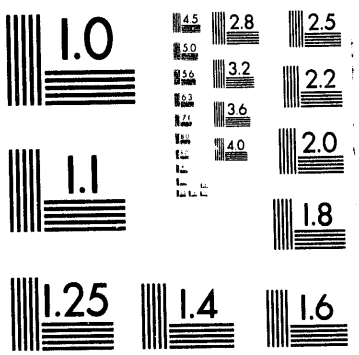
1.0
1.1
1.25
1.4
1.6
1.8
2.0
2.2
2.5
2.8
3.2
3.6
4.0
4.5
5.0

1 of 1

2

UCRL-ID-106454-94-1

Lawrence Livermore National Laboratory Safeguards and Security Quarterly Progress Report to the U.S. Department of Energy

Quarter Ending December 31, 1993

Greg Davis
Doug L. Mansur
Wayne D. Ruhter
Eric Steele
R. Scott Strait

January 1994

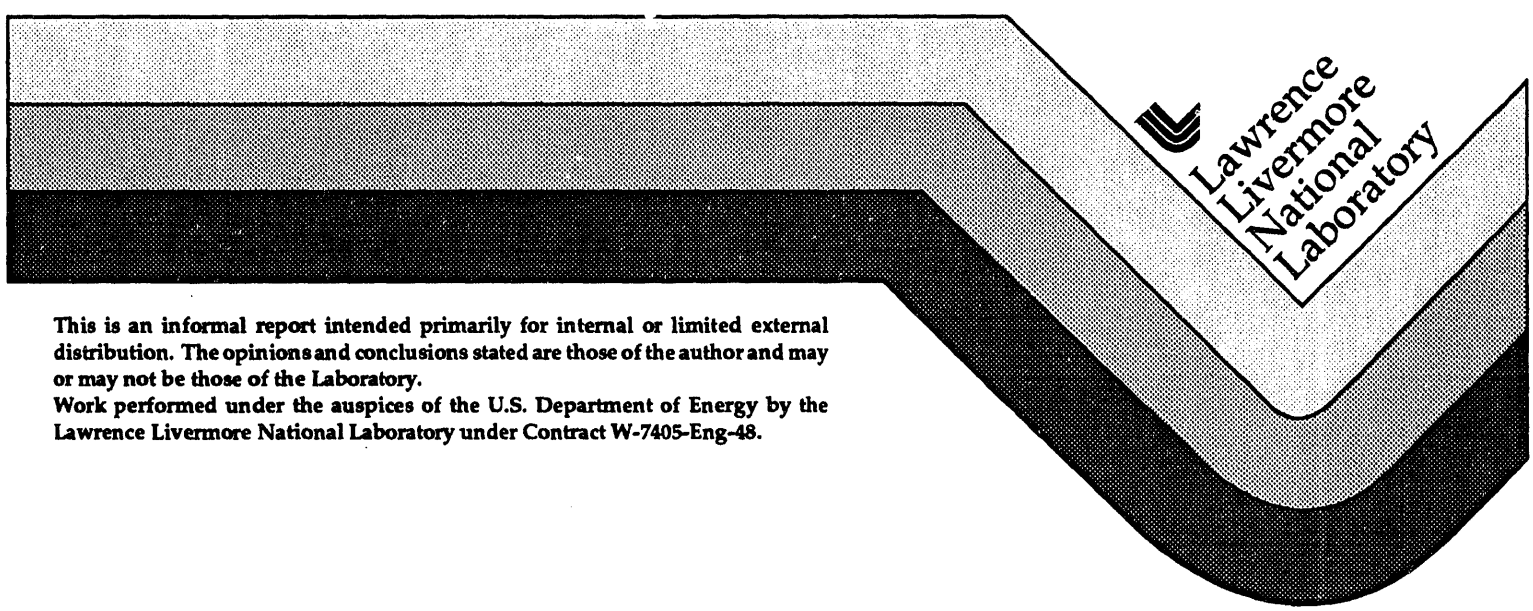

Table of Contents

Preface

The Lawrence Livermore National Laboratory (LLNL) carries out safeguards and security activities for the Department of Energy (DOE), Office of Safeguards and Security (OSS), as well as other organizations, both within and outside the DOE. This document summarizes the activities conducted for the OSS during the First quarter of Fiscal Year 1994 (October through December, 1993).

The nature and scope of the activities carried out for OSS at LLNL require a broad base of technical expertise. To assure projects are staffed and executed effectively, projects are conducted by the organization at LLNL best able to supply the needed technical expertise. These projects are developed and managed by senior program managers. Institutional oversight and coordination is provided through the LLNL Deputy Director's office.

At present, the Laboratory is supporting OSS in five areas:

- Safeguards Technology
- Safeguards and Decision Support
- Computer Security
- DOE Automated Physical Security
- DOE Automated Visitor Access Control System

The remainder of this report describes the activities in each of these five areas. The information provided includes an introduction which briefly describes the activity, summary of major accomplishments, task descriptions with quarterly progress, summaries of milestones and deliverables and publications published this quarter.

The LLNL welcomes the opportunity to apply its expertise in these technical areas. Although the aggregate of activities for OSS is modest, LLNL strives to provide quality responses to OSS needs and stands ready to assist OSS on these and other technical areas.

If OSS management or staff have questions about this report or LLNL's capability to assist in satisfying an OSS need, contact L. Lynn Cleland, 510/422-4951, or one of the program managers for the five technical areas.

Safeguards Technology Program

Wayne D. Ruhter, Program Manager
Nuclear Chemistry Division

INTRODUCTION

The Safeguards Technology Program (STP) is a program in LLNL's Nuclear Chemistry Division that develops advanced, nondestructive-analysis (NDA) technology for measurement of special nuclear materials. Our work focuses on R&D relating to x- and gamma-ray spectrometry techniques and to the development of computer codes for interpreting the spectral data obtained by these techniques.

Representatives of the Department of Energy Office of Safeguards and Security and Office of Research and Development visited LLNL for a program review on October 13-14, 1993. The Safeguards Technology program made a one-half day presentation on FY93 accomplishments and FY94 program plans as part of that review.

SUMMARY OF MAJOR ACCOMPLISHMENTS

I. NDA MC&A Measurement Technology R&D

- The Intelligent Actinide Analysis System (IAAS) is in routine operation for actinide isotopic analysis; upgrades and improvements continue.
- Progress is continuing on the Unix/Motif version of SpecView for use in conjunction with MGA.

II. Emission/Transmission Computed Tomography

- Preparations are being made for further studies of plutonium MSE buttons by transmission and emission tomography.
- Monte Carlo simulation of voids in plutonium buttons has begun.

III. Support to DOE Facilities in Implementation, Testing and Evaluation of LLNL Developed NDA Techniques

- The Plutonium Solution Assay Instrument is undergoing calibration and testing in preparation for delivery next quarter.

IV. Monte Carlo Simulation of Gamma-Ray Spectra

- Some simulations of planar CdZnTe crystals have been undertaken to determine by calculation the absolute and relative efficiency of this potential room-temperature gamma-ray detector material.

- A simulation of PIDIE #1 with a factor of forty increase in the number of particle tracks has been performed to further study the effects of statistics on MGA fits of simulated spectra.

