of all types of systems that depend on software.

The SEI was founded in 1984 to support the defense software development and user community, but its charter has recently been expanded to permit it to apply its expertise in support of other government organizations as recommended by the U.S. Congress in 1990. It is staffed by more than 250 technical and support personnel, drawn primarily from industrial organizations and universities.

NRC Affiliation with the SEI

More than 900 participants from academia, industry, and government met in Pittsburgh for the 1991 Software Engineering Institute Affiliates Symposium during the week of August 26, 1991. Included in this large group were four NRC employees: Joe Joyce of NRR, Emily Robinson and Louis Grosman of IRM, and Mark Stella of ACRS.

The SEI maintains an affiliate program that supports a large number of organizations. Through its technology transfer programs, including the affiliate programs, the SEI hopes to accelerate the dissemination of information on new software engineering technologies and methods. Organizations can affiliate with the SEI at one of three basic levels: (1) the information exchange level, (2) the technology exchange level, and (3) through residence of individual technical personnel at the institute.

The NRC presently participates in the SEI affiliate program at the information exchange level, by supporting NRC staff members' attendance at the annual SEI Affiliates Symposium, by obtaining and loaning to staff SEI educational pamphlets and technical materials, and through informal discussions with SEI technical staff on specific topics.

Applicability of SEI Work to NRC Needs

The NRC staff members at this year's affiliates symposium were present, in part, to assess the potential applicability of SEI work to NRC's current and future needs for licensing and regulating nuclear power plants having computer systems important to safety.

A number of operating plants either have plans to replace, or have already started to replace, their older analog protection and control systems with digital systems. Evolutionary and advanced reactor designs now being reviewed by the staff, such as the General Electric Advanced Boiling Water Reactor (ABWR) and the Combustion Engineering System 80+, utilize computer technology extensively in their control and protection systems, as well as in their control room display systems. Each of these applications depends upon properly engineered software for reliable and safe operation and for obtaining the necessary level of performance.

The rapid conversion to digital technology in nuclear power plant

(Continued on Page 5, "Software")

"*IEEE Software Engineering Standards Collection*" including the Standard Glossary of Software Engineering Terminology.

"*Applied Software Measurement*" by Capers Jones, McGraw Hill Software Engineering Serie

Now available in the NRC Library.

("Software" from Page 4)

designs requires that the NRC staff increase its expertise in this area and, more specifically, in the areas of software safety and reliability. The need to obtain a better understanding of these topics drives the present NRC staff interest in software engineering and related technologies.

Active research at the SEI is under way in a number of areas. Three which may be of the most relevance

Not only the NRC but other regulatory agencies worldwide are being confronted with the challenging task of certifying the safety of high-performance nuclear power control and protection systems using complex software.

to NRC's present needs for improving internal software engineering expertise are the software process area, the software engineering techniques area, and the real-time distributed systems area.

In the software process area, the SEI has described a systematic approach to creating software based on the best practices used in American software development shops. Adoption of and adherence to a systematic process for software development can improve an organization's ability to consistently develop high-quality software. The requirement for the use of a controlled process in the design of safety-related systems, components, and structures is a key tenet of safety regulation for the U.S. nuclear power industry.

Software engineering techniques being researched by the SEI include a number of innovative methods for obtaining software with high reliability and integrity. The effectiveness of formal (that is, mathematically precise) methods for verifying the correctness of a software implementation is also under study by the technical staff of the SEI. The Nuclear Installations Inspectorate of Great Britain has recently suggested that the Sizewell B computer-based reactor protection system software be completely reviewed through testing that includes the use of such formal methods.

The real-time distributed systems research area at the SEI includes work on a so-called Zero Defects Applications Kernel (ZDAK). The ZDAK is a design approach that provides both diversity and redundancy, with assured reliability of function, in software important to safety. A simple block diagram of the Zero Defect Application Kernel (ZDAK) concept is shown in Figure 1. It relies upon the parallel operation of two similar software modules to achieve the desired system function: one module is complex and, therefore, virtually impossible to certify as reliable, and the second is quite simple and because of its simplicity, completely verifiable. The complex software provides the high performance necessary for normal system operation, while the simple software detects faults that may occur in the more complex part of the system and takes control of the system until the fault in the complex software has been cleared.

Not only the NRC but other regulatory agencies worldwide are being confronted with the challenging task of certifying the safety of high-performance nuclear power control and protection systems using complex software. Such software cannot, in principle, be tested completely to verify its reliability. The ZDAK and related design approaches are consistent with the licensing criteria and principles that have been found acceptable in the past for certifying the safety of mechanical systems. The expanded understanding of software engineering principles and practices that can be obtained by working more closely with organizations such as the SEI will enable the NRC staff to better assess the safety of digital systems now being planned and incorporated into nuclear power plant designs.

Questions may be addressed to Mark Stella on 492-7344 or FTS 492-7344. SEI documents and symposia presentation materials may be obtained from Emily Robinson on 504-3490 or FTS 964-3490. ■

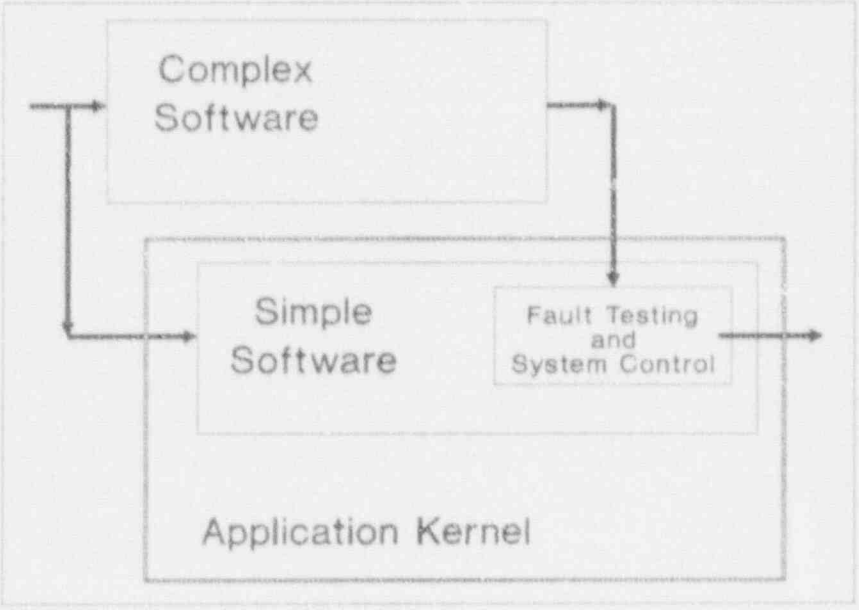


Figure 1. General Configuration of Zero Defect Application Kernel

Software Quality Assurance (SQA) Seminar Update

The August Software Quality Assurance seminar was very popular with NRC technical staff because it introduced software tools that are available to NRC staff on the INEL CRAY computer. Earl Marwil, an NRC contractor from EG&G Idaho Inc., presented a talk entitled, "Practical Experience with Software Tools to Assess and Improve the Quality of Existing Nuclear Analysis and Safety Codes." If you have computer programs that were developed before any structured emphasis on SQA, you may want to use these tools to verify the quality of your codes. Did you miss this seminar? Call Emily Robinson on 504-3490 or FTS 964-3490 to borrow the video for SQA Seminar #8. Videos of all previous seminars and handout materials are also available. ■

A Bit Too Literal

(From Editors Workshop Newsletter, Denville, NJ, June 1991)

At the dawn of the computer age, artificial intelligence was immediately pressed into service for translating documents from one language to another. The approach was quite straightforward. A Russian word in a bilingual dictionary is rearranged with the English equivalents into a sensible sentence.

