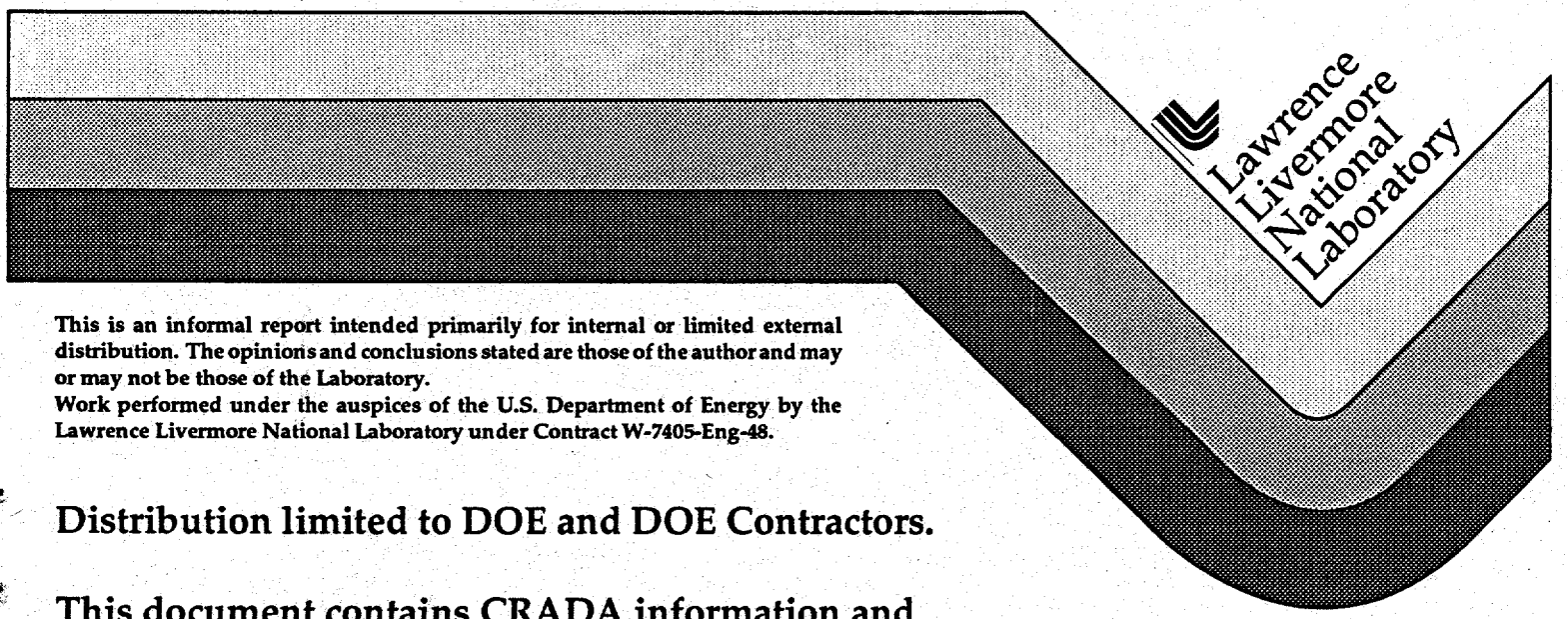
UCRL-ID-106454-94-4

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

Quarter Ending September 30, 1994

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

October 1994



Distribution limited to DOE and DOE Contractors.

This document contains CRADA information and therefore is not for public dissemination.

GH

DISCLAIMER

Work performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under Contract W-7405-Eng-48.

DISCLAIMER

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 Fourth quarter of Fiscal Year 1994 (July through September, 1994).

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.

The Safeguards Technology Program hosted members of the Office of Safeguards and Security at LLNL on August 17, 1994. At that time participants in the Safeguards Technology Program presented a review of recent accomplishments and plans for the coming year for each of the four funded tasks.

SUMMARY OF MAJOR ACCOMPLISHMENTS

I. NDA MC&A Measurement Technology R&D

- A modified version of MGA was developed to allow specification of a complex sample for absorption coefficient calculations, and successfully applied to a Pu/U/Cd alloy sample.

- GRPANL and PU238 codes were successfully adapted to determine the ^{238}Pu content in a variety of samples.

II. Emission/Transmission Computed Tomography

- Fabrication of the tomographic scanner for small dense samples is complete, and testing is ongoing.

- Analytical modeling of the sensitivity of transmission computed tomography is continuing, and is being compared to the results of Monte Carlo calculations.

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

- A second system to analyze for nuclear explosive-like assemblies (NELA) is being developed for Materials Management at LLNL.

IV. Monte Carlo Calculations of Gamma-Ray Spectra

- The porting to the personal computer of our Monte Carlo methodology for simulation of actinide spectra is continuing.
- Event histories generated in Monte Carlo simulations have been successfully written to disk and read back for analysis.
- A complex sample of enriched uranium with a small amount of weapons grade plutonium has been simulated in a high statistics calculation.

TASK DESCRIPTIONS AND QUARTERLY PROGRESS

Accomplishments achieved during the fourth quarter of FY94 by STP are described below:

I. NDA MC&A Measurement Technology R&D

B&R No.	Funding	Obligated
GD060102	$292K	$275K

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.

Plutonium Isotopic Analysis Development
Joseph B. Carlson, Kenneth E. Raschke, and Eugene A. Henry

Domestic safeguards R&D work related to MGA has concentrated on measuring of plutonium isotopics in 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 items has only been accomplished with a combination of analyses using both the MGA and GRPANL programs, with significant user interaction during the analysis. We have begun a program to study the analysis of a variety of "problem" samples in order to enhance the analysis performance and potentially reduce the amount of user interaction.

The urgent need to analyze samples containing ^{238}Pu lead porting several analysis programs into the Unix environment. The nature of these samples prevents MGA

from determining the isotopic ratios in these samples. The GRPANL suite of programs was ported as well as the PU238 code, which uses GRPANL output to determine ^{238}Pu content. This suite of codes are in use for the analysis of these samples.

Analysis of a spectrum taken from an unusual sample from Idaho, consisting of a relatively small quantity of Pu and U alloyed with a large amount of Cd, was attempted during this quarter. Again the nature of the sample prevents MGA from operating successfully. In fact the code diverges on several internal calibration calculations and will not run to completion. A special version of MGA was created that can be configured with virtually any sample composition before analysis is performed. The code then uses the composite absorption coefficients for the material specified during the calibration phases. For the Idaho sample, the modified MGA code produces answers consistent with the composition that the sample is believed to have.

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.

We are XMGA running under Unix/Motif and SpecView, and it is currently being evaluated by an analyst and by the MGA code physicist. We have developed an architecture or framework that covers all our second-generation or intelligent instrumentation and analysis concepts. This architecture is applicable to development efforts in both our domestic and international safeguards tasks. We continue to develop the Windows version of SpecView and winMGA, which will include tool bars, and will operate in C and C++ languages.

Enhanced Gamma-ray Signal Processing
Dean Beckedahl, Judith Kammeraad, Joseph B. Carlson, Kenneth Neufeld, and Allen V. Friensehner

Gamma-ray detection technologies using solid state detectors are important to many aspects of material control and accountability. While new detector materials are being investigated extensively, little effort is being expended on new approaches to signal processing. Emphasis has been on obtaining optimal energy resolution at the expense of other information contained in the signal from the detector crystal. However, it is well known that the leading edge of the output pulse of a solid state detector displays details which arise from the particulars of the gamma-ray interaction and the detector itself.