TASK DESCRIPTIONS AND QUARTERLY PROGRESS

Accomplishments achieved during the fourth quarter of FY93 by STP are described below:

I. NDA MC&A Measurement Technology R&D

B&R No.	Funding	Obligated
GD060102	$300K	$64.2K

The overall objective for this task is to research and develop state-of-the-art nondestructive analysis (NDA) instruments, methods, and techniques that address top priority material control and accountability (MC&A) problems and will result in improved MC&A of SNM at DOE facilities. Activities include assistance to the field in resolving major and significant problems associated with holdup, heterogeneous materials, lump corrections, waste measurements, and shipper-receiver measurements.

Intelligent Actinide Analysis System

William M. Buckley, Wayne D. Ruhter, Kenneth E. Raschke, and Austin L. Prindle

The intelligent actinide analysis system (IAAS) is a gamma-ray spectrometry system utilizing a distributed computer network that is intended to advance nondestructive actinide analysis systems for nuclear safeguards in performance, automation, ease of use, adaptability, systems integration, and extensibility to robotics. A major goal for these systems is a modular hardware and software design that will use commercially available components whenever practical to reduce development and maintenance costs. This will also allow easy modification for specific user requirements or technological extensions to the base instrument design. Another goal is to improve performance by assisting measurement technicians in setup and operation of the system for assurance of spectral data quality and results. The first system will be delivered to Materials Management at LLNL. Materials Management is supporting the hardware, documentation, and training costs.

The IAAS instrument was in operational use most of this quarter. The electronic noise problems that occur at high count rates have not been solved, but their effects have been moderated sufficiently to allow operation of the instrument. The IAAS has been sued to measure a variety of samples, including those in 18-inch calorimetry containers. The fixed position scan mode has been installed and tested. When operational needs permit during the next quarter, we will actively pursue solution to the noise problems, and install and test the remaining software upgrades.

MGA Development
Kenneth E. Raschke, Austin L. Prindle, Joseph B. Carlson, and Eugene A. Henry

Domestic safeguards R&D work related to MGA has concentrated on the measuring op plutonium isotopics of samples for Materials Management at LLNL. Because many of these samples now being measured are low in plutonium relative to other nuclides (uranium, ^{241}Am, for example), the analysis is not straight forward. Thus far successful analysis of some samples has only been accomplished with a combination of analysis with the MGA and GRPANL programs. We will be working to identify the problems associated with analysis of these samples with low plutonium content in order to enhance MGA performance for these samples.

Second Generation Software
William M. Buckley

The SpecView application is a viewing "engine" which will form the basis of new data acquisition, manipulation, analysis, and management applications under Microsoft Windows and Unix Motif environments. This will provide a common, vendor-independent graphical user interface that should simplify operations of systems and software, and reduce training requirements.

Work is continuing on a Unix Motif version of SpecView. The Motif version has some new capabilities which we will implement for the Windows version. The Unix Motif version of MGA will be the first application that uses SpecView in the Unix environment.

II. Emission/Transmission Computed Tomography

B&R No.	Funding	Obligated
GD060202	$150K	$36.0K

This technology combines the advantages offered by two well-developed, nondestructive assay techniques: gamma-ray spectrometry and computed tomography (CT). Coupled together these two techniques may be used to nondestructively and quantitatively measure uranium and plutonium in samples

where the U and/or Pu are heterogeneously distributed, distributed in lumps of varying size, or the sample matrix varies in density and composition. This technology potentially offers significant improvements over current segmented gamma-scanning (SGS) techniques.

Gamma-ray spectrometry passively and nondestructively measures the gamma-ray emissions from a sample. From the measured gamma-ray spectrum one can identify the radioactivities detected and determine their abundances, if appropriate corrections for sample self-attenuation are made. Transmission or active CT is a nondestructive technique, already widely used in medical and industrial applications, that uses an external-radiation beam to map photon attenuation within a sample. This attenuation data can be used to correct the emission data for sample self absorption. The result is an accurate, quantitative assay of all detectable radioactivities within a sample regardless of its form or composition.

Emission and Transmission Computed Tomography Application
Tzu-Fang Wang, and Eugene A. Henry

During FY93 a partial scan of a plutonium MSE button was accomplished using both transmission and emission computed tomography. Analysis of these data indicated that this button had voids, cracks, and isotopic inhomogeneities that could be of concern for the accurate determination of the isotopic content of the button. We have since identified two MSE buttons held by the Materials Management at LLNL that we can use for further extensive studies in a laboratory setting. The experimental apparatus for the first measurement was of a temporary nature. Consequently, we have completed the conceptual design of a tomography scanner suited to the study of MSE buttons in consultation with the Non-Destructive Evaluation group at LLNL. Plans to build the scanner (funded in part by LLNL) are underway. This scanner will be crucial to accomplishing the tomography studies in a timely, reproducible, and quality-controlled manner.

We have also performed a Monte Carlo simulation of a MSE button with and without a void, so we can evaluate the effect of the void in the button. The results from the simulation thus far have poor statistics due to enormous self absorption of the gamma-rays in the button, i.e. a lot of simulation time is spent tracking gamma rays that are eventually absorbed in the button. We are using several methods to improve the statistics in the simulation.

III. Support to DOE Facilities in Implementation, Testing and Evaluation of LLNL Developed NDA Techniques

B&R No.	Funding	Obligated
GD060302	$100K	$7.4K

The primary objective of this task is to assist DOE sites in implementation of LLNL developed NDA technology; in particular, assist Westinghouse Savannah River Company facilities; LLNL's Materials Management; and LANL's TA-55 facility. A brief description of activities under this task are given below.

Analysis of Plutonium Solutions

William M. Buckley and Kenneth E. Raschke

System integration and software development was completed on a Plutonium Solution Assay Instrument for Analytical Chemistry at LLNL. This instrument has been installed in the Plutonium Facility and is undergoing calibration and final testing. It will be delivered during the next quarter. This instrument will provide the first production use of the MGA program for isotopic analysis of plutonium solutions.

IV. Monte Carlo Calculations of Gamma-Ray Spectra

B&R No.	Funding	Obligated
GD060202	$150K	$33.7K

The simulation of gamma-ray spectra for a known radioactive source, sample matrix, and geometry can be an important tool in designing and understanding non-destructive analysis (NDA) instruments such as Pu gamma-ray isotopic analysis systems. There are also a number of significant and major MC&A problems associated with heterogeneous materials, lump corrections, holdup, waste, and shipper-receiver measurements that can be addressed with this calculational tool. The gamma-ray spectra from each of these problems can be simulated with a Monte Carlo method by mocking up various geometries and transporting the gamma-rays of a known source through the material to a detector. Monte Carlo calculations may be used to calculate plutonium "standard" gamma-ray spectra that may be used to determine such characteristics as systematic biases in spectral data-analysis codes. With so many possible variations of the problems described above, the simulation of gamma-ray spectra from them is more efficient and cost effective than the development and measurement of various reference materials.