Unfortunately, these literal translations often left much to be desired. When the Biblical phrase "The spirit is willing but the flesh is weak" was translated from Russian, it became "The wine is agreeable but the meat is spoiled" in English. Another program would have translated the slogan "Coke adds life" into the Chinese equivalent of "Coke brings your ancestors back from the grave." ■

Software Quality Assurance Training for the Division of High-Level Waste Management

By Kenneth R. Hooks and John T. Buckley, NMSS

The Division of High-Level Waste Management (HLWM), in the Office of Nuclear Material Safety and Safeguards (NMSS), has the responsibility to review the U.S. Department of Energy's (DOE's) application for a license to construct and operate a geologic repository for high-level radioactive waste. HLWM also has the responsibility to monitor and comment on DOE's site characterization activities during a pre-license application consultation period. As part of its efforts to characterize the site for the geologic repository and demonstrate compliance with NRC regulations, DOE must develop and use numerous software programs that model complex physical systems. HLWM must monitor DOE's development and use of this software. It may also develop and use its own software to verify the results of DOE models.

DOE is required under Title 10 of the *Code of Federal Regulations* (10 CFR, Part 60) to implement a 10 CFR Part 50, Appendix B quality assurance (QA) program and apply it to site characterization, design, construction, and operation activities of the high-level waste (HLW) geologic repository. This means that DOE software development and use must also comply with the QA regulatory requirements of 10 CFR Part 50, Appendix B.

HLWM has begun a training program for members of the technical and QA staff and the Center for Nuclear Waste Regulatory Analyses (CNWRA) (a federally funded research and development center contracted to provide technical assistance in the area of HLW) to improve their understanding of the development and implementation of appropriate QA controls for software, and methods for auditing the development and use of software under such QA controls. HLWM staff worked with Office of Personnel training staff to develop a statement of work (SOW) and, through competitive bidding, secure the services of a professional familiar with both computer software and QA to provide appropriate training for HLWM staff. The initial course was completed in August 1991, and was attended by personnel from HLWM, CNWRA, the NMSS Division of Low-Level Waste Management & Decommissioning, and the Office of Information Resources Management. A second training session is planned for April 1992.

The bulk of the 5-day course consisted of description and discussion of software QA program characteristics, based on a variety of United States and international standards. The software QA requirements described in the DOE Office of Civilian Radioactive Waste Management *QA Manual* were analyzed, as well as the guidance provided in "Final Technical Position on Documentation of Computer Codes for High-Level Waste Management" (NUREG-0856), and "Handbook of Software Quality Assurance Techniques Applicable to the Nuclear Industry" (NUREG/CR-4640). Prototyping of software, validation and verification of models, and documentation and auditing of software QA programs were also discussed in detail; and a sample QA audit checklist was reviewed.

The course will be modified, on the basis of student comments, so that the second session will emphasize quality software development more and auditing less. ■

NRC's Software Exchange and Information Activity

By Sharon A. Root, IRM

The Nuclear Regulatory Commission (NRC) recently entered into an agreement with the Department of Energy (DOE) to operate a software exchange and information activity for the NRC. This activity will provide the means for managing and controlling the dissemination of NUREG-documented computer software developed under NRC sponsorship. A central facility will serve as a software information center in support of NRC offices, NRC contractors, and the public.

This activity was previously performed for the NRC by the National Energy Software Center (NESC) at the Argonne National Laboratory. DOE centralized the management of its scientific and technical computer software by transferring the management function from NESC to the newly established Energy Science and Technology Software Center (ESTSC) at DOE's Office of Scientific and Technical Information (OSTI) in Oak Ridge, TN. The change consolidated DOE scientific and technical information management activities at one location.

ESTSC tests, packages, maintains, updates, distributes, and archives a library of NRC NUREG-documented computer software submitted to it by NRC staff and NRC contractors. Submitted software is screened for completeness and readability of computer media, and test problems are compiled and executed to ensure that they can be implemented as described in the associated NUREG. ESTSC assists software recipients in installing and using NRC software, and notifies them of corrections, revisions, and replacement releases as they are processed. ESTSC also coordinates with DOE and NRC staff regarding distribution of NRC-developed software to foreign countries.

For more information about the distribution of NRC scientific and technical computer software, please call Sharon Root on 504-2256 or FTS 964-2256. ■

Security in Electronic Messaging (e-mail) - Things You Should Know.

By Louis H. Grosman, IRM

Electronic mail, "e-mail," is one of the most popular applications designed for local area networks (LANs). By sending and receiving messages electronically, LAN users can communicate quickly and efficiently. Many LAN users are able to identify an immediate increase in personal productivity because of the reduction in "telephone tag."

Similar to the IBM 5520 Network, e-mail also allows users to flag a message as priority mail to call it to the immediate attention of the recipient. E-mail users can distribute messages to individuals, groups of users, or everyone on their LAN. One can send carbon copies and blind copies to other users and request a return receipt as is done with hard-copy memos.

E-mail has another useful function for the NRC workplace. As LANs are bridged together, one will be able to use e-mail to send files to users on other LANs. For example, a user on the Phillips Building LAN will be able to use e-mail to send a WordPerfect or Lotus file to a user on a LAN in White Flint.

Because many people will use e-mail to communicate information normally conveyed by telephone, they may fail to recognize the security risks inherent in this type of communication. E-mail messages are stored records of communications within a computer. Telephone conversations are not stored.

Government-provided e-mail is intended for official and authorized purposes only. E-mail users must exercise common sense and good judgment when using this Government resource. Personal and unofficial use is prohibited. NRC e-mail systems should not be used to disseminate information about any non-Governmental activities, including, but not limited to, charitable events, religious observances, fund-raisers, and personal business. Employees who abuse their e-mail privileges may have them withdrawn and may be subject to disciplinary action.

Employees must remember that **no** NRC LAN was designed with the safeguards necessary for handling classified (national security) information. Therefore, these systems must **never** be used for storing (even temporarily) or processing such classified information. Consistent with NRC policies, sensitive unclassified information (e.g., personal data, proprietary data, or data that have a high potential for financial loss), Official Use Only, and Safeguards data should only be entered in (or attached to) an e-mail message where expressly authorized by the policies of an NRC component.

Generally, e-mail system security features are placed in the context of communications security, which may include encrypting or scrambling message transmissions to prevent unauthorized access. Threats to individual privacy are increased with the widespread introduction of computer technology. When a computer is connected to a network, the information stored on the

(Continued on page 8, "Security")

("Security" from page 7)
network computer by an individual may become accessible to others, and individual control over this access may be limited. For example, some corporations have begun to scrutinize their employees' e-mail to determine if it is being sent for business purposes only. All commercial e-mail applications make some provisions for security, but security levels available among e-mail packages vary widely. These features generally include password access. For additional protection, messages can be encrypted upon transmission, and stored in an encrypted form to prevent unauthorized access.

An article in the November 1991 issue of ONLINE entitled, "Putting Out the Flames: the Etiquette of Law and E-Mail," offered the thought that, "The illusion of privacy with passwords and logon procedures may delude some e-mail users into thinking they have rights they do not have." The article concluded by saying, "Despite the illusion of privacy, e-mail is anything but confidential. Remember that your e-mail is an extension of and a reflection of you." ■

Local Area Network (LAN) Data Base Applications

By Gerald K. Tomlin, IRM/RES

For the past 4 or 5 years, the Office of Nuclear Regulatory Research (RES) has been using several database applications on its local area network (LAN). The RES staff uses these applications to maintain information on subjects such as research project descriptions, status of action items, foreign travel, international contacts, RES staff room and phone numbers, management and printing of contract data, and forms generation.

The applications were developed using a personal computer (PC)-based relational database software package, Paradox 3.5. This software, found on many NRC PCs and some networks, has proven easy for beginners to use. It also provides sophisticated and extensive capabilities which include an application language for application developers. One of its many virtues is that it runs very well on networks and allows the development of multiple-user applications. Such applications enable everyone on a network to share information while, at the same time, providing security for sensitive information.

Some of the LAN-based RES applications are as follows:

Research Project Management Information System: This system contains descriptions of active RES projects. Typical information consists of a project's title, RES project manager, contractor, budget, objective, status, research completed, planned research, deliverables, significant findings, and regulatory applications. The system is currently undergoing extensive modifications.

Action Tracking Management Information System: Tracking action items (such as those from WITS, or FOIAs) assigned to RES is the function of this system. Typically there are 80 to 90 items active at any one time and, at present, 1500 closed items in the system. Information in the system is maintained by the System Administrator, Anita Summerour, and can be referred to by anyone on the LAN.