The goal of a new project being proposed for FY1995 for internal funding at LLNL is to conduct research and development applying available expertise in high bandwidth signal processing technology and methodology in order to utilize high frequency information in solid state detector signals. The proposed approach will be to measure and analyze the shape of the pulse with enough detail to accurately determine the spatial distribution of the disposition of gamma-ray energy within the crystal. This information could be used to enhance a number of key detector technologies, including suppression of Compton background without anticoincidence techniques, increased sensitivity for detection of specific radioisotopes, and improved energy resolution for room temperature detectors. This effort was supported at a low level during the last part of FY1994 by the Safeguards Technology Program in anticipation of LLNL funding in FY1995.

Progress in this project during the last quarter occurred in three areas: 1) noise characterization of the detector and recording system has been made; 2) detector response modeling and system response measurements have been done; and 3) a proper collimation system has been devised. The measurement of quantitative noise figures for the detector and recording system is crucial to modeling and devising discrimination techniques. The detector response modeling and system response are necessary to be able to understand the leading edge of the detector signals to be measured. The collimation will provide very accurate spatial information as part of the test data to be taken.

II. Emission/Transmission Computed Tomography

B&R No.	Funding	Obligated
GD060202	$146K	$137K

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

We have finished putting together the framework of our newly designed tomographic scanner apparatus. The collimator, alignment apparatus, and staging (borrowed from the Nondestructive Evaluation Division) have been integrated into the frame. We have started preliminary tests of the system and the collimator design using PIDIE sources and a 15% HPGe detector. The background in the room as mainly due to the decay of the ^{228}Th decay chain, probably from previous handling of $^{232,233,234}U$ in the hot cells in the room. We will design shielding for the detector. Rotational and translational stages to replace those currently on loan have been ordered. Hardware purchases for the scanner were funded by LLNL, and many fabrication services have been provided at no cost to the program by EG&G.

We are modeling the sensitivity of transmission computed tomography to determine the size and geometry of plutonium particles in media that are relatively transparent. Analytical expressions for the transmitted photon intensity of single spheres and cubes have been derived. These expressions have been analyzed to determine the dependence of transmission on the particle size, the collimator aperture size, the energy of the transmitted photons, and other variables. An interesting result is that particle size and geometry determination is facilitated by using a variety of gamma-ray energies, indicating that a multiple gamma-ray source that spans a wide energy range is optimum. Monte Carlo simulations of transmission with these variable are been carried out and compared the results from the analytical expressions.

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

B&R No.	Funding	Obligated
GD060302	$92K	$79K

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.

Support of Isotopics Analysis Systems 1 and 2
Joseph B Carlson

Routine support for running MGA was provided during this quarter to add the capability to automatically run MGA for samples measured with Materials Management isotopic systems 1 and 2. No code changes were made in the MGA program.

System to Analyze for Nuclear Explosive-Like Assemblies (NELA)
William M. Buckley, R. G. Lanier, Austin L. Prindle, and Allen V. Friensehner

A gamma-ray screening system has been developed for use by Material Management at LLNL for verifying the presence or absence of special nuclear materials in a sample. A second rack-mount NELA system is being prepared for delivery to LLNL Materials Management.

Measurement of ^{238}Pu in samples
Kenneth E. Raschke, Austin L. Prindle, and Joseph B. Carlson

Throughout this quarter we have been actively involved in the measurement and interpretation of ^{238}Pu samples. Analysis is complicated by ^{228}Th interferences, (n,n') reactions on both the sample and the detector, and detector deterioration because of the high neutron flux. Materials Management supported the measurements, interpretation, and detector maintenance. The software modification and integration activity was accomplished under the NDA R&D task.

IV. Monte Carlo Calculations of Gamma-Ray Spectra

B&R No.	Funding	Obligated
GD060202	$146K	$146K

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

Event histories generated in Monte Carlo simulations are crucial in understanding the details (e.g. coordinates, form, weight, energy, and angles) of a photon interacting with a detector crystal. We have successfully written and read back the event histories generated by the MCNP4A code with both the UNIX and PC-DOS platform. Our 3-GByte disk plays an important part in storing these histories for later analysis. A detailed history dump of what happened in a Ge crystal using a SPARC-10 processor will generate a 150 MByte file in a day of computing time.

We have just finished a high statistics simulation of 85% ^{235}U, 14% ^{238}U, and 1% of PIDIE #1 plutonium mixture. This simulated spectrum will be used to investigate the situation where there is a weapon grade Pu contaminant in an enriched U sample. Both MGA and MGAU codes will be used to analyze this spectrum so that problems encountered in such a situation can be understood. This will help determine what improvements should be taken in the next generation MGA or MGAU codes so they can reliably analyze such samples.

Porting Monte Carlo Simulation Capabilities to the Personal Computer
Tzu-Fang Wang

The new generation of personal computer platforms with processors operating at 90 or 100 MHz will allow users to inexpensively simulate informative plutonium spectra over a weekend, or detailed spectra suitable for analysis code intercomparisons in several weeks. With this capability, many users can generate spectra for themselves that contain a realistic representation of the physics of photon transport, and will not have to rely on models that only approximate spectral features. Thus we are extending our simulation capability to the personal computer platform.

As a first step, we have successfully ported the GAMGEN code to a personal computer which has a 386 processor and employs the DOS memory extender capability. GAMGEN is the code that generates the gamma-ray energies and intensities for aged actinide samples as input to MCNP. The user interface for GAMGEN has been rewritten for a personal computer VGA display. We have conducted alpha testing of the PC GAMGEN code, and have corrected problems related to file I/O and numerical precision.

We have purchased a personal computer with a 90 MHz processor. This computer performs typical MCNP calculations at a speed equal to a SPARC-10 processor. However, the entire personal computer with display, keyboard, 1 GByte disk, etc. is a fraction of the cost of a single SPARC-10 processor. Spectra simulations have been successfully calculated with this personal computer.

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

I. NDA MC&A Measurement Technology R&D

B&R No. GD060102

Begin investigation of needs for improved gamma-ray assay programs to address broader range of measurement problems--completed 9/94.

Report on plan to address need for improving gamma-ray assay programs in measurement systems--completed 7/94 and 8/94.

II. Emission/Transmission Computed Tomography

B&R No. GD060202

Fabrication the tomography scanner for R&D studies--completed 8/94.

Initial measurements with scanner begun--9/94.

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

B&R No. GD060302

Plutonium Solution Assay Instrument--delivered 2/94.

Upgrade of Intelligent Actinide Analysis Instrument--completed 7/94.

Documentation written for the system to analyze for nuclear explosive-like assemblies (NELA)--completed 6/94.

Proposal made to upgrade LANL two detector system and Pu-238 analysis system --presented 3/94 (LANL unable to fund hardware at this time).

Report on measurement experience with Pu-238 isotopic analysis instruments--data not provided to LLNL.

IV. Monte Carlo Calculations of Gamma-Ray Spectra

B&R No. GD060102

Modification to Monte Carlo methodology in include a more realistic electron scattering function and more realistic assignment of statistics from a detector response function--completed 4/94 and 7/94.

Monte Carlo calculations used to predict the effects of sample heterogeneity and matrix variation on measured gamma-ray spectra--completed 8/94.

Report on improved Monte Carlo code--delivered 5/94 and 8/94.

Calculated gamma-ray spectra for MSE plutonium button with heterogeneous Am distribution--delivered 8/94.