Monte Carlo Simulation of Plutonium Gamma-Ray Spectra
Tzu-Fang Wang, and Joseph B. Carlson

During the previous quarter we have made Monte Carlo simulations of the HPGe gamma-ray spectra of standard Plutonium Isotopic Determination Intercomparison Exercise (PIDIE) sources #1 through #7. These simulated spectra are in good agreement with those measured experimentally. However, the residuals after the MGA fit to the Monte Carlo simulated spectra showed a characteristic pattern. Increasing the statistics of the simulated spectrum of PIDIE #1 by a factor of ten resulted in a significant improvement in the goodness-of-fit indicators from a fit of the spectrum with MGA. We have just completed another simulation of PIDIE source #1 with a further increase by a factor of four in particle tracks (and increase of about forty over the first simulation). These data will be analyzed to verify our hypothesis that statistical effects are responsible for the pattern of residuals from MGA fits of simulated spectra.

Monte Carlo Simulation of CdZnTe Crystal Efficiency
Tzu-FangWang

We have performed some Monte Carlo simulations of planar crystals made from cadmium-zinc-telluride (CdZnTe) material [Cd(50%)Zn(10%)Te(40%)]. CdZnTe material is thought to be a possible candidate material for a room temperature high resolution gamma-ray detector. We first determined the absolute efficiency of a CdZnTe crystal of area 20 mm x 20 mm with the thickness ranging from 1 mm to 20 mm using the standard 1.33-MeV point source on the center axis 25 cm from the crystal surface. The absolute efficiency of these planar crystals ranged from 8.05×10^{-7} to 4.29×10^{-5}. For comparison, a 3 in x 3 in NaI detector (which subtends a solid angle approximately ten times as large at a distance of 25 cm from a point source) has an absolute efficiency of 1.33×10^{-3}. A comparison of the CdZnTe crystal efficiency with that of a standard LEPS detector is being undertaken. We have also calculated the relative efficiency of the CdZnTe planar crystals using energies of a uranium source. For example, the efficiencies of a 20 mm thick crystal relative to those of the 2 mm crystal are 1.02 at 72 keV, 1.11 at 102 keV, 1.52 at 143 keV, 2.3 at 202 keV. and 3.08 at 258 keV.

We have ordered a 3-gigabyte hard disk to be used in conjunction with our Monte Carlo calculations using MCNP. With the large data storage capability, detailed particle track histories can be retained and sorted to investigate effects such as random and coincidence summing in gamma-ray detectors. Previous operating systems problems on the MCNP computer cluster have been overcome.

APPENDIX A: A SUMMARY OF ALL MILESTONES AND DELIVERABLES FOR THE QUARTER

I. NDA MC&A Measurement Technology R&D

B&R No. GD060102

The Intelligent Actinide Analysis System (IAAS) is in routine operation.

An investigation of isotopic measurement problems that are outside of the present MGA application has been started.

II. Emission/Transmission Computed Tomography

B&R No. GD060202

Monte Carlo simulation of a plutonium MSE button with voids has begun to study the effect of the voids on isotopic determination.

III. Support to DOE Facilities in Implementation, Testing and Evaluation of LLNL Developed NDA Techniques

B&R No. GD060302

The Plutonium Solution Assay Instrument is undergoing calibration and testing.

IV. Monte Carlo Calculations of Gamma-Ray Spectra

B&R No. GD060102

We have simulated a spectrum for one standard plutonium source (PIDIE #1) with forty times as many tracks as our first simulation to continue to investigate the source of patterns in the residuals after the MGA fit of a simulated spectrum.

Simulations of planar CdZnTe crystals have been undertaken to calculate the relative and absolute efficiency of detectors made from this material.

APPENDIX B: A LIST OF ALL PUBLICATIONS PRODUCED DURING THIS QUARTER

There were no publications produced during the quarter.

Safeguards and Decision Support

R. Scott Strait, Deputy Associate Program Leader
Fission Energy and Systems Safety Program

INTRODUCTION

The purpose of the program is to develop systematic approaches and analytic tools for evaluating and enhancing the effectiveness of safeguards and security systems. We develop methodologies and tools for evaluating material control and accountability systems, measures protecting against insider threats, and measures that may contribute to the deterrence of threats. We transfer the technology developed through workshops and field consultations, and we evaluate available tools to determine their applicability to DOE safeguards and security interests. We also provide technical support to OSS on program planning, assessment and integration, and implications of arms control treaties.

SUMMARY OF MAJOR ACCOMPLISHMENTS

- Supported the Central Training Academy in teaching one ASSESS Course;
- Completed determination of user requirements for the DOE Security Clearance Electronic Processing, Transfer, and Recordkeeping (SCEPTR) System; and
- Completed preliminary design for pilot system of the SCEPTR System

TASK DESCRIPTIONS AND QUARTERLY PROGRESS

I. Safeguards Systems Studies LLNL 91019-94

B&R No.	Funding	Obligated
GD 06-02-05	$70K	$21K

This task develops systematic approaches and analytic tools for evaluating and enhancing the effectiveness of safeguards and security systems. We develop methodologies and tools for evaluating material control and accountability systems, measures protecting against insider threats, and measures that may contribute to deterrence of threats. We also transfer the

technology developed through workshops and consultations, as needed. We provide field assistance in the application of evaluation methods, and tools. We evaluate available tools to determine their applicability to DOE safeguards and security interests.

At our May 1993 program review, we were asked to provide input for OSS News & Views rather than publish our own newsletter. Last quarter, we provided that input to Ken Render of Battelle PNL, and the articles we submitted are slated for the next issue of News & Views (originally scheduled for publication October 1). We anticipate receiving many requests for ASSESS after the publication of the newsletter.

This quarter, we performed in-house testing of the Material Accounting (MA) activity database (completed last quarter) in the new Protracted Insider module of ASSESS, developed to support the requirement (in DOE 5633.3A) to perform vulnerability assessments for protracted theft or diversion. The testing comprehensively checked the completeness and consistency of the mapping logic for the list of MA activity detection event descriptions and potential insider MA activity defeat methods. In the course of in-house testing, we made additional refinements to the user-friendliness of the module by adding a message that helps remind the user to save recently input MA data. The algorithms for computing MA activity effectiveness were also rechecked and a minor bug was fixed. Additional detailed technical assumptions underlying the MA database model were formalized in an in-house document that can be easily added to documentation already existing for the module.

Our largest-effort task this year is the development of a vulnerability assessment technology transfer manual. We have been coordinating the planning of this work with Sandia and expect to increase our level of effort in the coming quarter.

II. Analysis of Safeguards and Security Requirements of Treaties that Impact DOE Mission

B&R No.	Funding	Obligated
GD 05-08-03	$132K*	$1K

This task provides OSS with comprehensive technical reviews of the safeguards and security implications of pending arms control treaties. Under this task, we analyze impact on DOE sensitive facilities and related inspection readiness planning requirements. We also evaluate alternative approaches to readiness to determine most efficient methods to achieve treaty compliance and protect DOE vital assets.

This quarter we were not requested to provide OSS with significant support on treaty requirements. On December 10, we briefed the OSIA and their contractors on our experiences with evaluating the risk of disclosure of sensitive information from on-site inspections. We presented our work on START suspect-site inspections, warhead dismantlement verification, and Open Skies.

*All carry-over from prior years.

III. CTA Support

B&R No.	Funding	Obligated
GD 05-06-02	$56K*	$27K

This task supports the DOE Central Training Academy (CTA) in preparing course materials and presenting safeguards courses in areas of LLNL expertise. This quarter, we supported CTA in the presentation of one ASSESS Course at CTA.