Foreign Travel: RES staff travels abroad more than staff from any other NRC office. When RES staff initiate their plans for foreign travel, management assistants from each RES division enter those plans at their LAN-connected PCs. The System Administrator, Evelyn Gregory, then uses the system to send data on all RES planned travel to the EDO for the required approval and processing.

Foreign Contacts: This system contains a listing of nearly 500 international contacts doing business with RES in 132 organizations and 176 locations in 34 countries. The System Administrator, Evelyn Gregory, maintains the information for all RES LAN users.

(Continued on page 9, "NIH")

Controlling NIH Computer Timesharing Costs

By Herbert M. Parcover, IRM

There are several easy ways to reduce costs when you or your office are using the National Institutes of Health (NIH) computer system. The greatest savings (60%) can be realized by running print and/or batch jobs during discount periods. The discount periods are between 5:00 p.m. and 8:00 a.m. Eastern Standard Time during the week and at any time during the weekend. To have your batch run automatically during the next discount period, use the list command "DISCOUNT" or use the "//*DISCOUNT" statement after the job statement.

Money can also be saved by storing data sets on NRC private packs (i.e., NRC001 through NRC004) instead of public packs (i.e., File01 through File99). Simply resave your data sets on NRC packs, verify the new location, and then scratch the more expensive public pack storage. Also, scratch unneeded data sets and all migrated data that are of no further use. Where possible, move data to your personal computer (PC).

Lastly, eliminate all NIH access initials that are never used, by submitting an NRC Form 380 to Herbert Parcover, MNBB-7602. ■

("NIH" from page 8)

Electronic Phonebook: As its name implies, this is a listing of RES staff phone numbers, room numbers, and organizational components. The System Administrator is Jeff Wolman.

Contracts Funding: Used by the staff of RES's Financial Management Branch, this system quickly generates the package of documents necessary to transfer funds to DOE laboratories and other contractors for RES projects. The System Administrator is Mary Lee Bevan.

Using Paradox and its application language, stand-alone or network applications like the ones listed above can be quickly and easily developed for other NRC organizations. Similar Paradox applications are now operating in the Office of the Inspector General (OIG) and in the Office of Information Resources Management (IRM).

For further information or a demonstration of existing applications, contact Gerry Tomlin in RES on 492-3603 or FTS 492-3603. ■

FLOW!

By Emily W. Robinson, IRM

The Los Alamos Vulnerability and Risk Assessment (LAVA) software is being used at the NRC by the Codes and Standards Section staff for evaluating security of NRC computer systems with respect to environmental and human threats. As active users of LAVA, two NRC employees participate in the Federated LAVA of Washington (FLOW) User Group. The group held its first meeting at the NRC White Flint Building in July 1991 with 12 people in attendance from 8 agencies. The second meeting was held in conjunction with the meeting of the National LAVA User Group at the National Computer Security Conference, Omni-Shoreham Hotel, Washington, D.C., in October 1991. There were seven speakers, two from NRC. Emily Robinson, co-chair for FLOW, reported on the local group, and Dara Gordon gave a talk entitled "Experiencing the LAVA Process." In March, the local group plans to meet at the Interagency OPSEC Support Staff building in Greenbelt. ■

Artificial Intelligence User Group

By Leslie E. Lancaster, RES

The NRC Artificial Intelligence User Group (AIUG) met at the NRC White Flint building on November 19, 1991. The speaker was Russell J. Davis from the Planning Research Corporation.

He spoke on "Peeling the Viral Onion," which dealt with computer viruses and expert systems. Mr. Davis is very knowledgeable about computer viruses. He can be reached at (202) 453-9021.

The group met again at White Flint on January 14, 1992. The speaker was Dr. Milton White, Chairman, International Association of Knowledge Engineers, who spoke on the role of the knowledge engineer in artificial intelligence problems. Dr. White can be reached at 770-4621.

NRC is planning to sponsor artificial intelligence training courses and needs the support of the user group. If you have any suggestions or questions regarding these training courses, please contact Carolyn Bassin on 492-8526 or FTS 492-8526.

If you would like to join AIUG, obtain more information, or have any questions, plese call Les Lancaster on 492-3969 or FTS 492-3969. ■

In Memoriam
Grace Murray Hopper
1906 - 1992

Legendary Pioneer Computer Scientist U.S. Navy Rear Admiral, Retired

Many NRC staff were privileged to hear this courageous, brilliant, and tireless Navy Admiral speak at the Women's History Month celebration at the Crowne Plaza in March of 1989. In her lifetime, Adm. Hopper won many Navy awards, and in 1991 she received the National Medal of Technology from President Bush. She was a scientist, teacher, and challenger.

At the time of her retirement, the Navy Secretary said, "She has challenged at every turn the dictates of mindless bureaucracy." She was a creative force in the building of the first large-scale digital computer, the MARK I, and subsequent MARK versions, as well as the UNIVAC I. She created the initial design of the COBOL language, and developed many new software tools. Her sense of humor was delightful, and she loved to tell the story about debugging the MARK I...when the first "bug" was literally a 2-inch moth that died in the circuitry.

Adm. Hopper was one of the great contributors to twentieth century knowledge, and will be impossible to replace!

NUDOCS NEWS
NUCLEAR DOCUMENTS SYSTEM NEWSLETTER

The NUDOCS/AD User Suggestion Box

NUDOCS/AD User Support services answers questions for all NUDOCS/AD users. The On-Line User Suggestion Box is just one of the many services administered by this group. The Suggestion Box gives users of NUDOCS/AD the opportunity to express opinions and voice concerns about the NUDOCS/AD system, to ask questions, or to share NUDOCS-related information with other users.

Access

To access the Suggestion Box, use the **TAB** key at the NUDOCS/AD Main Menu to position the cursor next to "User Suggestions." Press the **ENTER** key. (See Figure 1)

The On-Line User Suggestion Box Screen

The Suggestion Box screen is divided into three areas as shown in Figure 2.

The Identification Area

The top area of the screen is used to identify suggestions and their authors. Fields in the identification area include:

Name: When the Suggestion Box is accessed, the cursor will be located at the Name field. Type your name and press the **ENTER** key. The cursor will move to the Subject field.

Subject: Type a short description to identify your suggestion and press the **ENTER** key. The cursor will move to the Phone Number field.

Phone Number: Type your office phone number and press the **ENTER** key. The cursor will move to the Priority field.

Date: The current date is automatically provided by the system. No changes are necessary in this field.

Priority: The Priority code is a numeric value between 1 and 9 that indicates the priority level of the suggestion. A priority value of "1" represents the highest priority. A priority value of "9" represents the lowest priority. The default priority value is "5."

The Priority code may be changed by typing over the default code of "5." Press the **ENTER** key when the Priority code is set. The cursor will move to the suggestion area.

Status: The status code is assigned

(Continued on page 11, "NUDOCS")

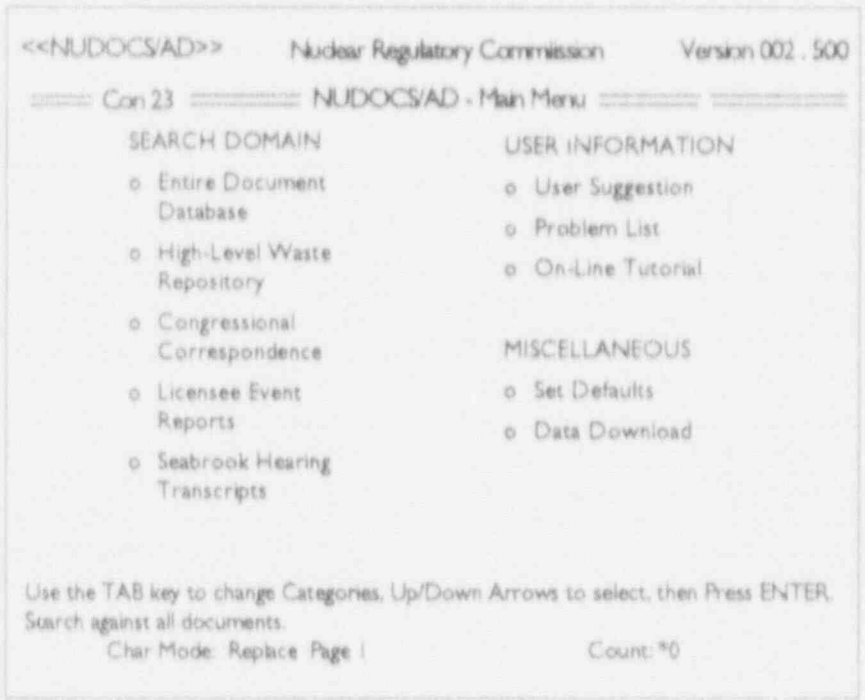


Figure 1

("NUDOCS" from page 10)

by the NUDOCS/AD User Support Services Group. This code indicates the current status of the suggestion and can only be changed by NUDOCS/AD User Support Services. The following status codes are currently in use:

N - New entry
R - Under review
P - In process of implementation or resolution
C - Completed or resolved

Press ENTER To Update( ): Used for submitting a suggestion.

