**Lawrence Livermore National Laboratory
Safeguards and Security Quarterly Progress Report
to the Department of Energy
Office of Safeguards and Security**

**Wayne D. Ruhter
Rokaya Al-Ayat
Charles E. Cole
L. L. Thomas**

Quarter Ending December 31, 1990

This is an informal report intended primarily for internal or limited external distribution. The opinions and conclusions stated are those of the author and may or may not be those of the Laboratory.
Work performed under the auspices of the U.S. Department of Energy by the Lawrence Livermore National Laboratory under Contract W-7405-Eng-48.

RECEIVED by US

FEB 19 1991

Table of Contents

Preface	LLNL-i
Safeguards Technology Program	STP-1
Introduction	STP-2
Funding.....	STP-2
I. Science and Technology Base Development	STP-2
• Intelligent Actinide Analysis System	STP-3
• Deterioration of Pu Isotopic Analysis with Neutron Damage to HPGe Detectors.....	STP-5
II. Onsite Test and Evaluation and Facility Support	STP-6
• Isotopic Analysis of Plutonium Samples Enriched in ^{238}Pu	STP-6
• Actinide Isotopic Analysis System for Los Alamos Plutonium-Handling Facility	STP-7
III. International Safeguards.....	STP-10
• MGA Workshop	STP-10
• Transportable X-Ray Fluorescence Analysis System.....	STP-10
Safeguards Systems Studies	SSS-1
Introduction	SSS-2
Funding.....	SSS-2
I. Safeguards Systems.....	SSS-3
Safeguards and Security (ASSESS)	SSS-3
• Developing Models and Software for Dealing with Active Violent Insiders	SSS-4
• Material Control and Accountability Order 5633.3 Requirements.....	SSS-6
• Evaluate the Effectiveness of the Personnel Security Assurance Program (PSAP)	SSS-6
II. Resolution of Nuclear Material Anomalies: Inventory Difference Anomaly Resolution Team.....	SSS-6

MASTER

DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED

III. Quality Improvement of Protection Planning: Support for the Development of the MSSA Verification Guide.....	SSS-8
Conferences, Papers, Reports, and Miscellaneous.....	SSS-8
Computer Security Studies	CSS-1
Introduction.....	CSS-2
Funding.....	CSS-2
I. Research Projects in Collaboration with UC-Davis.....	CSS-3
II. System Security Maintenance Software.....	CSS-3
III. Distributed Audit Standards and Requirements.....	CSS-4
AVLIS Safeguards RD&D	LIS-1
Introduction.....	LIS-2
Funding.....	LIS-2
I. Revise the Long-Range AVLIS Safeguards RD&D Plan to reflect current AVLIS deployment schedule.....	LIS-2
II. In conjunction with DOE/OSS, coordinate a meeting of the Enrichment Program Safeguards Review Group (EPSRG)	LIS-2

Preface

The Lawrence Livermore National Laboratory (LLNL) carries out safeguards and security 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 1991 (October through December, 1990).

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 four areas:

- Safeguards Technology
- Safeguard System Studies
- Computer Security
- AVLIS Safeguards

The remainder of this report describes the activities in each of these four areas. The information provided includes an introduction which briefly describes the activity, funding information, and the activity task descriptions and summary of accomplishments.

The LLNL welcomes the opportunity to apply its expertise in these technical areas. Although the aggregate of activities for OSS is modest, the 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, FTS: 532-4951, or one of the program managers for the four technical areas.