We continue to work with CTA to limit our teaching role to the most technical course subjects as CTA personnel take on an expanded teaching role. This year CTA is teaching the insider VA section without LLNL support. However, we continue to have a major teaching role in the ASSESS Course, and CTA personnel have not yet begun to have substantial participation. We have proposed areas of the course for transfer to CTA personnel next fiscal year. CTA has told us that they plan the development of an advanced VA course, and they have requested our participation in that endeavor.

The Protracted theft module of ASSESS is ready for distribution to the field, but has not been distributed due to lack of training resources. We have discussed the training options with OSS and CTA, and the most cost-efficient option seems to be to develop a self-guided tutorial. The tutorial would explain the concepts and modeling approach for protracted theft scenarios, as well as teach the ASSESS Protracted module user interface. The tutorial, along with exercises, would be aimed at experienced ASSESS Insider module users. Per CTA request, in July we submitted a proposal for developing this tutorial.

*No funds have been received by LLNL to date.

IV. Electronic Transfer of Personnel Security Data Technology Development

B&R No.	Funding	Obligated
GH-03	$2,950K	$262K

We are in the beginning phases of this three-year project. The overall project will develop an integrated system for the electronic transfer of personnel security data between the DOE and the Office of Personnel Management (OPM) and between DOE Operations Offices. This system for Security Clearance Electronic Processing, Transfer, and Recordkeeping (SCEPTR), will use existing hardware and software to the extent possible. The system will be compatible with the OPM main frame computer in Boyers, PA, and with currently Federal Bureau of Investigation (FBI) approved electronic imaging for transfer of fingerprints. DOE operations to be automated include the clearance process at the field offices and the contractor sites.

This quarter, we completed the systems analysis of the current paperwork process, the identification of all information flows, and the users needs and requirements. We have completed and internally reviewed the SCEPTR Phase I Requirements Document. We complete most of the preliminary design for the pilot system and are placing orders for the required hardware and software for development and deployment of the pilot system. We will be hosting a design review on January 26, 1994 at our Laboratory for DOE field office and DOE contractor clearance office personnel.

Individual activities this quarter included:

Visited OPM/FIPC facility in Boyers, PA to understand OPM processing, to determine OPM user requirements, to consider methods for accessing PIPS database, and to discuss methods for transporting fingerprints.

Visited DOE Oak Ridge field office, Y-12, DOE Albuquerque field office, and Sandia National Laboratories to meet with personnel security personnel and review their security clearance process. The objectives were to understand the existing system and to identify the user needs.

Numerous discussions with and visits to the local offices of several commercial vendors to understand their capabilities and their applicability to the SCEPTR system. These vendors included hardware and software vendors for computers, forms software, live-scan fingerprint systems, and communications software.

Met with representatives of Sandia to discuss applicability of CDOCS to the clearance processing system. Discussion centered on integration of CDOCS

system for existing clearance processing files with automated system for all new files and on the relative benefits of CDOCS compared to commercially available products.

APPENDIX A: SUMMARY OF ALL MILESTONES AND DELIVERABLES:

I. Safeguards Systems Studies LLNL 91019-94

B&R No. GD 06-02-05

None this quarter

II. Analysis of Safeguards and Security Requirements of Treaties that Impact DOE Mission

B&R No. GD 05-08-03

None this quarter.

III. VA Fundamentals and ASSESS Courses

B&R No. GD 05-06-02

- ASSESS Course presented at CTA, December 6-17.

IV. Electronic Transfer of Personnel Security Data Technology Development

B&R No. GD 06-02-04

- Completed initial identification of user requirements
- Completed preliminary pilot design

APPENDIX B. A LIST OF ALL PUBLICATIONS PRODUCED DURING THIS QUARTER

1. "SECPTR Site/User Survey Details," December 21, 1993.

2. Draft of "SCEPTR Requirements Document, Phase I," December 22, 1993.

Computer Security - Distributed Systems

Doug L. Mansur, Program Manager
Computer Security Technology Center

INTRODUCTION

The Computer Security Technology Center (CSTC) serves the Department of Energy and its community by providing expertise and solutions to the many information security problems present in today's computer systems and networks. Incidents of intrusions, computer viruses, the purposeful replacement of legitimate software for illegal purposes, and similar acts are being addressed by the creation of security software, the delivery of incident response expertise, and research and development into secure systems.

SUMMARY OF MAJOR ACCOMPLISHMENTS

I. Computer Incident Advisory Capability (CIAC)

The Computer Incident Advisory Capability (CIAC) assisted DOE sites with computer security incident handling and provided research into new security vulnerabilities.

CIAC was busy with Advisory/Information Bulletins, issuing six of these which addressed significant problems with a variety of Unix utilities; one discussed an SGI configuration problem. The other information resource services, Felicia and Irbis, also continued to be accessed regularly by our DOE constituency.

The Project Management Plan (PMP) timelines are being adjusted as needed to reflect incident handling demands. The PMP will be reviewed periodically by CIAC, DOE/HQ, and DOE/SAN.

II. Network Intrusion Detector (NID)

Tasking statements, budgets, and milestones were finalized. Several presentations to members of the DOE community were given. We put into place hardware and software to enable continued support, development, and testing of NID. We also obtained sponsorship from another Federal agency for additional NID development.

III. Security Profile Inspector for Unix and VMS Operating Systems (SPI/UV)

SPI 3.0 was granted ADPR&I release approval. A memo of understanding outlines the methods that will be employed for distribution. The SPI source

code and User's Guide are available electronically to all DOE users. Tapes and hard copy are also available.

A SPI/VMS maintenance release (version 1.2-2) was made to provide compatibility with DEC Alpha machines running VMS 1.5.

Sun Microsystems has agreed to devote internal resources, working with the SPI team, to develop a standard for binary authentication tables, and to then proceed to publish such tables for the software produced by Sun.

IV. Text Analysis Project (TAP)

The current prototype TAP software (based on three DOE Classification Guides) was used to search a DOE classified text file from the DOE Classification Office in Germantown. TAP found seven of the eleven known classified sections of text (a 64% hit ratio). An initial draft version of a TAP User's Guide was written.

V. Network Mapping and Detection of Unauthorized Cross-Connections (NetMap)

Definition of the initial scope and goals for the NetMap Project was completed this quarter, augmented by two presentations to OS&S staff visiting LLNL. Investigations of existing network management software have begun.

VI. Computer Viruses: Prevention, Detection, and Mitigation

Discussions are underway to define specific tasks to be incorporated into a planned sub-contract to UC Davis to meet our research objectives in the area of malicious code.

VII. Distributed Auditing System (DAS) Development and Standards

Debra Banning of SPARTA Inc. published an article on DAS in the November, 1993 issue of the EDP Audit, Control, and Security Newsletter.

Investigation into three new areas of interest began: 1) identifying what "should" be audited to provide the necessary information for multiple uses of audit data; 2) determining what audit data are currently lacking or not useful with respect to vendor products; and 3) devising a plan for adding a new node to the DAS.

VIII. Computer Security Guidelines Development

Although this task is not funded for FY94, it is being reported because the effort is being completed with FY93 obligated funding resulting from the lateness of the contract award with SPARTA, Inc. The current VMS System Security Guideline is being enhanced to improve its overall outline, to include new technical areas, and to update existing information in line with the new versions of the VMS operating system. The existing Guideline continues to be in demand and is being distributed on request.