The Suggestion Area

The suggestion area is used for entering details of the suggestion. This field may be scrolled to allow enough space for complete descriptions.

Type the first line of the suggestion, press the **ENTER** key to move to the second line in the suggestion area. At the end of each line continue to press the **ENTER** key until the suggestion is complete. Then press the **TAB** key to move the cursor to the Update field. Press the **ENTER** key to submit the completed suggestion.

Press **ESCAPE** to exit the Suggestion Box after submitting a suggestion.

The Response Area

The response area displays replies to suggestions that have been reviewed by NUDOCS/AD User Support Services and the Document Management Branch, IRM. This area may also be scrolled. User Support Services personnel check the Suggestion Box daily to determine if any new entries have been made.

When a suggestion is entered, NUDOCS personnel change the Status Code to an "R" indicating that the response is under review. An interim response acknowledging the suggestion is entered in the response area. The submitter is called to acknowledge receipt of the suggestion and request additional clarification, if necessary. When a response has been written and approved by the Document Control Branch, the Status Code is changed to a "C" and the final response is entered in the Suggestion Box.

Actions taken in response to suggestions may include the submittal of:

- Problem Reports
- Discrepancy Reports
- Enhancement Requests
- Requests for Additional InformationReferrals to the Appropriate Organization

Most suggestions are either requests for corrections or enhancements to the system. Requests for corrections identify problems with existing data or procedures. These problems are usually solved in a relatively short time. Requests for enhancements are usually software-related. At the direction of the NRC, suggestions of this nature are forwarded to the NUDOCS development staff for analysis.

List of Suggestions

All suggestions are available for review by NUDOCS/AD users. While at the Suggestion Box, press **F2** to display a listing of all current suggestions. To read an entire suggestion and response, position the cursor next to a suggestion by using the **DOWN ARROW** key and press the **ENTER** key. The entire suggestion will be displayed. Press **ESCAPE** to exit the Suggestion Box or **F2** to relist current suggestions.

Suggestions remain on-line for two weeks after a final response is displayed. The User Support Services Group ensures that the author of every suggestion is contacted and informed of the resolution to his/her suggestion. If you have any questions about the Suggestion Box or any other feature of NUDOCS/AD, contact the NUDOCS Hotline, 492-8603 or FTS 492-8603. ■

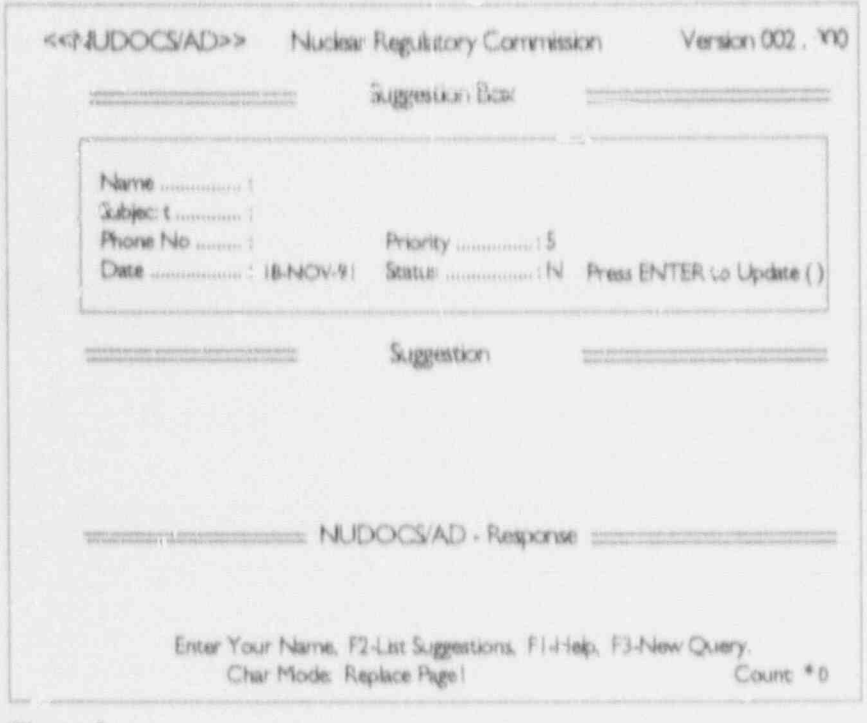


Figure 2

SIGN ON WITH SINET

Two New SINET Systems Coming On-Line in Early 1992

Integrated Events System (IEVENTS)

The Integrated Events System (IEVENTS), scheduled for implementation into SINET in February 1992, represents a cooperative effort between AEOD, NRR's Events Analysis Branch (EAB), and IRM. The major goal of IEVENTS is to tie together all the information about each event, so that a broad, inclusive profile exists detailing the technical and administrative history of the event.

AEOD (using its Operations Center local area network (LAN)) has developed a data collection mechanism for gathering event notifications (ENs), preliminary notifications (PNs), and daily reports (sometimes referred to as morning reports). These data will be made available to SINET. Other data in addition to these textual descriptions are also collected at this time. Licensee Event Reports (LERs), the final reporting stage, are already collected and passed to SINET (Figure 1).

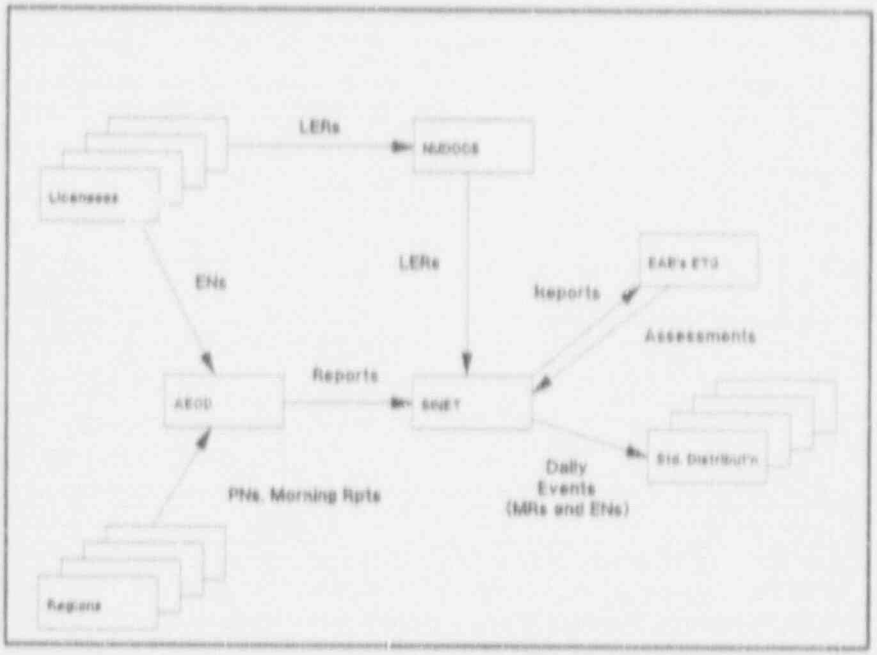


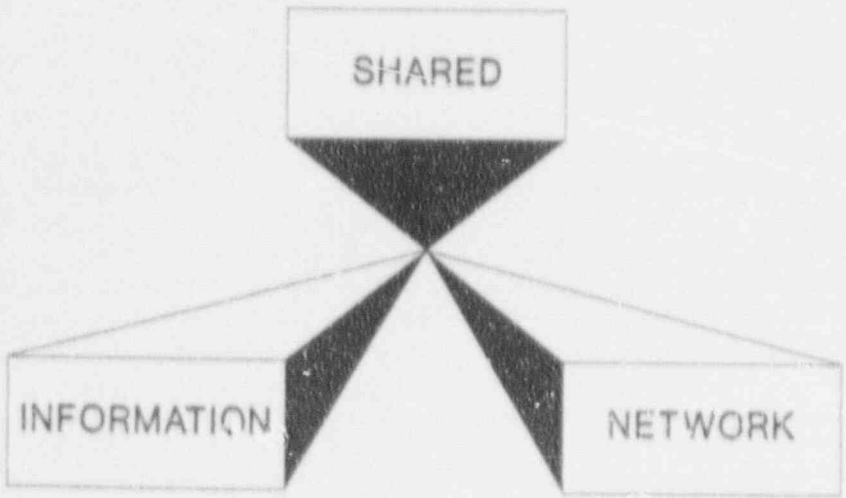
Figure 1: Integrated Events--Process Model (Conceptual Level)