Safeguards

Technology

Program

(STP)

**Quarterly Progress Report
to the DOE Office of
Safeguards and Security**

Quarter Ending December 31, 1990

Wayne D. Ruhter, Program Manager
Nuclear Chemistry Division

January 1991

STP-1

Safeguards Technology Program

Wayne D. Ruhter, Program Manager
Nuclear Chemistry Division

INTRODUCTION

The Safeguards Technology Program (STP) at Livermore supports the Technology Development Program of the Office of Safeguards and Security (OSS) in three subprogram areas (tasks):

I. Science and Technology Base Development

- Intelligent Actinide Analysis System
- Deterioration of Pu Isotopic Analysis with Neutron Damage to HPGe Detectors

II. Onsite Test and Evaluation and Facility Support

- Isotopic Analysis of Plutonium Samples Enriched in ^{238}Pu
- Actinide Isotopic Analysis System for Los Alamos Plutonium-Handling Facility

III. International Safeguards

- MGA Workshop
- Transportable X-Ray Fluorescence Analysis System

FUNDING

The STP funding levels for FY91 are:

	<u>B&R No.</u>	<u>Amount</u>
I. Science and Technology Base Development	GD-06-01	\$350K
II. Onsite Test and Evaluation and Facility Support	GD-06-03	\$100K
III. International Safeguards	GD-06-04	<u>\$105K</u>
		Total \$555K

TASK DESCRIPTION AND SUMMARY OF ACCOMPLISHMENTS

The projects being worked on during FY91 under each of these tasks are described in the following report on FY91 first quarter progress.

I. Science and Technology Base Development

The overall project objective for this task is to research and develop state-of-the-art NDA instruments, methods, and techniques that address top priority MC&A problems; and that will result in improved MC&A of SNM at DOE facilities. A brief description of each activity under this task and the progress made on each during the past quarter is given below.

Intelligent Actinide Analysis System

William M. Buckley, Zachary M. Koenig and Wayne D. Ruhter

We have begun development of the Intelligent Actinide Analysis System (IAAS). This system represents a step forward in gamma-ray spectrometry, nondestructive assay systems for Safeguards in the areas of automation and ease of use. The prototype system will be delivered to Materials Management at LLNL, which has agreed to pay for the hardware, documentation, and training costs. We have conducted several meetings with Materials Management to determine requirements, design goals, and a basic architecture for this system. 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 customer requirements or technological extensions to the base instrument design.

We have chosen a distributed architecture for the IAAS. The functions of data collection, motor and shutter control, sensor monitoring and data analysis can take place on different computers on the instrument network shown in Fig. 1. With this approach, all of the real-time functions will be handled on inexpensive single-user platforms (PC compatible), using inexpensive commercially available software or software libraries. Using PCs for data collection and instrument control, we will be able to purchase more software rather than having to develop it and the instrument-control software we do develop should be simpler and less expensive than if we performed these functions on a minicomputer or workstation. Using PCs for direct instrument control will allow us more flexibility in how the instrument functions are automated than the current approach of custom-built control boxes. Coordination and monitoring of these functions and analysis of the data will be performed on a multi-tasking computer workstation with a windowing, graphical, user interface that provides the operator or scientist with a wide range in flexibility of the instrument display.

Deterioration of Pu Isotopic Analysis with Neutron Damage to HPGe Detectors, Zachary M. Koenig, Raymond Gunnink, Wayne D. Ruhter, and David C. Camp

Determination of plutonium (Pu) isotopics is important in safeguards applications for shipper/receiver inventory and material control and accountability (MC&A) measurements. Frequently, isotopic results are obtained from high-quality gamma-ray spectra taken with high-purity germanium (HPGe) detectors. Small variations in energy resolution or peak shape may have large effects on the determination of the relative isotopic abundances depending on the analysis code used. Poor quality spectra result from numerous factors including incorrect pole-zero adjustment, excessive count rates, pulse pile up, electronic noise, and radiation damage from neutrons.

An n-type coaxial (20% rel. efficiency, 50mm dia. x 51mm) and a p-type low-energy photon spectrometer (LEPS) HPGe planar detector (16mm dia. x 13mm) were exposed to a total integrated dose of 5×10^9 neutrons/cm² from a 2 microgram ²⁵²Cf neutron source. At intervals of successively increasing integrated neutron flux exposures, spectra from both detectors were analyzed for energy resolution and peak shape parameters using ¹³³Ba and weapons grade Pu, as well as ²⁴¹Am and ⁵⁷Co for the LEPS detector and ⁶⁰Co for the COAX detector. Pu spectra were analyzed by MGA to monitor deterioration in the code's isotopic analysis capability.