TASK DESCRIPTION AND QUARTERLY PROGRESS

I. Computer Incident Advisory Capability (CIAC)

B&R No.	Funding	Obligated
GD060303	$410K	$70K

The Computer Incident Advisory Capability (CIAC) team members continued to assist DOE sites with numerous computer security incidents.

Interest continued in the Satan Bug Virus, with numerous requests for more information coming to Bill Orvis. An anti-virus program vendor called Satan Bug is annoying and difficult to remove, but is not intentionally damaging (like the Brazil Virus) and does not warrant hysteria. With respect to the Merry Xmas Virus, he notes that a commercial CD-ROM caused a virus alert by a virus scanner. Bill determined that this was spurious and alerted the anti-virus vendors.

While CIAC duty person, Sandy Sparks handled an incident involving two DOE sites. CERT notified CIAC that they had information that two DOE sites had been probed by an intruder. CIAC notified both sites; one site appeared to have been penetrated. That site rebuilt the penetrated system to ensure that if the intruder(s) had gotten any passwords, they would be unable to make use of them. The site expressed appreciation for CIAC's assistance.

Steve Weeber worked with the LLNL Computer Security Organization (CSO) to investigate a possible intrusion of a Laboratory Unix system being used at an employee's home. Steve physically inspected the system for signs of intrusion and tampering, and provided CSO with a report summarizing his findings.

Steve also worked with Herb Langenbach of Brookhaven National Laboratory to establish a secure means for making an information server available for Internet access. After examining the system, its configuration, and its software, Steve concluded that the system was adequately secured.

Allan Van Lehn's hotline activity included fielding questions on viruses and anti-virus software, X-terminal vulnerability, FTP access, and problems regarding the faxing of advisories.

Rich Feingold's hotline activity included a Satan Bug Virus inquiry, request for clarification of Data Physician PLUS! issues, sending out information on Macintosh security, and handling a Firewalls News Group posting about a new sendmail vulnerability.

Bill examined the Brazil Virus and sent copies to the anti-virus community. The Brazil Virus is very threatening to software resources. It triggers after 120 hours of computer use and writes random data to the hard disk. VirHunt 4.0B and Scanv 106 do not detect Brazil, though Scanv does detect a generic boot infector. F-Prot 2.09D detects it. So does the CPAV Windows version, with the current virus definitions file, but not the CPAV DOS version.

Bill examined a commercial disk that Vi-Spi reported to have the Tremor Virus but it appeared to be a false positive. There was nothing that looked like a virus on the disk; no other anti-virus programs detected anything and the program disk was not infecting. Also, he researched the Cansu Virus for Phil Sibert and sent Phil a copy of the CIAC virus database information.

Karyn Pichnarczyk's hotline activity included checking into several Internet probes, various virus (including Satan Bug) questions, a person who is against using anti-virus software, and inquiries from other government agencies.

Steve Weeber investigated the compromise of a machine at a DOE site by an external intruder. The intruder gained access to the machine by convincing a naive user to change the access controls on her account. It was later determined that the intruder then gained root access through the use of a previously unknown set of vulnerabilities. The local administrators secured the system and are considering using NSM to augment their security controls. Steve has been working with Sun Microsystems and expects a patch release to address this new vulnerability in the near future.

Steve was also contacted by the administrator of a major DOE mail hub regarding messages that had been received indicating an attack on a machine at an educational site by a machine at another educational site. Steve contacted both sites involved, and was able to determine that the activities were merely tests of recently discovered vulnerabilities.

CIAC issued the following advisories/bulletins during this quarter:

E-01 Vulnerabilities in Sun sendmail, tar, and audio
E-02 Vulnerabilities in SGI IRIX Default Configuration
E-03 Unix sendmail Vulnerabilities
E-04 xterm Logfile Vulnerability
E-05 SunOS/Solbourne loadmodule and modload Vulnerability
E-06 Solaris System Startup Vulnerability

No workshops were presented this quarter, although Rich maintained contact with several sites who are interested. He does have one scheduled for WIP in February.

Sandy created the bulk of a presentation on managing unclassified computer security which will be incorporated into the workshops.

Presentations:
Rich attended the annual INEL computer symposium, Innovations and Applications. He presented papers on Electronic Resources and Quantum Cryptography. Sandy made presentations on CIAC to the DOE's CSSMs during their annual meeting in Oakland. She also briefed personnel from the DOE's Safeguards and Security program when they visited LLNL during the quarter.

Rich attended the Super Computing '93 computer symposium. He made a presentation and was a discussion leader at the Director's Roundtable Session on Computing and Network Security.

Sandy attended the Automated Information Systems Security II Course ISC-211: Classified Networking in Oak Ridge. She prepared and presented two sessions: one on firewalls and the other on CIAC today.

Sandy also made a presentation on the status of CIAC to Bob Caldwell and others from Security Affairs who visited the Laboratory this quarter.

Constituent Interface:
At Idaho Falls, Rich met with many computer security officers, including twelve at a formal meeting he arranged. In addition, he had a long, detailed conversation with Ahmad Zadah, the new DOE CPPC for that area. They discussed some interesting and effective ways for the entire Idaho Falls location to effectively and economically utilize CIAC's strengths and expertise.

CIAC met with Ron Tencoti, head of the NASA Computer Incident Response Team, to discuss mutual needs, concerns, and opportunities for sharing expertise and resources. We expect to have a good working relationship with our NASA counterparts. They are a fairly new team and can learn much from our years of experience.

Conferences /training attended:
Rich attended the annual INEL computer symposium, Innovations and Applications. He also attended the Seybold San Francisco Symposium, investigating multimedia, video conferencing, and the latest in publishing/presentation technologies.

Allan attended a presentation by Caravell Networks on their monitoring and control software.

Steve attended the 4th USENIX Computer Security Symposium in Santa Clara. He attended a tutorial on the construction of Unix firewalls, which he felt would significantly aid him as he implements the CIAC firewall in the near future. While at the conference, Steve was able to spend considerable time with vendor representatives and individuals from the CERT Coordination Center, planning the handling of several serious vulnerabilities.

Allan met with Mr. Craig Jepson of the Livermore office to learn more about computer security plans in Digital Equipment Corporation (DEC). In recent restructuring, some groups were phased out and well known people left DEC, but computer security is still a vital concern.

CIAC Notes and DOE Newsletter submissions:
Allan was assigned to be the editor of *CIAC Notes*. He wrote and collected various articles from the other team members. Some of the articles were submitted to Phil Sibert for the IRM Update. Others were submitted to Randy Bishop for the Office of Safeguards and Security S&S News and Views publication. *Notes* will be distributed electronically via list processing software. It was converted from MS Word to ASCII and PostScript forms for mailing and distribution via CIAC's Information Server Systems, Felicia and Irbis. We will begin soliciting subscribers and distributing issues in January, 1994.

CIAC Firewall:
Steve continued to work on the deployment of the firewall. He supervised the installation of the new router and 10base-T concentrator and is working with the LLNL networking group to obtain the necessary network addresses.

Assistance to LLNL for the Security Evaluation (SE):
Since CIAC has been approached about helping DOE sites prepare for security evaluations and inspections, Sandy and Doug Mansur took this opportunity to become involved in a local SE and learn more about this process. Members of CIAC served on a friendly inspection team to look at LLNL's primary administrative computing facility. Their observations and comments were useful to the reviewing organization and CIAC gained valuable experience.