EAB has developed a PC-based events assessment system (to help the branch prepare its evaluations) that captures some of the data gathered by AEOD, as well as much data currently collected in SINET. EAB generates characterizations of each event and releases these to other NRC offices. Much of the data currently collected by SINET is passed to the events assessment system via a download procedure performed on demand by EAB.

The SINET events database serves as a medium of exchange between these systems, providing the agency with a centralized, organizing repository where data are placed for all offices to use.

The major features of IEVENTS are: (1) collecting and distributing as many types of event reports as possible, (2) linking (wherever practical) different reports describing the same event, and (3) an easy means of performing on-

(Continued on page 13, "SINET")



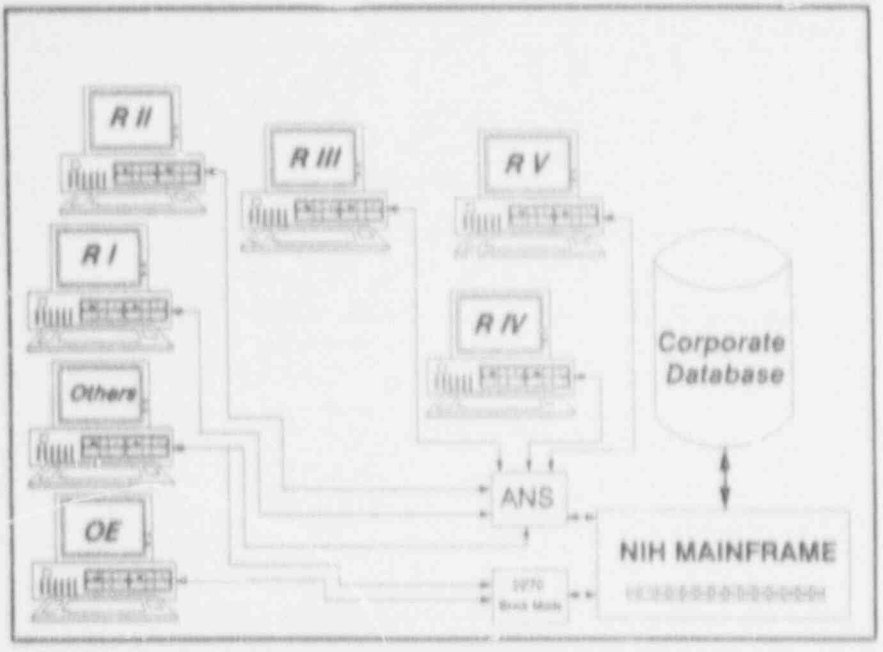


Figure 2: Enforcement Action Tracking System Conceptual System Model

("SINET" from page 12)

line searches and retrievals, and of generating hardcopy reports.

If you have questions concerning the Integrated Events System, please call Garrie Williams on 492-5029 or FTS 492-5029, or Wil Madison on 492-7781 or FTS 492-7781.

Enforcement Action Tracking System

The Office of Enforcement (OE) requested that IRM convert the existing Enforcement Action Tracking System (EATS) from a PC-based environment to the corporate environment (SINET). This request is based on the need for regional access to enforcement actions in order to more uniformly determine violations and severity levels. Additionally, an interface with the SINET Inspection Follow-up System (IFS) allows inspectors and other regional IFS users to track escalated enforcement items. EATS is scheduled for implementation into SINET in January 1992 (Figure 2).

EATS enables management to (1) schedule work within the office, (2) derive statistical information important to the enforcement process, (3) generate reports that allow enforcement specialists to monitor the progress of enforcement action cases, and (4) use reports from the system for summary information, some of which get reported at the Commission level.

Initially, approximately 12 people in the headquarters Office of Enforcement and 8 regional enforcement coordinators will have access to the corporate EATS. Access to the system is subject to restrictions placed upon data access by the Office of Enforcement. If you have questions concerning EATS, please call Margie Dimig on 492-7047 or FTS 492-7047, or Wil Madison on 492-7781 or FTS 492-7781. ■

Do you have an idea for an article?

Call and let us know -- 492-8309

Floppies Safe

December 16, 1991, Vol. 4, No. 5, p. 5, RT IMAGE

The effects of low-level ionizing radiation and magnetic fields such as those found in airport x-ray machines and metal detectors have been proven not to affect floppy computer disks, according to a presentation at [Radiological Society of North America] RSNA.

"We found no changes whatsoever from the exposure to the x-rays or changes to the magnetic fields until we got up to 1,000 gauss," said co-author Joel E. Gray, PhD, Professor of Radiological Physics, Mayo Clinic, Rochester, MN, at the presentation.

In the study, researchers exposed normal 3.5 inch floppy disks to varying levels of both x-rays and magnetic scanners. The x-rays ranged from 100 to 1000 rad, one million times the strength of a normal one-millirad airport x-ray machine. Normal exposure to humans throughout 1 year is 120 rad. No change was found in the disks.

The magnetic test field was from 10 to 1,000 gauss, and there was no effect until higher dosage was applied, and as expected, the contents of the disks were erased. Airport metal detectors range from 1 to 3 gauss. ■

Co-authors of a scientific exhibit on the topic presented by Dr. Gray during the RSNA meeting are J. Tabel, RT, and L. Cesar, RT.

ITS TRAINING LAB NEWS

Exploring the ITS Training Laboratory

Consider some of the reasons for coming to training at the ITS Training Laboratory. (Check as many as apply.)

- ☐ The course is related to my job requirements.
- ☐ The course is designed to meet my objectives while keeping me away from my job the minimum amount of time.
- ☐ The classes are small and it is easy to learn; there's time for individual assistance.
- ☐ Training offers an opportunity to add to my professional development.
- ☐ The courses are interesting and the instructors are well versed in the materials.
- ☐ I heard the classes were really filled up and it was sometimes hard to get in, so I decided there must be some good things happening there.
- ☐ I like the reference materials in the manuals that are provided when taking courses at the ITS Lab.
- ☐ Everyone gets their own PC to work with so we can try out all the features.
- ☐ I am motivated to learn as much as possible; the ITS Lab makes it easy to gain that knowledge.

If you checked fewer than four of the above, you must visit the ITS Lab soon!

Designing The Training Experience

Adult education is an area that is rapidly gaining prominence and stature. Experience has shown that actively promoting training in motivational and production-based subjects results in better job performance and improved morale.

Central to the issue is

- Who should be taught?
- What information should be included?
- How should the material be presented?
- Should job aids be included?
- What means are there to measure the effectiveness of the training?

At the ITS Training Laboratory, when a subject has been identified as a possible training target, a systematic approach to instructional development is taken. The goal is always to design courses that will ensure maximum learning, retention, and application to specific NRC needs. First, a needs analysis is performed. Individuals are interviewed to identify what data they have, how they want to use it, and what end-products they are anticipating. A determination of who will be required to know and use the software is made.

Second, a course blueprint is developed to include the features that will meet the NRC's specific objectives identified in the needs analysis. Hands-on exercises are developed to provide experiential learning. Course content is written to support the exercises and provide after-class reaffirmation of the procedures.