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

"Advanced Concepts for Gamma-ray Isotopic Analysis and Instrumentation", William M. Buckley and Joseph B. Carlson, presented at the 1994 INMM Annual Meeting, UCRL-JC-116145, 35th Annual Meeting Proceedings.

"Three Dimensional imaging of Molten-Salt-Extracted Plutonium buttons using both active and passive gamma-ray computed tomography", T. F. Wang, E. A. Henry, W. D. Ruhter, H. E. Martz, G. Patrick Roberson, and L. O. Hester, presented at the 1994 Symposium on Radiation Measurements and Applications, Ann Arbor, May 16-19, 1994; submitted to Nucl. Instr. and Meth.; UCRL-JC-116139.

"A Gamma-Ray Verification System for Special Nuclear Material", Robert G. Lanier and William M. Buckley, presented at the 1994 INMM Annual Meeting; UCRL-JC-116387, 35th Annual Meeting Proceedings.

"Monte Carlo Simulation of Plutonium Gamma-Ray Standards", T. F. Wang, J. B. Carlson, Z. Koenig, W. D. Ruhter, T. S. H. Lee, and J. Winn, presented at the 1994 Symposium on Radiation Measurements and Applications, Ann Arbor, May 16-19, 1994; submitted to Nucl. Instr. and Meth.; UCRL-JC-116138.

Safeguards and Decision Support

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

INTRODUCTION

The Fission Energy and Systems Safety Program (FESSP) Safeguards and Decision Support program area provides support to the DOE and other government sponsors in two related areas: (1) development and application of systems approaches for improving the security of nuclear and other critical facilities; and (2) decision analysis and risk management to support policy and decision making processes. The purpose of the program is to integrate advanced analytic methods with an understanding of technologies, economics, and the policy making process. We develop systematic approaches and analytic tools for enhancing the effectiveness of safeguards and security systems, including MC&A, physical protection, and personnel security. 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

- Pilot system of DISS Electronic Transfer module for security clearance electronic processing, transfer, and recordkeeping operational at LLNL, DOE OAK, and OPM.

TASK DESCRIPTIONS AND QUARTERLY PROGRESS

I. Electronic Transfer of Personnel Security Data Technology Development

B&R No.	Funding	Obligated
GH-03	$2,975K	$2,973K

As of the end of September, the DISS/ET pilot system was functional and we were sending test data from LLNL to the DOE Oakland Operations Office and on to the Office of Personnel Management (OPM). DISS/ET provides 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 module of DISS for security clearance electronic processing, transfer, and recordkeeping uses existing hardware and software to the extent possible. The system is compatible with the OPM main frame computer in Boyers, PA, and with current 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.

The transmission of the first live data through the pilot system is scheduled for Monday, October 31. This is a one month delay from the original target date of September 1994. The pilot system supports applicant entry of SF-86 and Security Acknowledgment forms, scanned images of applicant fingerprints and a signed SF-86 Part 2, page 10, review and processing of case data by the LLNL Clearance Office, review and processing of case data by the DOE Oakland Operations Office, transmission of data and scanned documents to an ET Gateway computer at the OPM in Boyers, PA, printing of the scanned fingerprints and documents at the OPM, and upload of the QSP data to the OPM PIPS system.

The June 1 demonstration of the system to the user community demonstrated sample applicant data entry, storage in the database, user review, fingerprint and document scanning, case transmission to the OPM, and printout of documents. Actual transfer of data to the OPM PIPS system was not included in the test.

Since the demonstration, the following has been accomplished:

- Development of all PC and UNIX based software
- Definition and development of the full pilot system database schema
- Integration of Identicator CardScan system PC scanning software for fingerprint and other document scanning and printing with ET.
- Development of the full SF-86 and Security Acknowledgment user entry forms.
- Development of Contractor and DOE User Interface forms sets.
- Acquisition of production system and additional development system hardware and commercial software.
- Development of a test plan and detailed test scripts.
- Integration testing of all aspects of the system.
- Installation of the production hardware at the OPM, DOE Oakland, and the LLNL Clearance Office.
- Development of user guides and training materials - these are draft format only for the pilot deployment.
- Planning visits at three operations offices and their affiliated prime contractors to plan 1995 deployment of ET.
- Development of draft security plans for ET. This includes a DOE HQ Blanket plan and a local DOE Oak plan.

On September 19, an end-to-end demonstration of the system was given here at LLNL to the DOE HQ Office of Safeguards and Security (E. Wagner and A. Stottler), the OPM (P. Lattimore and K. Dillamen), and representatives of the DOE OAK, NV, and RL Operations Offices.

Initial operation of the pilot system will be parallel to the existing paper system. This will allow full validation of correct transmission of cases to the OPM. Parallel processing will continue through the period of pilot evaluation by the user community. Concurrently, the DISS/ET team will continue development, bringing the system to full functionality.

Problems noted in our last quarterly report concerning the CUI/DUI Communications Security have been resolved. Security of the interactions between DOE or Contractor reviewers and the RPS Database is provided by LanGuardian encrypting routers by UUNET. The LanGuardians are installed and operational. A secure version of Oracle SQL*Net, called Secure Network Services is a potential software solution to the above security between users and the database. A beta copy should be available to the team within a month for evaluation. If the evaluation is favorable, Secure Network Services may replace future LanGuardians.

We have found some limitations in the JetForm commercial forms software, which is the basis for the user interfaces. The software may inhibit future functionality. We have met with JetForm local representatives and technical support personnel. JetForm has full detail of these limitations and has promised to respond to our concerns. We also are exploring other ways of dealing with the limitations.

Draft requirements specifications and documentation of existing systems for both the adjudication support (ASIST) and existing personnel file image capture have been completed. The development of adjudication support software is part of our FY95 tasking. The software is necessary to help the security specialists manage electronic reports on background investigations once the OPM is able to transmit their reports electronically. The analysis of the requirements for image capture of existing personnel files was requested by DOE HQ in response to needs of the Operations Offices. Many of the Operations Offices are considering purchasing or developing systems to image existing personnel files. The analysis performed by LLNL was focused on eliminating duplication of effort and ensuring that such systems were compatible with DISS/ET. Reports on both of these efforts are under final review by the DISS/ET project team.

In the fourth quarter, we received additional funding and tasking to explore the impacts of using trusted operating systems and labeled databases for DISS. These technologies are normally only required for classified systems. We

performed a survey of the available products and investigated those that appeared to be most applicable. This information gathering included discussions with representatives of other Federal agencies that may have more experience with these technologies. Based on this research, the Secureware based trusted operating system was deemed the best choice at this point. We gained experience with both the SCO and HP versions of this product. Most of the DISS UNIX-based software was then ported to a B2 level environment on an HP workstation. This port excluded the database and database related ET software. Throughout this effort, we coordinated our efforts with the staff of MMES, who received complementary tasking and funding. We are in the process of documenting our findings.

II. OSS Enterprise Information Resource

B&R No.	Funding	Obligated
GH-03	$200K	$200K

This project re-engineers and extends the DISS personnel security databases. It is the first step in an overall plan to modernize the computer systems of the OSS in order to form an integrated solution to the organization's needs. The product of this project will be an operational replacement for DISS which incorporates modern software design and allows for easy enhancements, low maintenance costs, and growth in functionality. The modernized DISS will include most of the functionality currently provided by independent systems currently operated by many Operations Offices.