Sandy utilized her experiences in the unclassified computer security area to create a training class for LLNL which can be tailored to meet the specific requirements of any DOE site. She assisted AIS, Administrative Information Systems Department, in preparing for this SE.

DOE Client Wish List

Idaho Falls requests:

1. Help with Computer and Network Security awareness.
2. Rational threat model showing risks and "horror stories."
3. Help align DOE orders with "reality."
4. Help make efficient use of security resources.
5. Help protect the "tremendous volume" of desktop information.
6. Bring security "up to speed," focusing on new technology.
7. Need help interpreting rules, providing a modern, realistic picture.
8. A SPI-like tool for PCs.
9. Firewalls "cookbook."
10. Improved Data Physician distribution.
11. Guidelines, checklists.
12. CIAC Gopher server.
13. "Newsletter" to share experiences (all DOE information technology security).
14. More targeted bulletin distribution.
15. Series of technical "bulletins" at management level.
16. USEnet newsgroup.
17. More training and awareness, possibly satellite and video alternatives.
18. Training materials on-line. Lesson plans. Criteria on who should be trained.
19. Ways to articulate issues to management.
20. Automated training.
21. Training "games."
22. Definition of abuse.
23. Improve, remove "policeman" characterization.
24. White hat visits.
25. Help prepare for I&E.
26. LAN security consulting.

Rocky Flats requests:

1. They would like our council on Internet connections, MLS's, trusted paths, password management and control, and several other areas.
2. More motivation/description in bulletins.
3. Concerned with off-site network links; passwords traveling in clear text on LANs.
4. Would like DOE clarification of desktop, LAN, encryption issues (important); multi-level security (important); VMS for classified (two passwords); single user access for classified SNM (feel situation is getting worse).
5. User education/formal training.
6. Internet security document.
7. AppleTalk and other protocols on LAN (mixed protocol situation.
8. Password generation for PCs; password management, controls, and

resource controls.

9. System management activities; LANs; UNIX servers.
10. Impact of downgrading clearances.
11. Get names and telephone numbers out.
12. Deliver an electronic newsletter/monthly bulletin.
13. Offer a virus clearing house.

Oak Ridge requests:

1. Would like computer security training films; even a tape of a CIAC workshop session would be helpful.
2. Would like a "how to do it" document to use in satisfying DOE Order 1360.2B. (Apparently similar requests have come from other sites.)
3. Could CIAC help their sites prepare for an inspection? (There have been repeated concerns expressed about the upcoming I & Es.)
4. A half-day workshop on overall computer security.
5. What are the CPPM responsibilities regarding LANs, distributed systems, and desktop systems.
6. An electronic newsletter.
7. A one hour computer security awareness briefing (with war stories) for management.
8. More white papers and white hat visits to sites.

Fermilab requests:

1. A Network Incident Procedures document detailing procedures, line(s) of command, ESnet liaison, and reporting.
2. Alternative methods of communicating with CIAC should the network become unavailable.
3. A backup procedures document.
4. Clarification of CIAC's role vis-a-vis CERT/CC.
5 Find a way to alert DOE sites of vulnerabilities before a fix is available.
6. A report on unfixed vulnerabilities from vendors.
7. Support for SGI.
8. Help them push on vendors to fix security problems. CIAC offers more clout.
9. Strong coordination when multiple sites are involved.

Energy Research Community requests:

1. Help in generating a DECnet and IP site security document.
2. Information gleaned form LISTSERVers and security conferences.
3. A database of all known security problems and appropriate patches.
4. Assistance in validating tools for detection and deterrence of attackers.

CIAC Felicia Bulletin Board System Activity:

	Oct	Nov	Dec
Logons	53	61	38
Persons	15	17	11
Sites	14	17	10

CIAC Irbis FTP Server Activity:

	Oct	Nov	Dec
Logons	220	230	194
Persons	92	75	74
Files Transferred	1023	1083	844

CIAC E-Mail Traffic:

	Oct	Nov	Dec
No. of messages	123	194	268

Client Feedback

Constituent support:
Steve responded to the following requests:

1. Information regarding the construction of Firewalls for Unix systems. Steve provided the requester with documentation and offered to collaborate with him in this area.
2. Product summaries of available tools to monitor AppleTalk networks.
3. Tools to discover/disable the network sniffing capabilities of networked computers.

Kudos:
"Yes, I got the bulletin. Thank you very much. This has saved me a lot of work." --- Richard Smiley, Kokomo IBM PC Users Group.

Constituent support and Kudos:
Rich received favorable feedback regarding CIAC from Gary Christoff, LANL.

Karyn was nominated to be on an exclusive mailing list for anti-virus information (CARO).

Positive comments about CIAC from Rich's INEL meeting, October, Idaho Falls:

"CIAC is a tremendous alert system."
"Good alerts."
"Very effective."
"Nice to know you're there."

II. Network Intrusion Detector (NID)

B&R No.	Funding	Obligated
GD060103	$375K	$56K

We demonstrated capabilities and outlined present directions for the Network Intrusion Detector software package at two reviews for DOE OS&S, one on 10/15/93 and one on 11/05/93.

We finalized our work proposal for FY94 and started work on product configuration management and on assembling a user package for release in January, 1994.

Preparations were made to present a course to CSSM's and others in Automated Information Systems Security at Oak Ridge in January, 1994.

We acquired the sponsorship of the Defense Information Systems Agency for making improvements to the user interface of one of the key modules of the package and for further work in enhanced signature recognition.

III. Security Profile Inspector for Unix and VMS Operating Systems (SPI/UV)

B&R No.	Funding	Obligated
GD060103	$315K	$117K

SPI 3.0 obtained ADPR&I approval for release. A memo of understanding outlines the methods that will be employed for distribution. The SPI source code and User's Guide are available electronically to all DOE users. Tapes and hard copy are also available.

A SPI/VMS maintenance release (version 1.2-2) was made to provide compatibility with the DEC Alpha systems running VMS 1.5.

The current tasking centers upon producing a VMS compatible version of SPI which utilizes most of the current SPI 3.0 (Unix) code. Progress made in this area includes the creation and testing of MMS (Module Management System) files that issue the code compilation directives. These tests helped indicate areas of porting sensitivity. In addition, DEC Command Language (DCL) conventions for referencing files, directories, and devices have been studied to identify those portions of the SPI data-extraction system which must be expanded to accommodate VMS system inspections.

More generally, much of the SPI code has been upgraded to treat data with

dynamic memory, rather than static arrays, in order to avoid overflow problems which sometimes occur when SPI is applied to large network server systems.

Sun Microsystems agreed to devote effort working with the SPI team to develop a standard for binary authentication tables. The goal is to have Sun, as well as other OS vendors, maintain and publish such tables for the software they produce. These tables would be used by the SPI Binary Inspector Tool to authenticate critical system software and determine security patch levels. The SPI project leader enlisted the cooperation of the Texas A & M University "Tiger" security developer, Doug Schales, in an effort to produce an industry-wide standard. The SPI team produced an implementation of the Secure Hash Algorithm (SHA) from specifications provided in NIST FIPS-180. The algorithm is being investigated as a candidate for use in standardized authentication tables.