Third, the course materials are read by individuals thoroughly familiar with the software package to check for inaccuracies and misleading statements. The exercises are keystroked to make sure that every step is called out and precise directions given.

Finally, a pilot of the course is presented. The audience for a pilot includes those individuals who know the objectives and are acquainted with the software, as well as "real student testers." This group evaluates the course from the user's standpoint, offering a different and important perspective in this instructional design process.

After final revisions, the course is scheduled for open registration. Should the materials be specific to a narrower audience, the course is scheduled for the specific group within the Agency that will benefit most.

Throughout the training development and in each of the course presentations, instructors will refer to those attending the class as "participants." There is good cause for that distinction. Adult learners are more than "students." Each individual brings special knowledge and experience to class to enhance and broaden the understanding of all others attending. The interaction in the classroom of shared unique experiences aid in the instructional process. The active interchange of ideas and concepts help other participants learn.

Class (Structured) Education vs. Individualized Learning Experiences.

An alternative to the interactive, structured circumstances of the ITS

(Continued on page 15 "ITS")

("ITS" continued from page 14)

Lab is the computer-based training available at the Individualized Learning Center (ILC). Self-study through the use of interactive courses is the solution for many who are unable or unwilling to give up a day to train at the lab. This new approach offers individuals an opportunity to train at their own pace and in the privacy of their own work area. Skillful, tested training in many packaged software and technical applications is available for those individuals. Call the ILC (492-4514) for a copy of the computer-based training catalog. ■

Revised Method for Importing Data from dBASE to WordPerfect

In the revision of the WordPerfect courses taught at the ITS LAB, new materials and exercises were added. In the "WordPerfect Enhanced Documents" (MD) course, the method for importing data from dBASE to WordPerfect was redefined. If you have taken the "Enhanced Documents" class and are comfortable with the merge feature in WordPerfect, the ITS Training Lab recommends your use the following method to import your sorted and selected information from dBASE into WordPerfect.

For the purposes of this article, the following paths are assumed to exist on your computer.

Your database file is assumed to exist on \dBASE.

Your WordPerfect program files are assumed to exist on \WP51

Your WordPerfect documents are assumed to exist on \WP51\WPDOCS

If your dBASE directory and WP directories are different, alter your command lines accordingly.

In dBASE, type the following commands. Items in brackets [ ] are to be supplied by you.

- USE [yourfile.dbf]
- Identify the fields in the database that you want to import into WordPerfect.
- Index your file to sort by the desired fields.
- At the dot prompt, type the following command. ([sp] means leave a space. [filename.sdf] is the temporary file that will contain your data until it is converted into a WordPerfect secondary file).

COPY [sp] TO [sp] \WP51\ [filename.sdf] [sp] FIELDS [sp] [List field names separated by commas] [sp] DELIMITED

As an example:

COPY [sp] TO [sp] \WP51\list.sdf [sp]FIELDS[sp]last, first, mailstop, phone[sp]DELIMITED

The resulting file will have all of the fields surrounded by quotation marks ("") and separated by commas. Each record will end with a hard return and the data in the temporary file will look like this:

"Perez","Maria","1F22","570-1215"
"Peters","Sam","W306","492-4920"

You have completed all you need to do in dBASE.

- QUIT

At the DOS prompt, type:

CD [sp] \WP51 (to change to your WordPerfect program directory where the CONVERT.EXE file resides)

Type: CONVERT [sp] \WP51\[filename.sdf] [sp] \WP51\WPDOCS\[newfile]

"\WP51\filename.sdf" is your input file created in dBASE.

"\WP51\WPDOCS\newfile" is the new secondary file that will be written to the WordPerfect documents subdirectory.

The Convert Menu will display.

- type 9 to select Mail Merge

  At the field separator prompt, type a comma [,]

- At the record separator prompt, type 13 and 10 surrounded with braces [{13}{10}]. This represents the ASCII characters for a carrier return and a line feed.
- At the characters to be deleted prompt, type a quotation mark ["]

The convert program will create a secondary merge file that can be used with MERGE to create personalized letters, lists, labels, and other documents. The final form the data would take would depend on the primary file designed for the merge.

If we were to convert the sample delimited file used as an example above, the finished converted document would appear in WordPerfect 5.1 as expressed below:

Perez {End Field}
Maria{End Field}
1F22 {End Field}
570-1215 {End Record}
Peters {End Field}
Sam {End Field}
W306 {End Field}
492-4920 {End Record}

(In 5.0, the fields would end with the ^R code and the record with ^E.)

Please note: The order that the fields were copied from your dBASE file is the same order they will be numbered in the secondary file.

As in the example above, the order of the field names in dBASE will be the order of their use in WordPerfect:

Last	Field 1
First	Field 2
Mailstop	Field 3
Phone	Field 4

See your WordPerfect Reference for ways to name fields rather than use numbers in WordPerfect. ■

ITS TECH NOTES

This section of the newsletter provides tips and technical information of interest to NRC computer users. If you have any questions regarding "Technotes" or if you wish to contribute an item, contact the ITS Support Centers: for PC and NIH items, call 504-3490 and for DG items, call 492-3491. You may also drop by and visit in OWFN 3-C12.

Personal Computers

Wanted: More Memory

How memory is used in your system depends on the interaction of three factors:

- type of memory
- application program requirements
- hardware or software required to provide needed memory

The three types of memory obtainable on all PC-based systems are:

- base memory (also called conventional)
- extended memory
- expanded memory

The diagram below illustrates these types of memory. The diagram includes examples of software that are used within each type of memory.

Base Memory

Most personal computers today use a base memory of up to 1 megabyte (Mb), which is the maximum amount of base memory possible. Of this 1 Mb, 640 kilobytes (Kb) are reserved for the disk operating system (DOS), application programs, and device drivers. The remaining 384 Kb are referred to as high or reserved memory. The reserved memory is used by the hardware installed in the system.

All IBM PC and compatible systems can generate 1 Mb of base memory. To obtain the amount of base memory required by an application, Memory Management Software can be installed. This software temporarily moves resident programs out of the 640 Kb base memory to an area above it (reserved, extended, or expanded) so that more of the 640 Kb base memory is available for processing.

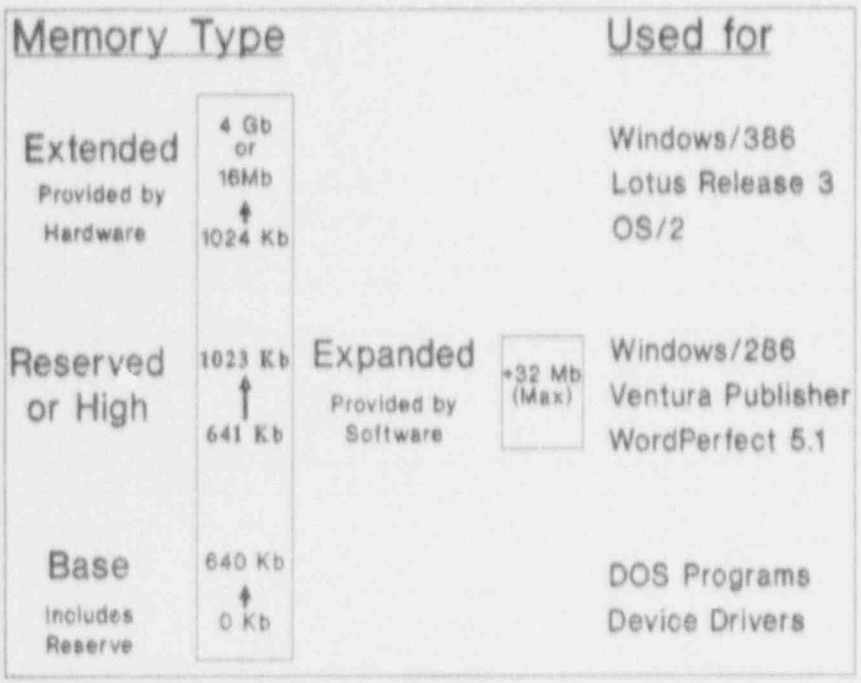
Extended Memory (provided by hardware):

Extended memory, the level above the base 1 Mb, is an additional 15 Mb to 4 gigabytes (Gb) of memory that is **directly accessible** by a computer's microprocessor (depending on the processor). Directly accessible means the computer can generate the address (location) of needed data and files in memory.