Neutron damage to the LEPS detector began to affect MGA's results at 4×10^9 neutrons/cm² and MGA was unable to analyze the Pu spectrum at 5×10^9 neutrons/cm²; whereas the COAX detector spectrum was no longer analyzable above an exposure level of 5×10^8 neutrons/cm². The results from MGA of neutron damage to a HPGe detector used for Pu isotopic measurement are summarized as a function of Pu isotope uncertainties shown in Table 1. These data indicate how well MGA can continue to analyze spectra until the code simply fails.

In the past quarter, we annealed the two detectors and compared both detector's performance to their original specifications. There was a problem in the recovery of the LEPS detector and it has been returned to ORTEC for repair. Once the LEPS detector is returned to LLNL, we plan to expose both HPGe detectors again to successively increasing neutron flux to determine if minor amounts of additional neutron shielding (phase two) modify the unshielded detector results. During the past quarter, we received an electrically-cooled cryostat and have begun initial tests with it. In a third phase we will use the electrically-cooled cryostat to cool the HPGe detector to below 77° K to see what effect, if any, these measures have on prolonging the "life" of the detectors. An abstract based on this work was submitted to the 4th International Conference on Facility Operations - Safeguards Interface.

neutron flux (neutrons/cm ²)	---	3.7x10 ⁹	4.7x10 ⁹
Pu-238	1.7	3.9	All isotopic
239	0.3	0.5	components
240	0.4	0.8	unresolvable
241	0.25	0.5	at this exposure
QFIT	1.19	5.83	

Table 1. The Pu isotopic percent error and Q-fit from MGA at various neutron exposures.

II. DOE Sites Operational Support Activities

The primary objective of this task is to assist DOE sites in implementation of LLNL developed NDA technology. In particular, it is to assist in the implementation of STP designed/developed systems at Savannah River Plant's New Special Recovery (NSR), Receipts Assay Facility (RAF), and H-Canyon facilities; LLNL's Materials Management; LANL's TA-55 facility; and at Hanford's Pu-238 handling facility. A brief description of progress in activities under this task are given below. Most of the costs of the activities described below are borne by the facility for which the work is being done.

Isotopic Analysis of Plutonium Samples Enriched in ²³⁸Pu

Wayne D. Ruhter and David C. Camp

We have constructed a gamma-ray spectrometer system for Westinghouse Savannah River Company (WSRC) to measure the relative plutonium isotopic abundances in plutonium samples enriched in ²³⁸Pu. In December, we installed the system in WSRC's H-Canyon facility. This completed one of our milestones for our on-site support tasks. Once installed, we collected twenty-four spectra on nine different samples to test and evaluate the system. The samples ranged from 20% to 85% in ²³⁸Pu enrichment. A summary describing this project has been submitted for presentation at the Fourth International Conference on Facility Operations - Safeguards Interface.

In general, the results obtained on these samples were good. The accuracy obtained on the ²³⁸Pu abundance was on the order of $\pm 1.5\%$. There were two samples for which the results were not as good. We examined in great detail at Livermore the spectra from these two samples and found evidence that they contain the element fluorine that results in an interference in one of the gamma rays we measure, which biases the results. We modified our analysis methodology to eliminate the source of

bias and asked Savannah River to remeasure these samples to confirm the presence of fluorine.

A similar system is being built for Westinghouse Hanford Company (WHC). Their system is to be installed in WHC's Radioisotope Power Systems Facility (RPSF) for nondestructive assay of iridium-clad PuO_2 fuel pellets enriched in ^{238}Pu , known as fuel clads, in conjunction with calorimetry. On October 1, Wayne Ruhter participated in the 80% design review of the system at Hanford. The design was approved and a contract has been awarded for construction of the sample enclosure/detector shield hardware. The hardware is planned for delivery by mid-March and will cost \$73,000. This is approximately 50% greater than our original estimate; due primarily to changing regulations and additional requirements. It is an indication of the problems we face in estimating costs for fixed-price contracts. All of the electronic hardware has been delivered and will be tested.