The DISS/PSDB (Personnel Security Database) team has begun systems analysis of the existing personnel security databases, including the Central Personnel Clearance Index (CPCI), the Classified Visit Control System (CVCS), DOE Authorized Visit Access Control System (DAVACS) and complementary systems at several Operations Offices. Site visits to Savannah River, Oak Ridge, Oakland, Richland, Las Vegas, and Rocky Flats Operations Offices have been completed. The team is reviewing the CPCI and related headquarters systems, reviewing the interface needs of the Operations Offices and M&O contractors, and developing requirements an design for integration of this functionality. These systems analysis and requirements definition is being coordinated with a parallel effort for the Weapons Data Access Control System (WDACS) funded by DP-31. The systems requirements definition should be completed by the end of December 1994.

III. Analysis of Insider Threats Against Computerized Nuclear Materials Accountability Applications LLNL 94005-94

B&R No.	Funding	Obligated
GD-06-01-03	$340K	$320K

This project is developing methodology to be used in the evaluation of insider threats against computerized nuclear materials accountability applications. This methodology is important, because the Department relies heavily on computer systems to manage nuclear materials accountability data and to detect diversion of nuclear materials. The project will assess current materials accounting applications to identify information flows representing insider activities with potential serious consequences. We will document a methodology for performing insider analysis of current application systems, such as LANMAS, as well as for future designs. The assessment of applications will be useful in future materials control and accountability (MC&A) and computer security policy development.

After completing systems familiarization for current and planned MC&A applications, we proceeded with further development of the information analysis methodology of human-initiated actions. We developed an analysis structure that provides an organizing mechanism for evaluating insider threats against computerized MA systems. This structure incorporates the major MA subsystems, authorized users and transaction activities. This structure supports the development of an analysis protocol/checklist, linked to performance criteria and potential vulnerabilities.

IV. Safeguards Systems Studies LLNL 91019-94

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

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 consultations, as needed. We continue to provide field assistance for ASSESS and in the general application of evaluation methods, and tools. We evaluate available tools to determine their applicability to DOE safeguards and security interests.

Our largest-effort task this year is the development of a vulnerability assessment technology transfer manual. We have developed questionnaires for vulnerability assessment tool users and developers and have been coordinating the planning of this work with Sandia. We have begun participating in the development of ASTM vulnerability assessment standards. The OSS has had the questionnaire for distribution and it has been revised to incorporate OSS comments. Although this task is not scheduled to receive additional funding in FY95, we are committed to compiling, reviewing, and analyzing the responses to the questionnaire. We have continued to support ASSESS users in the DOE complex with answers to questions and distribution of software.

V. 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. In a related effort we participated in a LLNL OPSEC assessment of the impacts of on-site inspections at LLNL.

*All carry-over from prior years.

VI. CTA Support

B&R No.	Funding	Obligated
GD 05-06-02	$28K	$28K

This task supports the DOE Central Training Academy (CTA) in preparing course materials and presenting safeguards courses in areas of LLNL expertise. We had no teaching obligations this quarter. We have reviewed the ASSESS user's manual prepared by a CTA sub-contractor.

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.

CTA has told us that they plan the development of an intermediate 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.

APPENDIX A: SUMMARY OF MILESTONES AND DELIVERABLES:

I. Electronic Transfer of Personnel Security Data Technology Development

B&R No. GH-03

Date	Milestone or Deliverable	Status
12/13/93	Preliminary systems design	Milestone met
12/31/93	Design document	Delivered
3/31/94	UNIX computers for the OPM site gateway, the DOE OAK site gateway, and the LLNL site gateway with commercial operating system software	Delivered
4/1/94	Begin test at LLNL and DOE/OAK	Milestone met
5/31/94	Telecommunications and security systems integration complete	Milestone met
6/30/94	Complete system ready for test and evaluation	Milestone met
6/30/94	Appropriate communications equipment needed to complete and SMTP mail connections at all pilot sites with all software	Delivered
9/30/94	Complete test and evaluation	Milestone delayed until October 28, 1994
9/30/94	Systems at DOE OAK, OPM, and LLNL operational	Delivered

II. OSS Enterprise Information Resource

B&R No. GH-03

None this year. Completion of systems analysis and definition of requirements will be completed by December 31, 1994.

III. Risk-based Evaluation of Computerized Nuclear Materials Accountability Systems LLNL 94005-94

B&R No. GD 06-01-03

Date	Milestone or Deliverable	Status
5/31/94	Substantially complete systems familiarization	Milestone met
6/30/94	Develop information analysis methodology	Milestone met
6/30/94	Program review briefing	Delivered
8/31/94	Extend methodology to applications system components and interfaces	Delayed until FY1995
9/30/94	Document methodology for performing insider analysis of application systems	Delayed until FY1995
9/30/94	Final report on the risk-based management approach	Delayed until FY1995

IV. Safeguards Systems Studies LLNL 91019-94

B&R No. GD 06-02-05

Date	Milestone or Deliverable	Status
4/1/94	Complete survey on VA techniques	Milestone met
4/30/94	VA Articles for OSS Newsletter	Pending resolution of questionnaire
9/30/94	Technology transfer manual on VA tools and techniques	Awaiting distribution of questionnaires by OSS

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

B&R No. GD 05-08-03

None this year.

VI. VA Fundamentals and ASSESS Courses

B&R No. GD 05-06-02

Date	Milestone or Deliverable	Status
12/31/93	ASSESS course	Delivered

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

DOE DISS/ET Pilot System by R. Scott Strait and Ernest E. Wagner, UCRL-JC-118253, July 1994 (This paper was prepared for submittal to the Institute of Nuclear Materials Management).

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 continued to assist DOE sites that were experiencing Unix-based attacks, such as the "sniffer," occurring through public networks like the Internet. Sniffer attacks and automated attack scripts continue to afflict sites that do not keep their host systems up-to-date with security patches. Recent attacks are more sophisticated than those previously seen.

CIAC completed a "white hat" visit as part of Woody Hall's CS Quip program to help sites understand their information security profile and to have additional information to use in improving their computer security programs.

In addition, sites experienced an increase in virus outbreaks. One particularly damaging virus was the "One_half" virus. CIAC's response saved one organization many hours and dollars in helping them prevent further infection and clean up damaged systems.

II. Network Intrusion Detector (NID)

A prototype version of real-time NID has been completed and an alpha version is about to be released to clients. An additional capability has been added to NID—the ability to catalogue all services offered to the "outside" from computers within a given security domain. We anticipate its use to

check for adherence to specific policies at some large DOE organizations.

The capability to recognize and parse NFS and SNMP packets has been developed. This will be used to allow NID to recognize attack signatures within these protocols.

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

SPI underwent extensive revision to address new security vulnerabilities, the majority of which were treated by revisions to the suite of CQL inspection scripts. The former BIT subsystem was replaced by a revised Binary Authentication Tool employing the proposed BASIS standard format authentication tables. Release of SPI 3.2, with upgraded documentation, is expected to occur in the third week of October.

Work toward a unified SPI (Unix+VMS) system continued, with the compile and install procedures being rewritten to accommodate the VMS DCL (DEC Command Language) and allow NFS-mounting of the sources from a Unix development area.

IV. Text Analysis Project (TAP)

A subset of the prototype version of the TAP software was successfully transported to Sandia, Albuquerque; this prepares us for a beta test at the Sandia site in the near future. We have implemented an initial workstation screen design for an enhanced TAP user interface, and the design has been through an initial review process.