IV. Text Analysis Project (TAP)

B&R No.	Funding	Obligated
GD060103	$315K	$26K

Work began on improving the analysis techniques within TAP, and research was initiated to develop a method of automatically encoding other DOE Classification Guides. Discussions continue with the DOE Classification Office concerning the possible use of TAP to aid document review and release. Additional test files to further calibrate the prototype TAP software are being sought both at LLNL and in Washington.

V. Network Mapping and Detection of Unauthorized Cross-Connections (NetMap)

B&R No.	Funding	Obligated
GD060103	$210K	$16K

The NetMap Project began with a series of planning meetings, culminating with two presentations to representatives of DOE OS&S. The project goals were defined as providing tools for the secure management of computer networks, including such tasks as connectivity mapping, inventory, documentation, and the detection of unauthorized systems and cross-connects. An emphasis was placed on using commercially available software wherever possible, adding additional functionality as required.

The evaluation of available network management software has begun. Information, demonstration packages, and product documentation were

requested for several systems, including packages offered by Sun Microsystems, HP, and IBM.

VI. Computer Viruses: Prevention, Detection, and Mitigation

B&R No.	Funding	Obligated
GD060103	$55K	$3K

The process for establishing a sub-contract to UC Davis to meet our research objectives in the area of malicious code was initiated.

VII. Distributed Auditing System (DAS) Development and Standards

B&R No.	Funding	Obligated
GD060103	$100K	$19K

Debra Banning of SPARTA Inc. wrote an article on DAS that was published in the November, 1993 issue of the EDP Audit, Control, and Security Newsletter (front page).

The issue of identifying what "should" be audited to provide the necessary information for multiple uses of audit data was investigated. A plan to gather this information was devised: 1) review intrusion detection system development requirements for audit data; 2) examine past damage assessments and determine what information was useful or lacking; and 3) determine the best method of identifying audit data used by industry (e.g., questionnaire or article to solicit input).

A second issue of determining what audit data are currently lacking or not useful with respect to vendor products was also examined. An approach to determine this was devised: 1) review audit data that were found useful in detecting or tracking past intrusions; and 2) establish meetings with key vendors, such as Sun and DEC, to discuss current and future plans in this area.

Preliminary work on devising a plan for adding a new node to the DAS was begun. Nodes being considered are Sun OS C2, DEC Vax/VMS, and IBM MVS. The plan will identify: 1) the availability of each node; 2) the difficulty and time-frame to integrate a particular node; 3) the (dis)advantages to integrate a particular node; 4) the required integration resources; and 5) the required DAS modifications to facilitate the integration.

APPENDIX A, A SUMMARY OF ALL MILESTONES AND DELIVERABLES FOR THE QUARTER

I. Computer Incident Advisory Capability (CIAC)

B&R No. GD060303

Project Status Reports

FAX Vulnerability Study (Allan & Bill):
Bill Orvis is currently examining an inexpensive fax modem to see if it can be modified into a fax interception device. Commercial interception devices are very expensive, but inexpensive fax modems are showing up on many machines. Manufacturers information on the chip sets used in inexpensive fax modems has been obtained. This was needed before attempting to modify a fax modem into a fax interception device. We have obtained publications from the international standards organizations covering fax usage. This study continues to proceed at a reduced pace, due to higher priority activities.

CIAC Virus Update:
The document, "Computer Virus Information Update, CIAC-2301," is complete and is being prepared for publication. The "CIAC Virus Update (CIAC-2301 Rev. 1)" is complete and is being prepared for publication. The "CIAC Virus Update (CIAC-2301 Rev. 2)" is in preparation.

Using Felicia and Irbis:
The document, "The FELICIA Bulletin Board System and the IRBIS Anonymous FTP Server, CIAC-2303," is complete and is being prepared for publication.

Discretionary Access controls:
Allan researched and wrote a report on discretionary controls in Novell Networks for Bill Devaney at DOE HQ.

DEC workstation console security:
Allan put the finishing touches on the document, "The Console Password Feature for DEC Workstations, CIAC-2303."

Unclassified Audit Preparation Guide/Protecting Sensitive Unclassified Data :
Sandy created the bulk of a presentation on managing unclassified computer security. This will form the basis of these documents. Sandy completed an extensive training module on Managing Unclassified Computer Security which was used in a training session of the Laboratory's unclassified CSSOs. This material will now be incorporated into CIAC's workshop suite and will be converted into a document to be issued to CIAC's constituency.

System Backup Guidelines:
Allan researched and wrote a white paper on the many considerations that must be addressed before preparing a system backup strategy and policy. The paper was sent to Bill Devaney at DOE HQ.

Virus Database:
The virus database continues to be updated. Bill has analyzed the Merry Xmas Virus and has started examining the Brazil Virus. Karyn continues her Invircible evaluation.

Virus research:
Bill examined a demo version of the Virus Alert anti-virus package from TCT International. It appears to be a reasonably good package, but most of the advanced features were not available on the demo. He also examined the version of CPAV that comes with DOS 6 and found it to detect most viruses; however, there are inconsistencies between the DOS and Windows versions. Each detects different viruses. For example, using the most current update, the DOS version does not detect Brazil but the Windows version does.

Felicia and Irbis File Servers:
The files on the computer security file servers continue to be updated.

CIAC Publications:
Four CIAC documents are in the final stages of review and release:
1. Guide to the CIAC-2300 Series Documents
2. Computer Virus Update - CIAC-2301
3. The Felicia Bulletin Board System and the Irbis Anonymous FTP Server - Computer Security Information Sources for the DOE Community - CIAC-2302
4. The Console Password Feature for DEC Workstations - CIAC-2303

In addition to repeated requests for additional computer security information from CIAC, we have created an electronic CIAC Notes service. This has been announced and users are self-subscribing to this new service.

II. Network Intrusion Detector (NID)

B&R No. GD060103

No milestones or deliverables to report this quarter.

III. Security Profile Inspector for Unix and VMS Operating Systems (SPI/UV)

B&R No. GD060103

LLNL ADPR&I approved release of SPI 3.0 for Unix systems. The SPI 3.0

User's Guide was published. The source code and User's Guide (PostScript) are available electronically. Tapes and hard-copy are also available upon request.

IV. Text Analysis Project (TAP)

B&R No. GD060103

No milestones or deliverables to report this quarter.

V. Network Mapping and Detection of Unauthorized Cross-Connections (NetMap)

B&R No. GD060103

No milestones or deliverables to report this quarter.

VI. Computer Viruses: Prevention, Detection, and Mitigation

B&R No. GD060103

No milestones or deliverables to report this quarter.

VII. Distributed Auditing System (DAS) Development and Standards

B&R No. GD060103

No milestones or deliverables to report this quarter.

APPENDIX B. A LIST OF ALL PUBLICATIONS PRODUCED DURING THIS QUARTER

Heberlein, L. Todd, "Thumbprinting: A Technical Report" [in edit], Department of Computer Science, University of California, Davis.

Ko, Calvin, Deborah Frincke, Terrence Goan, Jr., L. Todd Heberlein, Karl Levitt, Biswanath Mukherjee, Christopher Wee, "Analysis of an Algorithm for Distributed Recognition and Accountability," Proceedings of the First ACM Conference on Computer and Communications Security, November 3-5, 1993, Fairfax, Va., Association for Computing Machinery.