Actinide Isotopic Analysis System for Los Alamos Plutonium-Handling Facility *Zachary M. Koenig, William M. Buckley, Raymond Gunnink, and Wayne D. Ruhter*

The inventory measurement of a sample's total plutonium and other actinides content is determined by two nondestructive measurements. One is a calorimetry measurement of the sample's heat or power output, and the other is a gamma-ray spectrometry measurement of its relative isotopic abundances. The isotopic measurements needed to interpret the observed calorimetric power measurement are the relative abundances of various plutonium and uranium isotopes and americium-241. The Los Alamos actinide analysis system carries out these gamma-ray measurements.

In the past quarter, the instrument was completed, tested, and delivered to the TA-55 Nuclear Material Storage Facility (PF-41) at Los Alamos National Laboratory. Long- and short-term stability tests were completed on two Pu standards. The results of the long- and short-term precision measurements are plotted in Figs. 2 and 3, respectively. The solid line in the plots indicates the reference value of the standard. The dashed lines indicate the $\pm 0.5\%$ variation from the reference standard value. The precisions of both the long- and short-term measurements were well within $\pm 0.5\%$. Also included with the plots are the mean, standard deviation, and chi-squared values. The two Pu standards, STDISO6 and STDISO12, 6 and 12% Pu-240 samples, are both well characterized standards and are available to LANL for comparison. Tests with a Pu sample off-center (from the sample platform) and with a high gamma-ray background (200 grams Pu-238) were completed and shown not to affect the results of the system.

The actinide analysis system was delivered to LANL in December and a 2-day training course was taught to the operational personnel that covered both hardware and software operation of the instrument. In addition, a user manual was written for the instrument that included system settings and operation, operator interface and procedures, output formats, and error messages. A paper describing this work was submitted to the 1991 INMM meeting.

Figure 2. Fifteen consecutive short-term precision measurements with 6 and 12% Pu-240 standards.

Figure 3. Three week long-term precision measurement with 6 and 12% Pu-240 standards.

III. International Safeguards R&D

The objective of this task is to assist international safeguards authorities (Euratom, IAEA, etc.) in implementing LLNL-developed NDA techniques for the MC&A of SNM and to develop instrumentation and procedures for international safeguards as required.

During the past year we have been working with Euratom in the implementation of the MGA code for inspector use and the development of a transportable x-ray fluorescence analysis instrument.

MGA Workshop

Raymond Gunnink and Wayne D. Ruhter

Drs. Ray Gunnink and Wayne Ruhter visited five European facilities during a three week trip that began on October 6, 1990. Our first visit was to the IAEA where the principal purpose was to describe the MGA plutonium gamma-ray isotopic analysis code and conduct hands-on workshops for IAEA inspectors and other staff members. About thirty-two IAEA personnel attended the seminars where the algorithms and methods used in MGA were explained and where the instrument and measurement setups were described. Following the seminars, hands-on training sessions were conducted for two different groups of thirteen inspectors.

A second purpose of our visit to the IAEA was to obtain information to develop system requirements and a work plan for our new ISPO A.153.8 task. Upon our return, we prepared a draft of the system requirements and task work plan, and sent it to our technical contact at the Safeguards Analytical Laboratory. He has reviewed and made minor changes in our draft, and has submitted it to the IAEA's Support Program Administration for their approval.

We next visited the JRC laboratory at Ispra, Italy where we also conducted a three day workshop of seminars and hands-on exercises. This workshop was attended by 39 participants. About 9 were Euratom inspectors and the remaining participants came from various European nuclear facilities, laboratories, and commercial companies. This accomplished our first milestone for FY91 under this task. During this workshop we received requests from representatives of BNFL and Cogema for copies of the MGA code, which we have given them for test and evaluation purposes.