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

The implementation of the prototype NetMap tool was completed this quarter. Local testing and debugging was completed, and plans for a beta test of the software on a classified network were established.

VI. Computer Viruses: Prevention, Detection, and Mitigation

Work continued on devising new methods for identifying the presence of malicious code, especially polymorphic viruses. These methods will speed the analysis of new viruses by automating some of the tedious tasks that anti-viral researchers currently must undertake. These methods can be categorized into two areas: static and dynamic analysis.

VII. Distributed Auditing System (DAS) Development and Standards

We are continuing this effort using faculty and graduate students at UC Davis. A preliminary investigation into goal-oriented auditing and logging was begun.

VIII. Computer Security Guidelines Development

Although this task is not funded for FY94, it continues to be reported because the effort is being completed with FY93 obligated funding resulting from the lateness of the contract award with SPARTA, Inc. The VMS System Security Guideline update effort has produced a draft version that is currently being reviewed by LLNL personnel. This review has been positive to date and should be completed shortly. We plan to distribute this document after consulting with the sponsor and after identifying a proper distribution list.

TASK DESCRIPTION AND QUARTERLY PROGRESS

I. Computer Incident Advisory Capability (CIAC)

B&R No.	Funding	Obligated
GD060303	$501K	$466K

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

Key events in the last quarter of FY94 were: complete CIAC's first formal "white hat" effort for a moderately sized DOE site; prepare and present at the Sixth Annual Incident Handling Workshop sponsored by FIRST; handle two rather large virus incidents (KAOS4 and One_half); establish an electronic "work area" for Robert Caldwell's Quality Panel; make presentations about CIAC and today's threats to the DOE OIT Conference, Ed McCallum, and others from the office of Security Affairs; complete drafts of several new technical documents; present a workshop on Securing Unix systems for LLNL; and prepare for the FY95 planning meeting at DOE Headquarters. In addition, CIAC published 4 advisories/bulletins and distributed the third issue of CIAC *Notes*.

CIAC's first formal "white hat" effort was successful in several ways: the site reported they benefited greatly by "seeing" themselves through a hacker's eyes. The site experienced very graphically where their greatest efforts needed to be made in strengthening their information protection program. CIAC also presented a day-long tutorial on topics relevant to their security needs. The site is developing new operational procedures and is increasing their funding for their security program. CIAC personnel learned much from this process and are already fine tuning procedures, tools, etc.

CIAC was a strong contributor at the FIRST Incident Handling Workshop, presenting a day-long workshop on the technical aspects of incident handling, a paper on threats, and serving on panels that dealt with the problems that incident teams in FIRST face.

CIAC delivered a tutorial on Securing Unix Systems for LLNL (it was not a workshop because of the large number of attendees). This session was video taped by LLNL so that CIAC could distribute the information to other sites.

CIAC also completed near final drafts of several technical documents all of which will be available on-line in ASCII, PostScript, Word, and WordPerfect formats: *Securing Internet Information Servers, Unix Incident Handling Guide, Electronic Resources for Security-Related Information, Data Security Vulnerabilities of FAX Machines,* and *User's Guide to Data Physician.*

II. Network Intrusion Detector (NID)

B&R No.	Funding	Obligated
GD060103	$438K	$365K

We produced a prototype real–time version of NID. This prototype detects and signals, in real–time, the appearance of unexpected nodes within a security domain. Such service providers need to be carefully documented and monitored. In addition to its real-time signal, statistics on the intruder's partners, the protocols used, and the volume of data transferred are kept. This data is saved on disk for use by future post–analysis tools. During data collection, simple reports are produced on a periodic basis.

We also added a new mode to NID that produces a list of all computers within a security domain that provide selected services to computers external to that domain. In addition to the list, statistics on the daytime and nighttime volume of these services are kept. This data is also saved on disk for use by future post–analysis tools. During data collection, simple reports are produced on a periodic basis.

A user's guide to both of these NID extensions has been written. The code is currently being reviewed and tested, and will then be released to selected users for evaluation.

We continued distribution and customer support via telephone, fax, and U.S. Mail for the NID 1.0 release.

We developed an initial capability to parse, display, and understand the contents of both Simple Network Management Protocol (SNMP) and Network File System (NFS) packets. Work is proceeding to develop mechanisms to describe and recognize attack signatures within each protocol and to present this data to a security officer using NID.

We examined and collected new attack signatures for new types of intrusions. We continued collaborating with UC Davis on ways to recognize attacks that we Unix-specific file system mounting mechanisms.

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

B&R No.	Funding	Obligated
GD060103	$357K	$357K

Security functionality will be enhanced significantly with the pending release of SPI 3.2.

New security functionality includes permission and ownership checks for many additional user and uucp configuration files, inspection of both the "xterm" and "uucp" programs for Set-UID vulnerabilities, examination of FTP subdirectories to insure they are not links to other parts of the file system, reporting of dormant user accounts, and enhancement of the CQL user and group query capability.

A completely revised Binary Authentication Tool (BAT) replaces the former Binary Inspector Tool (BIT) in the new SPI 3.2 release. BAT employs flexible format, BASIS authentication tables. Preliminary tables for Sun/SunOS (4.1.2, 4.1.3U1), SGI/IRIX 5.2, and DEC/ULTRIX 4.4 operating systems have been generated, and will be made available in concert with the SPI 3.2 release.

A new release of the SPI user documentation is near completion. The single SPI User's Guide has been divided into two documents, to ease maintenance difficulties associated with very large files. These will be the SPI 3.2 User's Guide - revision 5, and the SPI 3.2 Reference Manual - revision 1.

The SPI/V (VMS) port is nearing a milestone with the testing of a revised "Build" hierarchy. This was needed to support SPI/VMS porting using common, NFS-mounted sources while allowing developers to use the Unix software development environment (editors, commands, etc.). We have successfully set up makefile scripts that allow a single module dependency file (modules.mk) that can be used by both Unix make and VMS MMS. We have prototyped Unix makefiles and VMS MMS files to drive the common file in each environment. We are working on defining the host dependent (Install) structure.

Additional SPI Training Workshops were presented at Los Alamos National Laboratory on July 7th and at Sandia, Albuquerque on August 16th. Sandia, Livermore has submitted a request for a SPI workshop in November.

IV. Text Analysis Project (TAP)

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

TAP's analysis capabilities continue to be improved: we are installing the DOE HQ supplied Classified Guidance System (CGS) thesaurus as part of the analysis rule base. We are translating the initial workstation screen prototype to the IBM Windows environment as an alternate user interface for TAP. We continue to look at commercial alternatives to supplement the TAP analysis

software. Additional test files to further calibrate the prototype TAP software continue to be sought both at LLNL and in Washington. We plan to release a version of TAP software suitable for network file monitoring in February 1995.

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

B&R No.	Funding	Obligated
GD060103	$182K	$144K

Implementation of the NetMap tool prototype was completed this quarter. The tool interfaces with the network management software database to determine the list of authorized network hosts and then interrogates the appropriate network address ranges looking for unauthorized hosts. The prototype also allows a set of addresses to be added to the interrogation list at run-time. These addresses allow for the detection of unauthorized network cross-connections.

The tool was tested locally and was found to be robust. It was executed for long periods of time with no evidence of memory leaks or performance degradation. Initial plans for a beta test in a classified environment were established. The beta test is expected to take place in early FY95.