Extended memory is provided by hardware. For PCs with less than 1 Mb of memory, a memory board with extended memory capability is required. Extended memory is not available on IBM and compatible PCs or XTs, which use an 8088 or 8086 microprocessor. The IBM XT/286, AT, and PS/2 Model 50, which use an 80286 processor, can address 16 Mb of memory. The PS/2 Models 70 and 80, which use an 80386 processor, can access 4 Gb of memory.

The increase in addressable memory is due to the increased instruction set made available by the newer processors; e.g., 8088/8086 family processors have an 8 bit instruction set/ 8 bit data path (8 bit processor); an 80286 processor has a 16 bit instruction set/16 bit data path (16 bit

(Continued on page 17, "Tech")



("Tech" from page 16)

processor); and 80386/80486 family processors have a 32 bit instruction set (32 bit processor). The 80386DX/80486 processors utilize a 32 bit data path. The 80386SX processor uses the 80286 16 bit data path, but is a true 32 bit processor.

Expanded Memory (provided by software):

Expanded memory provides 32 Mb of memory and works in high memory. The microprocessor **cannot** generate an address for software requiring expanded memory without an Expanded Memory Manager (EMM). EMM is a software component that is activated when the computer is turned on. EMM maps small pieces of the available memory (16K at a time) into the address space of the system. Each 16K piece of memory is called a page, and the area of the system that receives the page is called a page frame.

EMM acts as a traffic director between DOS and expanded memory, reserving a page frame in high memory for access by the processor. EMM tricks DOS into thinking that the portions of expanded memory are part of the available addressable memory. Unfortunately, EMM requires time to move expanded memory requests in and out of the page frame.

Expanded memory can be made available on all PCs if there is at least 1 Mb of base memory. In addition, extended memory can be used as expanded memory on the IBM XT/286, AT, and PS/2 Model 50, but an expanded memory board must be installed. The 80386 systems (IBM PS/2 Models 70 and 80) are also capable of using extended memory as expanded memory.

This month's ITS Tech Notes are extracts from recent issues of DOE's AOSS Communique. They are published with the permission of Brenda Cablentz, Editor.

Two other software solutions are available for providing expanded memory:

- LIM emulator for 80386 systems, which allows extended memory to be simulated as expanded memory
- LIMulator for 8088, 8086, 80286, and 80386 microprocessors, which allows hard disk space to be used as expanded memory.

Extended Versus Expanded

While this discussion may make it seem like expanded memory is simply an extension of extended memory, it is not. It is not necessary to fill all of your system's available extended memory capacity before expanded memory can be added. Expanded memory is an entirely different and independent entity; its installation and use do not rely on exceeding the capacity of extended memory.

In addition, although extended or expanded memory increases the system's memory capacity above the base 1 Mb, they are both hardware-dependent (as explained) and software-dependent. The type of memory used is also determined by the software specifications. For example, Windows/386, Lotus 1-2-3 Release 3, and OS/2 use extended memory; and Ventura Publisher, Windows/286, and WordPerfect 5.1 use expanded memory. Also, some applications cannot use either extended or expanded memory.

In Summary

Confused? Normally, it is unimportant for you or the system to know the difference between base, extended, or expanded memory. Your system will access the appropriate type of memory required by your applications; however, the type of memory available, your program needs, and the hardware and software (such as EMM) installed, all interact to assist in processing.

All of the above-mentioned factors must be taken into consideration before adding memory to your system. Matching a type of memory to your requirements provides the best return on the time and money invested in your hardware and software.

Shortcomings of a Recovery

At some point in time, just about every user will have that sinking feeling when a file that was desperately needed has been accidentally deleted; a "DEL *.*" command was issued in the wrong directory; or some disaster occurred causing a file to disappear. In many cases, there is hope. Because of the way DOS stores files, the data is usually retrievable. Recovery can require very specialized tools and training, but there are utility packages, such as Norton Utilities, PC Tools, and Mace Utilities, that simplify the procedure. The problem is that, while these programs may make data recovery easier, they do not always recover the complete document.

To understand why complete recovery is not always possible, it is necessary to know how DOS maintains data on a disk. Three main areas are used to store information about a file: the directory that contains the file name; the File Allocation Table (FAT) that tracks the disk space location and size used by a file; and the data area that stores the file's contents. When you save a file, its name and other important information is added to the directory. The system searches the FAT for space to store the file and records the location and other information in the FAT, and then the file is placed in the designated area(s). A file may be split into several segments and placed wherever space is available. DOS stores a file in the first available space, regardless of size. If more

(Continued on page 18, "Memory")

("Memory" from Pg. 17)

space is needed, it looks for the next free space, and so on, until the complete file is stored. Over time, as you save, delete, and copy files, the available areas become scattered, and a file's storage areas are much less likely to be contiguous.

When a file is deleted, the file name is deleted from the directory, but important specifications are kept. The entries in the FAT are cleared and the area used by the file is freed; however, the data remains in the area it was stored. If you realize **immediately** that you accidentally deleted a file, it is almost surely retrievable. However, if you continue to use your system, subsequent saves may overwrite the data (remember, the system reuses freed space) or reuse the directory entry where the filename was kept. This will complicate recovery.

When you attempt to recover a file, even if you immediately discover your error, it may not be successfully restored. For example, Norton uses an algorithm to make the best estimate of the space where your file was stored and then puts those areas together as the file. That estimate is based on the condition of the system at the time you run Norton, not at the time you originally saved your file. These may be compromised of unequal elements, and the resulting recovery may link the segments of your file together differently than originally stored. Consequently, the larger the deleted file, the more likely the recovery will be unsuccessful. Similarly, the more files you recover, the more likely that a single error in an early file recovery will propagate into more errors in later recoveries (for instance, if the first recovery accidentally uses an area really belonging to another file, which then uses an area belonging to yet another file, and so on).

Another, more difficult problem in recovering a file occurs when a utility program is used unsuccessfully (or improperly) to restore files. Consequently, much of the information that would have made recovery easier can be altered, and subsequent recovery efforts are greatly hampered. In some cases, data is irrevocably lost. If your software package automatically makes a backup copy you can retrieve that copy. Also, if you backup regularly, you may restore the file from a backup diskette. However, neither may contain your latest changes.

If you should ever realize that you've lost a file you need to stop work **immediately**. (Unfortunately, some application packages do not stop immediately but continue to do some file operations.) If you use a utility program, attempt recovery only if you **really** know what you are doing. Otherwise, contact the **[IRM Hotline]**, which staffs personnel who are experienced in file recovery. However, you must be patient. Recovery is often a time-consuming effort, and you may have to wait several days before your data is restored. If the data is important or the time to reenter it is long, it will be worth the wait. ■

Tracking Down Troubles with "SneakerNet"

Information transfer is an essential part of today's computing environment. It always involves potential risks of system contamination from viral infection, data loss from media mishandling, or disclosure of sensitive information. Security countermeasures--from stringent protection policies and guidelines to special software application--have been developed to make a PC less vulnerable. Unfortunately, none of these high-tech solutions protect against the most significant low-tech security problem: physical transfer of media by human beings, known as "SneakerNet."

SneakerNet exists everywhere removable storage media (e.g., floppy diskettes, tapes, removable disk packs, and cartridges) are used. Each time you take a floppy diskette to another PC to use a better printer or a different software, you create a SneakerNet link between those two PC systems. Although SneakerNet is often the most convenient, inexpensive, and flexible form of data transfer, it creates computer and physical security management concerns. Even simple SneakerNet links between systems in the same office can create security and data integrity problems because these links are particularly prone to user error. Introduction of the human factor presents numerous hazards and substantial security risks.

Think about how often you move a high-density 3.5" diskette. When full, each diskette can hold 300 single-space pages of word processing text. This high-storage capacity generates a great deal of potential loss if your SneakerNet procedures are not up to par.

SneakerNet problems include:

- A diskette carelessly left on a table is subject to environmental hazards, such as spilled coffee, heat, and other physical damage. Have you ever set a diskette down near an open can of soda or a full coffee mug?