We were very gratified by the level of interest and participation shown at our workshops, and received many positive responses that indicated they were very useful. The experience also gave us a much better appreciation of various measurement problems that are prevalent in the field. For example, we encountered several equipment problems which generally produced erroneous answers. As a result of these experiences, we are now incorporating new logic into the MGA program to warn the user of serious hardware conditions, or where possible, automatically correct the results when these conditions occur.

One equipment problem that gives rise to erroneous results is nonlinearity in the pulse-processing electronics of the gamma-ray measurement system. This means that the value for the gain varies from one region of the spectrum to another and that calculating the positions of peaks in the spectrum can be inaccurate. We have worked on this problem, during the past quarter, and are testing a modification to the code to allow for this problem in the electronics.

We next paid a one-day visit to the Cadarache Nuclear Research Center in France. The purpose of this visit was to discuss methods for calculating plutonium isotopic abundance ratios as a function of reactor burnup and other parameters. They offered to generate a set of isotopic abundance tables for us using a mutually agreed upon set of parameters.

Our fourth stop was at the Siemens MOX fuel facility near Hanau, Germany. A number of measurement problems were discussed with facility staff members. However, the principal purpose of the visit was to meet with members from IAEA and Euratom to discuss and come to closure on the specifications for two neutron coincidence/gamma-ray measurement stations that will be installed at the new MOX facility being built by Siemens. These stations will require state-of-the-art technology and highly optimized measurement parameters to meet the accuracy and precision that is desired. Because our MGA code will be used to interpret the gamma ray spectra, we were able to provide valuable input to the measurement and equipment specifications.

We also spent some time with Siemens personnel discussing their use of the MGA code. They have obtained the VAX version of the MGA code from the Argonne National Energy Software Center (NESC) and have installed it on a MicroVAX in their facility. We tested the code to ensure that it had been installed properly and made some modifications to the code to simplify its use with their spectral data format. This accomplished another milestone for our international safeguards task.

Our final stop was at the Atomic Weapons Establishment (AWE) in Great Britain where we had been invited to give an "in-depth teach-in" on the use of the MGA code to various users at this laboratory. This activity is covered by the charter of SUBWOG 30F related to exchange of information on instrumentation applied to the measurement of radioactive materials.

We came home exhausted, but with a feeling that we had accomplished all of our principal objectives; and, as a result of the trip, obtained many new insights and ideas on how we can improve the accuracy and reliability of our codes and measurement methods.

Transportable X-Ray Fluorescence Analysis System

Wayne D. Ruhter

The Safeguards Technology Program has been developing a transportable x-ray fluorescence analysis (XRFA) system for international safeguards authorities [EURATOM Safeguards Directorate (ESD) and the International Atomic Energy Authority (IAEA)] to measure uranium and plutonium concentrations in solutions. A

transportable XRFA system would enable their inspectors to perform in-situ measurements on plutonium- and uranium-nitrate solutions and thus avoid shipping samples back to their laboratories for analysis.

While in Europe, we discussed with Dr. Hans Wagner, with the Euratom Safeguards Directorate, his experience with a system we loaned Euratom for evaluation. In August, Dr. Wagner used the system at LaHague in France to measure uranium concentrations in nitric acid solutions. We discussed with Dr. Wagner several of his suggestions for improving the system, their requirements for a new system, and its costs. Dr. Wagner indicated again that Euratom is interested in purchasing a system from LLNL. ***We would appreciate assistance from DOE/OSS in making the arrangements for such a purchase.*** Upon our return to Livermore, we made several of the changes suggested by Dr. Wagner to the system we have at Livermore and are awaiting further word from Euratom regarding the purchase of such a system.