VI. Computer Viruses: Prevention, Detection, and Mitigation

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

Statically analyzing many variants of a particular polymorphic virus has lead to some promising results. By examining a statistically significant sample of variants, one can begin to discern a pattern of machine instruction use that can be used for detecting any of the virus' variants. Working within the confines of a set of heuristics, experiments with available polymorphic viruses show that each virus tends to use certain unique combinations of instructions that normal, uninfected programs do not use. Furthermore, variation across variants of a particular virus does not tend to be great enough to circumvent this technique.

Shortly, this data will be used in an automated classification system that is intended to promote faster determination of whether or not a program is infected with a particular virus. It should be noted, however, that these results are only preliminary.

Presently, the task of determining which instructions are important in the virus' signature is done manually. Also, the polymorphic viruses that were available (and therefore tested) were not from the most recent strains known to the anti-viral community. As new viruses are acquired, they will be used to further test this technique. In order for this technique to be more useful, an automated method for determining the importance of particular instructions must be developed.

The work on dynamic analysis continues in the development of the IBM PC simulator. Viruses can be single-stepped, or run in their entirety, while monitoring certain behaviors such as writing to low memory over DOS code, changing DOS executable files, etc.

Newly added modules include a hardware-level file system, a system clock, and an instruction pre-fetch queue. All modules have been implemented, although various testing and debugging tasks remain. The file system module allows the simulator to present virtual disc drives to the program being examined. This file system simulates a DOS hardware platform down to the level of the ports. The clock module simulates the action of the system clock for the 80x86 processor, adjusting the time depending on the particular duration of each executed instruction. The instruction pre-fetch queue module allows the simulator to close one avenue by which some viruses can evade detection.

These new modules will be tested against a collection of viruses, from simple overwriting viruses to complex polymorphic ones.

The virtual file system simulates a DOS machine at the hardware level. Thus, even software that makes direct calls to the hardware can be run on the simulator. The BIOS code from an IBM XT is copied into simulated ROM, and a copy of Microsoft DOS can be loaded from the simulated disk, through BIOS calls issued by the startup sequence that exists in ROM. Thus, this directly simulates the startup procedure that an actual XT runs when it is powered up.

The hardware is simulated by implementing virtual ports in software. In a real machine, the drive controller and Direct Memory Access (DMA) controller listen to these ports for specific commands. These commands come in byte strings of a known format. The simulated machine watches for these same byte strings, and acts accordingly. For example, if the byte strings denoting "format track" are received, then the appropriate "track" in the simulated drive is formatted. The code to monitor the ports has been completed, and it recognizes all byte strings that are known to be meaningful. It is possible that additional byte string commands may be discovered in the future, but the design provides for easy integration of any additional byte string commands.

Developing an event library to detect and analyze significant events that occur on the simulated drive (in order to recognize virus activity) is in its early stages. A File Allocation Table will exist on any simulated drive that has been DOS formatted. By monitoring this table, the simulator could determine which sectors of the disk contain .COM or .EXE files. If a suspicious program were to write to such executable sectors, this event could be detected instantly, since the byte strings to initiate this behavior must pass through the simulated ports.

The module to simulate the system clock has been implemented, but not yet thoroughly tested. The motivations for this addition were twofold. First, to facilitate detection of malicious code that checks the clock to determine whether it is being run on a simulator or on a real machine. Since debuggers and simulators take longer than a physical machine to execute instructions, a virus could check the system clock to determine whether an instruction sequence took a "realistic" length of time to execute. Second, simulating the internal DOS time counter makes it easier to test Time Bomb programs.

The instruction cache module currently simulates the 8086 pre-fetch queue, although in the future, the cache module can be upgraded to simulate the cache in other 80x86 processors. This module was motivated by viruses like "Whale," which can hide themselves from debuggers by writing over instructions after those instructions have already been fetched into the cache. The instruction cache module is fully implemented, and is currently undergoing testing and possible debugging. Testing will include running the "Whale" virus on the simulator, to detect its attempt to cover its tracks.

VII. Distributed Auditing System (DAS) Development and Standards

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

We focused on goal-oriented auditing and logging. We decided to focus on this because in order to design a standard log format, we need to know what those logs should contain.

First, we asked what information needed to be logged for each of several security policies to determine if a violation (or attempted violation) were to occur. We used the Bell-LaPadula (military) security policy, because it is well-known and often used in practice (in some form). We also used the Chinese Wall policy, which is much more complex and is also used in practice in the commercial world. We derived conditions under which a violation would occur, and what would show the violation.

We then considered which system calls a computer which implements these policies would show on an attempted violation (or real violation) of these policies. We have been looking at a Unix-like system (that is, an idealized one) and are extending our work to include SunOS systems.

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

I. Computer Incident Advisory Capability (CIAC)

B&R No. GD060303

4 Bulletins/Advisories:
- E-31 Sendmail -d and Sendmail -oE Vulnerabilities
- E-32 KAOS4 Virus
- E-33 SGI Help Vulnerabilities
- E-34 One_half Virus

CIAC *Notes*, Issue No. 3

5 technical documents:
- *Security Internet Information Servers*
- *Unix Incident Handling Guide*
- *Electronic Resources for Security-Related Information*
- *Data Security Vulnerabilities of FAX Machines*
- *User's Guide to Data Physician*

3 tutorials/workshops
- BNL
- LLNL
- FIRST Incident Handling Workshop

II. Network Intrusion Detector (NID)

B&R No. GD060103

The alpha version of real-time NID was completed. A capability to parse NFS and SNMP packets was also developed.

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

B&R No. GD060103

The Binary Authentication Tool was developed to replace the BIT tool.

IV. Text Analysis Project (TAP)

B&R No. GD060103

A prototype user interface was designed and is being reviewed.

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

B&R No. GD060103

The first phase of the NetMap prototype tool was completed and is being tested for robustness.

VI. Computer Viruses: Prevention, Detection, and Mitigation

B&R No. GD060103

Newly added modules to the IBM PC simulator include a hardware-level file system, a system clock, and an instruction pre-fetch queue.

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

As memtioned above.

DOE Automated Physical Security

Greg Davis, Program Manager

INTRODUCTION

The initial goal of the DOE Automated Physical Security task (DAPS) was to enhance the LLNL developed Argus Integrated Security system to meet DOE security needs and to transfer Argus to an appropriate commercial firm for use in the private sector.

Having entered into a Cooperative Research and Development Agreement (CRADA) with Martin Marietta Information Systems (MMIS) our goals are to impart Argus system development knowledge to MM, to cooperatively add commercial appropriate functionality to the Argus Security system, and to successfully complete the 3 year course outlined in the CRADA.

SUMMARY OF MAJOR ACCOMPLISHMENTS

I. The Martin Marietta CRADA members, with the support of LLNL assembled an Argus Demonstration System for use in commercial system marketing and development efforts. This system was shown at the American Society of Industrial Security (ASIS) annual convention which was held September 19-21 in Las Vegas, Nevada.

II. An alternative magnetic stripe card reader has been integrated with the Argus software for use in the access control and intrusion detection subsystems. This device is targeted for applications where reduced security and functional requirements exist which allow a more cost effective entry control device to be used in place of the LLNL Remote Access Panel (RAP).

III. A CRADA task to use SQL rather than EQL as the standard for the creation of database tables was initiated. The current effort focused on the creation of the access control subsystem tables for the enrollment database server which were required for the enrollment system changes that were incorporated in the Argus baseline 17.

IV. A joint MMTI and LLNL CRADA program review was held on 22 July 1994 at LLNL to review the CRADA tasks and objectives and to assess the progress to date on the CRADA effort.