DOE Automated Physical Security

Greg Davis, Program Manager

INTRODUCTION

The continuing goal of the DOE Automated Physical Security task (DAPS) is to enhance the LLNL developed Argus Integrated Security system to meet DOE security needs and to transfer Argus to the private sector.

Having identified an interested company, our objective is to enter into a Cooperative Research and Development Agreement (CRADA) to make the Argus Security technology ready for applications in the commercial sector.

SUMMARY OF MAJOR ACCOMPLISHMENTS

I. A Joint Work Statement document (JWS) was completed and approved. A complete CRADA proposal was submitted to and approved by the DOE.

TASK DESCRIPTIONS AND QUARTERLY PROGRESS

B&R No.	Funding	Obligated
GD 06 0201	$300K	$85K

Technology Transfer

The Joint Work Statement was approved by both the LLNL Technology Transfer office and the FESSP program office, signed by the LLNL Director, and sent along with the CRADA proposal to the Department of Energy for review and approval. We are on-track for a formal signing ceremony February, 1994.

We have been unable to secure further funding for the effort, and so the proposal was reduced to only the $300K per year available from OSS. Continued OSS funding in FY95 and FY96 is required to successfully complete the CRADA as defined. We consider this an absolute minimum required to sustain this CRADA activity. We will continue to look for funding elsewhere in the DOE to support this effort. The limited funds will impact the pace and scope of the CRADA. The delays activating the CRADA have already reduced the available funds for this years work.

A copy of the Joint Work Statement is being submitted to SA-134 for review.

The primary desired results is:

The development of a commercially viable Argus security product featuring:
- Reduced system cost (both hardware and software)
- System modified to an open architecture
- Increased flexibility in console configuration
- Increased user friendliness in enrollment and operation
- Decreased software maintenance requirements

The Technical Objectives include:
- System Engineering
- Database Standardization
- Databases Consolidation
- Console improvements
- Enrollment and Badging
- Additional Enhancements

Martin Marietta assembled a set of photographs that were provided by LLNL into an Argus briefing book. A copy of the book is being sent to SA-134 along with the Joint work statement. We were informed that this briefing book was used to brief Martin management and secure their support for the Argus CRADA. The text in the book was generated by the Martin Marietta engineers without input from LLNL. We will be working with Martin to ensure that references to LLNL in future documents will not be interpreted as an endorsement by LLNL of their commercial product.

Argus Standardization effort
There has been no activity in this area.

APPENDIX A, A SUMMARY OF ALL MILESTONES AND DELIVERABLES FOR THE QUARTER

DELIVERABLE **STATUS TABLE**

Original Deliverable	Description of Deliverable	Status
11/29/93	A Joint Work Statement for Argus CRADA will be Completed.	Completed 11/29/93
03/29/94	A prototype single small computer Argus Host with Access Control, Intrusion Detection, and Console operational capability will be demonstrated at DOE HQ or Livermore	On schedule
09/30/94	Final report on Electronic Security System standardization will be submitted. A year end report on CRADA activities will be submitted.	On schedule

APPENDIX B. A LIST OF ALL PUBLICATIONS PRODUCED DURING THIS QUARTER

None

DOE Automated Visitor Access Control System

Eric Steele, Program Manager

INTRODUCTION

The goal of this project is to minimize delays experienced by DOE employees for legitimate classified visits to DOE sites and enhance the ability of visitor facilities to positively identify the visitor.

An improved procedure for handling classified visits was developed as part of this task in FY 93 and support for the extension of these procedures to other sites is part of this year's objectives. Additionally, a feasibility study using hand geometry biometrics technology to validate visitors was completed, and the objective of this year's tasking is to extend these results to a prototype system that can be implemented complex-wide. Support for the extension of these procedures to other sites as well as making critical enhancements is part of this year's objectives.

SUMMARY OF MAJOR ACCOMPLISHMENTS

I. Start of an LLNL operational test of a encrypted DISS communications link.

II. Doug Sweeney traveled to DOE/HQ for installation of a second encryption device to begin comparison testing of encryption links.

III. Eric Steele and Melinda Lane traveled to DOE/HQ November 8th through the 10 to attend meetings with Glen Tayler and Sydney Teegarden of DP-68 regarding access to Weapons Data. Mr. Tayler agreed to allow the continued use of DAVACS for visits within the weapons complex require access to weapons data.

TASK DESCRIPTIONS AND QUARTERLY PROGRESS

Accomplishments achieved during the first quarter of FY 94 by STP are described below:

I.

B&R No.	Funding	Obligated
GD 06 0201	460K	100K

DISS Communications Security Analysis

Operational testing of the CYLINK Corporation's encryption equipment was initiated. This equipment was installed as part of the FY 93 tasking and is currently in operation between the LLNL clearance office and the DOE/HQ DISS system.

Doug Sweeney installed a second encryption device by IRE Inc. in order to compare the two encryption devices in operation. While at DOE/HQ Doug Sweeney had discussions with April Stottler, Geralyn Praskievicz, and Ron Sentell on encryption strategies. Further discussions on the encryption issue were held with CDSI programmers Rob Carpenter and Dan Smith.

Visitor Biometrics Verification

Continued work on the biometrics verification system. Screen applications and user interfaces are being developed. Coordination with HR-251 to allow modifications to the DISS computer system has started.

Classified Visit Procedures Improvement - Clearance Query Screen Enhancements

It was determined during the DAVACS testing period that additional data fields would be required on the Clearance Query screen. Survey forms were distributed to all facilities within the DOE complex requesting input for the additional fields. Survey results have identified the need for multiple clearance information including all active clearances, grant dates, and clearance numbers. This additional data on the Clearance Query screen will allow facilities to make a more informed decision regarding requests for classified visits.

A meeting has taken place at LLNL with Rob Carpenter, the CDSI programmer from DOE/HQ to discuss the feasibility of the additional fields. Mr. Carpenter concurred that the fields were feasible and a letter has been drafted to Ernie Wagner DOE/HQ for the final approval process. Mr. Carpenter indicated a 30 day turn around time would be required to complete the programming at DOE/HQ.

Classified Visit Procedures Improvement - Streamlining the Weapons Program Need-to-Know Access Requirements

The DAVACS process has made it possible for most DOE employees and contractors to travel without the use of a DOE Form 5631.20. The exceptions to these rules are DOE employees and contractors from non-weapons facilities who require access to weapons data. Eric Steele and Melinda Lane traveled to DOE/HQ November 8th through 10th to attend meetings with Glen Tayler and Sydney Teegarden, DP-68, and discuss the access requirements for Weapons Data.

Mr. Tayler agreed to allow the continued use of DAVACS for visits within the weapons complex which require access to weapons data. Glen has suggested addition fields within the DISS system to allow field offices to limit specific individuals access. A follow-up meeting is expected in January 1994.

APPENDIX A, A SUMMARY OF ALL MILESTONES AND DELIVERABLES FOR THE QUARTER

MILESTONES STATUS TABLE

Original Milestone	Description of Milestone	Status

No milestones are due in the first quarter.

APPENDIX B, A LIST OF ALL PUBLICATIONS PRODUCED DURING THIS QUARTER

None

DATE
FILMED
4/13/94
END