Safeguards

Systems

Studies

(SSS)

**Quarterly Progress Report
to the DOE Office of
Safeguards and Security**

Quarter Ending December 31, 1990

**Rokaya Al-Ayat, Associate Program Leader
Nuclear Systems Safety (NSS)/Safeguards Program**

January 1991

SSS-1

Safeguards Systems Studies

Rokaya Al-Ayat, Associate Program Leader
Nuclear Systems Safety (NSS)/Safeguards Program

INTRODUCTION

The overall goal of this program is to provide state-of-the-art analytic tools for evaluating the effectiveness of safeguards and security systems. These tools facilitate examining safeguards systems effectiveness against a broad spectrum of threats. Our efforts include the following activities:

I. Safeguards Systems Studies

- ASSESS software conversion and enhancements.
- Conducting courses on the use of various analytical techniques, models, and computer systems related to safeguards and security (S&S).
- Developing models and software for evaluating the effectiveness of safeguards against the threat of a single violent insider.
- Developing approaches for meeting material control and accountability Order 5633.3 requirements.
- Evaluating the effectiveness of the Personnel Security Assurance Program.

II. Resolution of Nuclear Materials Anomalies

- Techniques for analyzing anomalies indicating that nuclear material may be missing.
- Support of the DOE Inventory Difference Anomaly Resolution Teams (IDART).

III. Quality Improvement of Protection Planning

- Supporting the development of the Master Safeguards and Security Agreement (MSSA) verification guide.

FUNDING

Funding for these activities come from the following sources:

<u>Project Title</u>	<u>B&R No.</u>	<u>\$K Amount</u>
Technology and Systems Developments– Basic Systems Design, Integration and Evaluation: Safeguards & Systems Studies	GD0602	760

<u>Project Title</u>	<u>B&R No.</u>	<u>\$K Amount</u>
Technology and Systems Development– Basic Systems Design, Integration and Evaluation: Resolution of Nuclear Materials Anomalies	GD0602	169
Operational Support Activities– Additional Support	GD0508	150

TASK DESCRIPTION AND SUMMARY OF ACCOMPLISHMENTS

What follows, is a summary of work performed during the first quarter of FY91 in support of the above projects.

I. Safeguards Systems Studies

A. Analytic System and Software for Evaluating Safeguards and Security (ASSESS)

1. ASSESS Code Conversion and Enhancements

Microsoft has recently released a new Windows version 3.0 with greatly enhanced capabilities. The current version of ASSESS operates under Windows 286 version 2.1, and is being converted to run under the new Windows 3.0. When converted, ASSESS will have improved reliability, in large part due to the enhanced ability to use additional memory. Bugs that have been showing up in earlier versions of ASSESS will be corrected. In addition, most modules of ASSESS will have an improved interface that is compatible with Windows 3.0 styles, and new features will be added. The new features include:

- Importing Insider definition data and "user-defined information" from existing Insider files to new evaluation files associated with alternate Facility Description files.
- Moving table information into a word processor or spreadsheet program from Insider and Hand-off Collusion.
- Having the ability to choose and print the appropriate classification markings on printouts from the Insider and Hand-off Collusion modules.
- Providing more complete "Help" screens for the ASSESS Manager, Insider and Hand-off Collusion modules.

The Windows 3.0 version of ASSESS is currently undergoing beta-testing and debugging, and so far seems very reliable. Files created under previous versions of ASSESS are upwardly compatible. The new version of ASSESS will be released to the users at the next workshop planned for February, 1991.

2. ASSESS Course Schedule for FY 1991

We are in the process of developing a two-week ASSESS course to be taught at the Central Training Academy beginning in January, 1991. Unlike the one-week ASSESS course taught previously, the two-week course will have no prerequisites. We are planning a more comprehensive workshop than the one-week predecessor: in addition to the ASSESS code, it will cover the development of a Site Safeguards and Security Plan (SSSP)—especially the role of vulnerability assessments in producing Volume I, the Master Safeguards and Security Agreement (MSSA). The new workshop will present the philosophy and process of completing vulnerability analyses in support of MSSAs, including scoping the threats and targets to be addressed, structuring the analysis teams, evaluating safeguards, performance-testing, and identifying and analyzing the effectiveness of potential upgrades.

B. Developing Models and Software for Dealing with Active Violent Insiders

We are tasked with developing models and software for evaluating the effectiveness of safeguards against the threat of a single violent insider. Prior to this fiscal year, we presented a broad framework for dealing with active insiders. This framework divided the insider threat into categories according to action (passive vs. active), willingness to use violence, willingness to be detected, and decision process.