- Workstations on either end of the network may be incompatible. Not only does this lead to the inability to access data from the transfer media, but it introduces the additional risk of damage to the media, data, hardware, or software as you attempt to communicate.

(Continued on page 19 "Memory")

("Memory" from page 18)

- Media transfer might introduce viruses into either or both systems in the SneakerNet. If either Personal Computer (PC) is infected, you may transfer the virus to a diskette, and then to any system with which the diskette comes in contact. Possible data loss or damage will spread with every location involved in the SneakerNet.

- Removing data/media from the office area exposes it to compromise and loss. Media, especially small diskettes, can be easily lost, stolen, or quickly copied. Leaving the office environment also puts that media in potentially damaging situations, such as exposure to heat, light, magnetic fields, mishaps, and/or careless handling. If you ever misplace a diskette, even for a few minutes, the data could be compromised without your knowledge.

- Lack of attention to appropriate security measures during media relocations, combined with the high volume of SneakerNet transfers, increases the likelihood that information could be damaged, lost or compromised unintentionally. The key to maintaining data security is to be aware of the risks and guard against incidents.

SneakerNet is subject to the same management rules as paper. The most effective security solution for SneakerNet file transfer is the least expensive to implement. This solution centers on identification and analysis of potential problems and common sense.

When contemplating a SneakerNet transfer, know security requirements and system configurations at both ends of the network; practice standard workstation protection procedures; back up data before a transfer; and practice care in relocating media. Your SneakerNet procedures should include the following precautions.

- Keep diskettes in appropriate containers (e.g., dust jackets, diskette containers, or cardboard shipping folders) at the desk and during transport.
- Maintain common diskette maintenance procedures during transfer. For example, do not leave diskettes in a hot automobile or expose them to magnetic fields.
- Protect media at the highest classification level of data stored on them. Contact your Organization's security officer for more information on security measures for classified materials.
- As soon as possible after work is completed return media to its storage location. ■

INEL

New User IDs

The INEL Supercomputing Center is beginning to assign IDs that include digits, because they have more than 9,000 users. Current IDs will not be changed, so those of you who have been INEL users for a long time will retain your personal initials.

Manuals Available

Although the CRAY commands reside on-line in MAN pages, hardcopies of the CRAY User Guide and TRS (Tape Reservation System) User Guide may be obtained by calling INEL Scientific User Services, FTS 583-9440.

CRAY Zoo/Fiz

The CRAY utility zoo/fiz is close to performing the same function as the Cyber FILESET. If you liked that method of file management to save storage space, try this. MAN pages will give you the syntax and particulars.

Videos of INEL Symposium

The September 1991 symposium was videotaped and the NRC has video copies of the nine key speakers. Call 504-3490 or FTS 964-3490 to request a video on loan.

Topics and Speakers:

"Turning Visions Into Reality," Alan Kay, Apple Computer Inc.

"Trends in High Performance Computing," Dr. Sidney Karin, Director, San Diego Supercomputing Center

"Computational Requirements for the Human Genome Project," Dr. Charles Cantor, DOE Human Genome Project

"Managing Change in the Technical Environment," Dick Sellers, Digital Equipment Corp.

"Visualization in the 90's," James Warner, Precision Visuals Inc.

"Managing Information in the 1990's," Tom Woods, Liveware Solutions International

"North to the Pole," Paul Shurke, Co-leader of the 1986 expedition to the North Pole

"Geosberv Project," Tom VanSant, Eyes on Earth

"Virtual Realities: From the Concrete to the Barely Imaginable," Dr. Stephen Marcus, University of California

Computer Wizards

John Atanasoff is considered by many to be the founder of the computer industry. He thought and dreamed of a device based on Babbage's theories, using a digital approach, when such machines didn't even exist. One night, while driving fast across Iowa, he formulated a new idea and was able to conceptualize an electronic digital computer. He built a prototype in 1939, called the ABC computer, which used (1) electrons as the communications medium, (2) binary numbers in memory, (3) serial calculations, and (4) a memory device implemented by condensors to hold the plus or minus state. This prototype was the basis for the ENIAC computer. In 1990, Atanasoff was honored by the U.S. Commerce Department with the Medal of Technology, the nation's highest award bestowed by the President for technological achievements. ■

* U.S. Government Printing Office : 1992 - 312-471/60013

NUCLEAR REGULATORY COMMISSION
Computer Services Directory

ITS SUPPORT CENTER FACILITIES

Locations:

Philips Building, Rm P-358
7920 Norfolk Avenue
Bethesda, MD 20814

One White Flint North, 3C-12
11555 Rockville Pike
Rockville, MD 20852

Phone:
(FTS) or (301) 492-4160
(FTS) or (301) 492-4357

(301) 504-2353
(FTS) 964-2353

Center Hours:

7:30 a.m. - 4:15 p.m. M-F

Services:

Microcomputer assistance (Telephone & Walk-in), Demonstrations, ADP Technical Library, and Computer/Video-based Tutorials. NRC Project Officer, Ms. Phyllis Smith(492-4098); managed under contract by Mr. Lee Taylor, Operations Manager, Analytical & Research Technology, Inc.

TRAINING LABORATORY FACILITY

Location: 3rd Floor, Woodmont Building
8120 Woodmont Avenue
Bethesda, MD 20814

Phone: (FTS) or (301)492-4744 **Mailstop:** W-306

Laboratory Hours: 7:30 a.m. - 4:30 p.m. M-F

Class Hours: 8:30 a.m. - 3:30 p.m.

Services:

Three classrooms for formal ADP training providing "hands-on" instruction in the use of microcomputers and timesharing systems.

Note: The Training Laboratory is operated by the Graduate School, USDA under contract, and managed by the Office of Personnel, to provide training in end-user computing for the NRC staff. Technical guidance is provided by IRM. NRC Project Manager, Carolyn Bassin; GS/USDA Training Manager, Mary Holmes.

NRC END-USER COMPUTING SERVICES

Microcomputer Hardware/Software Acquisition, Upgrades:
Please contact your local ADP Coordinator to initiate this action.
John Burton, P-530, 492-4836

Microcomputer, Word Processor, other ADP Relocation:
Please contact your local ADP Coordinator to initiate this action.
Beth DeWoody, P-508, 492-4832

Microcomputer Hardware Installation and Maintainence:
Karen McElyea, P-500, 492-8906

Microcomputer Software Installation:
Software Support Desk, P-550, 492-8317

Word Processor, Other ADP Maintainence:
Please contact your local ADP Coordinator to initiate this action.
Beth DeWoody, P-508, 492-4832

Modem and Data Line Problems: P-810, 492-4666

Modem and Data Line Acquisition:
Stan Wood, P-626, 492-7723

Computer Room: Phillips 492-7713
White Flint 504-2885

Computer Security:
Louis Grosman, MNBB-7602, 492-5019

Timesharing Access/IDs:
Herb Parcover, MNBB-7602, 492-8699

AUTOS Program: James Schaeffer, P-532, 492-9832

Data General and INEL User Support:
Emily Robinson, 3C-14, 504-3490

AUTOS Helpline: 504-1517
IRM Hotline: 492-4160
LAN Hotline: 492-4243
NUDOCS Hotline: 492-8603
SINET Hotline: 492-4222
Telecomm Help Desk: 492-4666

Data General Systems Problems:
Judy Seeherman, P-600, 492-9687

IBM 9370: Kay Moses, 492-4167, Dave Barrow, P-600, 492-8308

IBM PROFS/E-Mail Support: Sharon Root, 3C-12, 504-2256

Electronics Records Support:
Brenda Shelton, MNBB-7714, 492-8132

Automated Graphics Support: Al Blunt, 2G-40, 504-2216

Commercial Database Support: Eileen Chen, P-160, 492-8501

Scientific Code Distribution: Sharon Root, 3C-12, 504-2256

Shared Information Network (SINET) Development:
Wil Madison, P-810B, 492-7781
EXSIS: John Beatty, P-712, 492-4164

Systems Development and Modification:
Bill Usilton, P-712, 492-8322
Dick Hartfield, P-712, 492-4328

Scheduling for ITS Training Laboratory
Eduardo Cunningham, W-306, 492-4744

Post this ice.