V. The report "Argus Functional Description" was completed. This report will support both the CRADA and Standardization activities. It provides a high level overview of the Argus integrated security system with a listing and brief description of all functions.

TASK DESCRIPTIONS AND QUARTERLY PROGRESS

B&R No.	Funding	Obligated
GD 06 0201	$420,804	$459,100

I. Final FY94 CRADA Report Narrative:

The key to transferring Argus knowledge is the integration of the CRADA team members into the Argus development groups.
Since the beginning of MM's presence on site February 28, 1994, our joint strategy has been for LLNL to train the CRADA team members in the areas needed to become Argus developers and then cooperate in the development of commercial security related features to be added to the Argus integrated security system.

Areas of training include: learning the inner workings of the Argus system, Argus related applications of software design, configuration management, security related application programming and the development and testing process used at LLNL. Since there are no classes available to teach these subjects, and developing classes would be prohibitively expensive and resource intensive, it was decided to integrate the CRADA team members into the development teams as new Argus programmers and have them learn the system by taking on development tasks. Senior developers were made available to provide assignments of ever increasing complexity and to teach the CRADA team members aspects of the Argus system required to successfully complete their tasks. This is the same process which is used to train all new Argus programmers.

The milestones and deliverables of this years CRADA efforts have been met.
As shown in the status table at the end of the report, the first years CRADA deliverables have been met. The most important of which is the signing of the CRADA between Martin Marietta and Lawrence Livermore National Laboratory.

The second deliverable was the demonstration of a small Argus system. This task served the purpose of familiarizing the new CRADA members with the Argus hardware, documentation, software installation and setup, and operation. It also provided an opportunity for the development by LLNL programmers of a general purpose video driver which was used to operate the video section of the demonstration system.

A milestone program review was held on July 22, 1994 to review CRADA tasks and objectives, and to assess the progress to date on the CRADA effort.

The meeting was attended by LLNL Program Leader CK Chou and Martin Marietta Vice President of Government Systems Dick Costa.

The CRADA members have contributed to Argus development tasks.
The main contributions of the MM team have been

1) The integration of a low cost commercial magnetic stripe reader into the Argus intrusion detection system. This device is targeted for applications where reduced security and functional requirements exist which allow a more cost effective entry control device to be used in place of the LLNL Remote Access Panel (RAP).

2) The conversion of some access control database tables to Standard Query Language (SQL) from the proprietary Ingres database language EQUEL. This is in support of the conversion to open systems task of the CRADA.

3) The generation of test procedures for the Release 17 Access Control Software. A draft detailed test procedure for the access control subsystem was available for use during the pre-release 17 testing.

The Martin Marietta CRADA Team's training and skills was, and remains, a poor match to the Argus development tasks. This has resulted in a slow start in their effort to aid in the Argus development effort.
Argus development tasks are primarily software oriented and the five-person MM team has been struggling to understand the Argus software. Only one individual came with training in the Ada language and in VMS. Ada makes up the majority of the Argus code and VMS is the operating system on which the programs run. Two others have worked in the area of database management systems (DBMS), but had no training in Ingres, the DBMS which is used to manage configuration and personnel data within Argus. The remaining two individuals are system engineers with no plans be software developers.

The MM CRADA team also had little or no experience in physical protection systems which is the purpose of Argus. None would have qualified as Argus programmers had they interviewed for the job. After seven months at LLNL, a few members of the MM CRADA team have started to contribute to the Argus development effort, both in software development and system design areas. However, as a whole, the MM team is mismatched to the task.

LLNL has expended significant effort in training the MM CRADA team in basic skills.
The CRADA team has attended Ada classes which is a prerequisite to developing the skills required for the job. However, considerably more time than expected has been spent by the LLNL Argus team in training the CRADA team members in the basic skills required by an entry-level Argus programmer. Argus high-level developers were required to instruct the CRADA team in beginning programming skills needed to accomplish the most basic Argus programming tasks. In at least one case, the individual was still unable to accomplish a simple programming task.

Performance of the MM CRADA team in programming deliverables has been poor.
Of the three CRADA members who are attempting programming tasks, two are operating on a low level requiring considerable instruction and direction and performing poorly, although one is delivering a usable software product. The third programmer is progressing well towards becoming a productive Argus development team member. This one is the source of the single significant technical software contribution to the Argus system by the CRADA programming team, the low-cost magnetic stripe card reader integration package.

Performance of the MM CRADA team has been good on administrative and configuration work.
While the plans to integrate the MM CRADA members into the Argus development team have not yet been successful, their training in Argus configuration and setup has met with success. While the set-up of the Argus Demonstration system for the ASIS show involved no significant development contribution from the MM CRADA team, it did require them to learn the basic elements of installing and configuring a subset of an Argus system. This included map and video system setup, Intrusion Detection and Access Control and enrollment system configuration, and central system installation and set up. These activities involved close interaction with the Argus development team and were similar to training that is provided to new Argus system users. Members of the team have also been successful in documenting aspects of Argus and in test plan generation.

The ability of this MM CRADA team to co-develop with LLNL on the Argus system is doubtful.
Due to their lack of basic programming skills and training, the MM CRADA team's ability to take on Argus development tasks has been minimal. Our initial expectations to fully integrate the CRADA members into the Argus development team are currently not being met. It is doubtful that the existing

MM CRADA team will be able to meet the developmental milestones scheduled for the coming Fiscal Year.

We have communicated this concern to MM management.
These concerns have been communicated in meetings and discussions with all levels of MM management up to Vice President. We believe that some changes are being made, but we have not been informed of the extent. Communications in this area have been poor, but we are hopeful that they are beginning to improve due to a series of recent calls and meetings between Program Leader CK Chou and Associate Program Leader Greg Suski with MM Vice President Dick Costa.

Argus Standardization effort
The Argus Functional Description UCRL-TB-118718 document has been generated and published. This document describes in some detail the high level operation of the Argus Integrated security system. It is being provided to both Sandia and to Ron E. Timm and Associates in support of their efforts to evaluate and develop Electronic Physical Protection System standards.

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
8/1/94	A prototype single small computer Argus Host with Access Control, Intrusion Detection, and Console operational capability will be demonstrated at DOE HQ or Livermore	Completed & demonstrated to Pocratsky & Toms
9/31/94	Argus Functional Overview document.	Completed
09/30/94	Final report on Electronic Security System standardization and on CRADA activities will be submitted.	Status reports have been provided

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

Argus Functional Description UCRL TB-118718

DOE Automated Visitor Access Control System
Greg Davis, 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. Biometrics
- CVCS query screen modification - Completed
- DISS modifications - Completed
- Enrollment, verification, and update features - Completed
- DAVACS Biometrics procedures - Completed

II. Encryption
- Canceled - Report completed

III. CVCS Clearance Query Screen
- Additional data fields for screen enhancement - Completed

IV. Streamlining the Weapons Program Need-to-Know Access Requirements
- An agreement has been reached to allow the continued use of DAVACS for visits within the weapons complex requiring access to weapons data