During this quarter our work on the violent insider focused on these tasks: developing "key" violent insider scenarios; database development; algorithm development for contraband entry; and algorithm development for timelines, interruption, and neutralization. We discuss each of these in more detail below.

1. Sample Violent Insider Scenarios

We have developed a few "key" violent insider scenarios which will be our initial focus in developing the algorithms and databases. The idea behind developing these scenarios is to ensure that the algorithms and database accommodate the key situations of interest and do not become unduly complicated by emphasizing less important scenarios. We plan to expand these scenarios by adding details down to the safeguards component level as an aid in the development of the databases and algorithms.

2. Database Development

We have outlined relevant factors for the defeat of safeguards components using force or violence. These factors include, whether the act is feasible by a single individual; the type of tools, equipment, or explosives required; the task

time; and the evidence created (noise, smoke, rubble). We are ready to work with Sandia National Laboratories to explicitly consider these factors for a wide range of forceful and violent acts.

We have also been working on a scheme to incorporate relevant factors such as those listed above into a format consistent with the current Insider module database. Specifically, we are working on ways to account for temporal aspects of defeating safeguards, such as long task times, residual evidence, and the fact that if a wall is blown up on the way in, it is still blown up on the way out. As the "key" scenarios are defined in more detail, we will select a database implementation approach that behaves best with the "key" scenarios.

3. Contraband Entry

A violent insider may require contraband in order to complete the theft of SNM. Accordingly, the violent insider software must contain algorithms that reflect the difficulty of smuggling in the required contraband. We have identified categories of contraband. These include handguns, explosives, tools, vehicles, and shielding materials. We have enumerated desirable properties that the contraband entry algorithm would have, and have explored possible algorithms which satisfy some of the properties. As the "key" scenarios are developed further, we will make a final decision on a contraband entry algorithm, and for the time being we are making the assumption that an insider will be able to acquire onsite or smuggle in any needed contraband.

4. The Role of Timelines, Interruption, and Neutralization

For the nonviolent insider, it is assumed that the theft attempt may take place over a large amount of time. In addition, interruption and neutralization are not considered to be important since the nonviolent insider is assumed to not be willing to kill or be killed. These assumptions do not hold for the violent insider, and algorithms must be developed which consider the full range of violent insider acts.

Neutralization in ASSESS is defined as the battle or engagement between the response force and the adversary force. For a single violent insider, the adversary force is only one person, and hence, if a battle were to occur, the insider would certainly lose. The real question is whether the facility will have ample time to "interrupt" the insider to ensure that the battle would indeed occur. To account for this, we need to model factors not modeled currently in ASSESS such as the interplay of detection, assessment, identification, and interruption. The approach we are leaning towards is to use a variant of the multilayer strategy construct in the Insider module. Multilayer strategies are useful to model theft strategies which span several layers, such as evacuations and exploiting weaknesses in transfer procedures.

5. Software Development Considerations

For purpose of code development, we have decided to develop the violent insider software as a separate "module" of ASSESS. A separate module is

necessary because we need the flexibility to try various algorithms and database approaches without being tied to the current Insider module structure. This separate module will, by necessity, contain much of the logic and algorithms of the current Insider module, and after development, it may be more natural to combine the Insider and Violent Insider modules.

6. Work for Coming Quarters

We plan to finalize work on the algorithms during this next quarter. The following quarter we plan to complete database elements, including defeat methods, strategies, and data sources. At the end of FY91, we plan to deliver preliminary software for the violent insider. This software will be ready for field testing.

C. Material Control and Accountability Order 5633.3 Requirements

Two meetings were held this quarter and guidance was received concerning the scope and priorities for developing approaches for meeting MC&A Order 5633.3 requirements. Two areas have been identified as having the highest priority. These concern incorporating into ASSESS the ability to handle protracted and rollup attempts by a single nonviolent insider. Collusion of insiders is of lower priority. A memo has been prepared describing a possible approach that could be implemented this year. The content of this memo will be discussed at length with Dave Crawford and Ron Cherry at the upcoming program review in Livermore.