TASK DESCRIPTIONS AND QUARTERLY PROGRESS

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

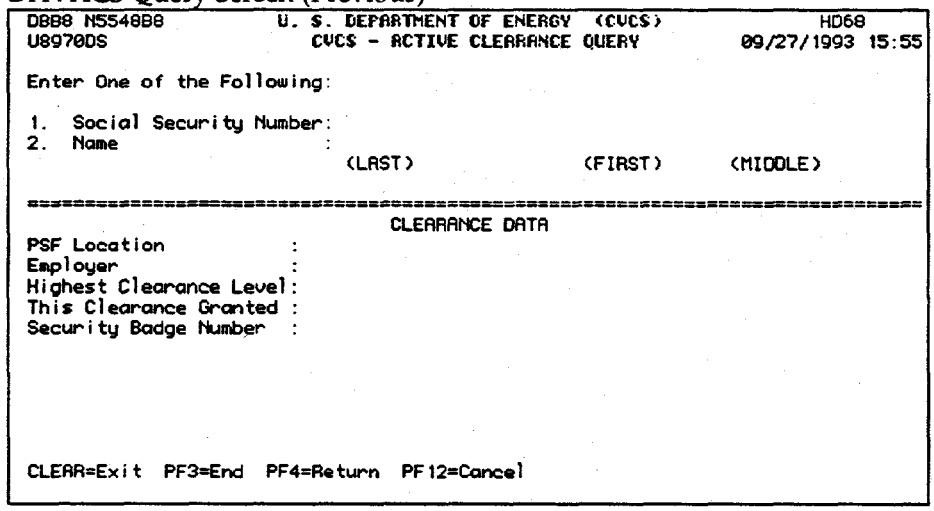
B&R No.	Funding	Obligated
GD 06 0201	439K	350K

I. Classified Visit Procedures Improvement - Clearance Query Screen Enhancements

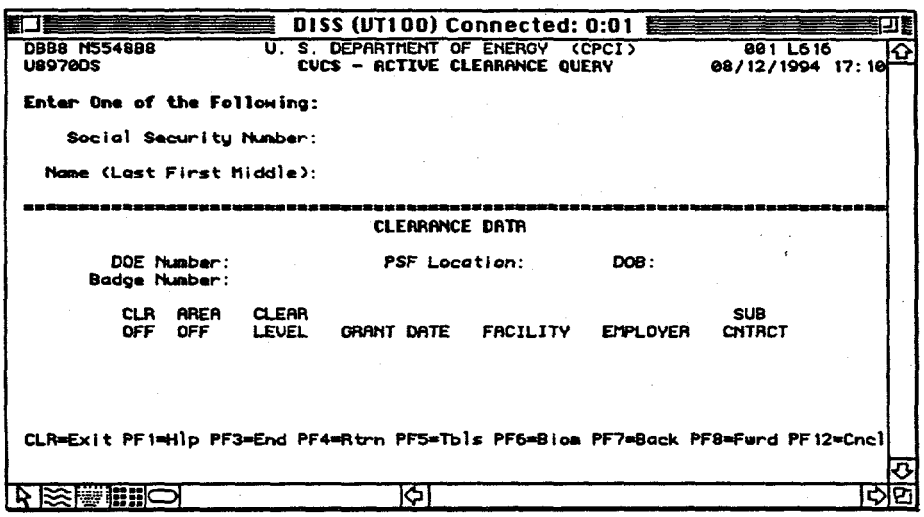
It was determined during the DAVACS testing period that additional data fields would be required on the Clearance Query screen. Additional data will allow facilities to make a more informed decision regarding requests for classified visits.

- Survey forms were distributed to all facilities within the DOE complex requesting input for the additional fields.
- Survey results identified the need for multiple clearance information including all active clearances, grant dates, and clearance numbers.
- Clearance Query screen was redesigned to accommodate the additional fields requested. The new screen was put into production on June 23, 1994 and is currently on-line.
- Screen now includes the capability of viewing the DOE number, all active clearances that are held by the visitor, the Operations and/or Area offices which hold those clearances, grant dates, as well as the visitor's facility and employer codes.

DAVACS Query Screen (Previous)



DAVACS Query Screen (Revised)



II. 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.

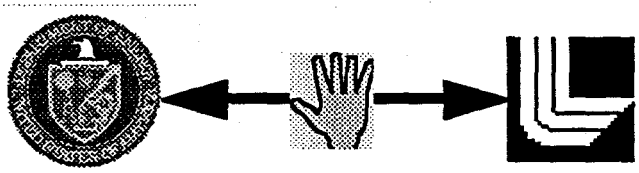
- Glen Tayler, DP-312, agreed to allow the continued use of DAVACS for visits within the weapons complex that require access to weapons data. Glen has suggested addition fields within the DISS system to allow field offices to limit specific individual's access.

- Updated project proposal to re-engineer the Weapons Data Access Control System (WDACS), July 1994.

- Working with Glen Tayler, DP-312, to draft the Weapons Data Guidance Memorandum.

- This will allow "L" Access to CRD, SFRD, and CFRD weapons data.

III. Visitor Biometrics Verification



Visitor biometrics verification required the extension of the DISS computer system to accept biometrics data supplied by field offices and sites; the development of a

workable and practical biometrics verification system suitable for installation in visitor control centers; and the implementation of policies and procedures which allow day-to-day use of the system.

Changes to the CICS test region (CICSTEST), of the DISS computer system , were completed on June 23, 1994. These changes allow updating of biometrics templates within the system. With the proper authorization in a users log-on profile, enrollment and updating of the biometrics template can now be accomplished. Driver software to automatically update the biometrics template will be completed promptly.

Additional routines to handle user interfaces and errors have been developed. These additional routines provide users of the biometrics enrollment system an automated procedure for enrollment and verification of successful enrollment as well as supplying enhanced feedback.

DAVACS operational procedures, including biometrics enrollment and verification, has been completed.

Requirements for the installation, location, and authorized users were requested in preparation for the installation of a biometrics station at DOE/HQ.

IV. DISS Communication Security Analysis

This task has been canceled as per direction from Darryl Toms. A Draft report was completed and delivered.

APPENDIX A, A SUMMARY OF ALL MILESTONES AND DELIVERABLES

MILESTONES STATUS TABLE

Original Milestone	Description of Milestone	Status
01/01/94	Classified Visit Procedures Improvement - Document additional data field requirements of DISS/CVCS Query screen; draft report to DOE HQ for review and concurrence	Completed
01/15/94	Classified Visit Procedures Improvement - Identification of DISS/CVCS data fields for file transfer to DOE sites	Canceled - DISS ET, CPCI Project
03/01/94	Classified Visit Procedures Improvement - Implement the CVCS Query screen with additional data field to the DISS production system	Completed
03/01/94	Classified Visit Procedures Improvement - Implement DISS/CVCS data fields into production system for file transfer to DOE sites	Completed
03/01/94	DISS Communications Security Analysis - Begin encryption test	Canceled
03/15/94	Classified Visit Procedures Improvement - Begin testing by LLNL of DISS/CVCS data fields for file transfer for DAVACS back-up and cancellation of active visits based on terminated clearances	Canceled
04/01/94	Visitor Biometric Verification - Completion of Macintosh based biometrics verification station	Completed
05/15/94	Classified Visit Procedures Improvement - Complete testing by LLNL of DISS/CVCS data fields for file transfer for DAVACS back-up and cancellation of active visits based on terminated clearances	Canceled
07/1/94	Visitor Biometric Verification - Completion of DISS modifications to support biometric verification of visitors	Completed

07/15/94	Classified Visit Procedures Improvement - Document procedure to handle terminated clearances on a timely basis. Complete draft of procedures for DOE implementation and forward to DOE HQ for review and concurrence	**Canceled - DISS ET, CPCI Project**
9/30/94	Visitor Biometric Verification - Operational plan for biometrics verification of visitors complex-wide	**Completed**

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

None