It was also agreed that close interaction with the Brookhaven National Laboratory personnel supporting the development of the MC&A guidance documentation is needed. Although no meeting has been scheduled, we hope to have one in the near future.

D. Evaluate the Effectiveness of the Personnel Security Assurance Program (PSAP)

A draft report entitled "A Model for Evaluating the Effectiveness of Personnel Security Assurance Programs" has been completed and is undergoing internal review. The approach described is ready to be demonstrated at an operating facility. Discussion is underway to identify a potential site.

II. Resolution of Nuclear Material Anomalies: Inventory Difference Anomaly Resolution Team

The mission of the Inventory Difference Anomaly Resolution Team (IDART) is to provide technical support to the DOE for resolving discrepancies that occur when accounting for special nuclear material. A discrepancy in SNM inventory could be attributable to a variety of causes: errors in bookkeeping or measurement, an accidental misdirection of material, or an actual diversion of material. It is important to

be able to quickly identify the most likely cause and provide assurance that a diversion of material has not occurred. The IDART project supports the DOE in resolving discrepancies in three ways: (1) establishment and maintenance of a special team from the DOE complex to assist facilities in resolving discrepancies, (2) development of analytical tools to for evaluating discrepancies, (3) recommending improvements to material control and accounting systems that can facilitate the resolution process.

1. IDART Software - During FY90 a menu driven spreadsheet based program that assists analysts in performing an anomaly resolution analysis was developed. During this quarter, refinements were made and testing was conducted to ensure that it is fully operational for both the Macintosh and IBM PC environments.

2. Anomaly Resolution Workshops - In November, we presented our third workshop on the analytical approach for resolving inventory discrepancies. Attendees included DOE personnel as well as several DOE contractors from operating facilities. Attendees learned a systematic approach for determining all possible causes for a discrepancy, identifying possible evidence, and combining observed evidence with prior knowledge to determine the most likely cause of the anomaly. Particular attention is given to sensitivity analysis and determining factors that have a significant effect on the analysis results. Attendees also get practice applying these techniques to the IDART computer software. After the workshop, we solicit student feedback and make improvements to the workshop in terms of both structure and content.

3. Improving Anomaly Resolution Capability - Experience in applying the anomaly resolution methodology has shown that evidence derived from the facility's Material Control and Accounting (MC&A) system can play a crucial role in quickly and accurately resolving an anomaly. The ability to definitively resolve an anomaly often depends on the types of measurement data available and on the way records of the various transactions that occur in a processing facility are maintained. We can facilitate the resolution of anomalies by incorporating properties into an MC&A system that can make tracing material flows and movements more precise and expedient. We are developing an analytical method for evaluating an MC&A system's capability with regards to anomaly resolution and for identifying improvements that will enhance resolution capability. The benefits with regard to the anomaly resolution process will be to help IDART make more definitive determinations. In addition, this analytical method will improve a facility's capability for internally resolving an anomaly and thereby reduce the number of incidents where IDART activation would be required.

During November and December, we began structuring an approach for doing formal evaluations of an MC&A systems anomaly resolution capability. The approach involves characterizing the different configurations of material in a process cycle including the legitimate material locations as well as possible unintentional locations. The methods for recording and/or measuring transitions between locations are also characterized. The analysis would then proceed to evaluate the interactions of the whole system to determine problem areas where the capability for resolving a discrepancy would be low. Enhancements to the MC&A system that will improve the resolution capability would then be suggested.

A white paper fully describing the approach will be presented during the second quarter. We also intend to test the methodology on an operating facility in the third quarter.

4. Projected Work

During the rest of the fiscal year, we will focus our effort on developing the analytical approach for evaluating MC&A systems anomaly resolution capability. We will also continue to be available for IDART activations and the annual meeting of the IDART core team will be scheduled. Another workshop on the analytical approach for evaluating anomalies will also be offered in May.

III. Quality Improvement of Protection Planning: Support for the Development of the MSSA Verification Guide

On September 6, 1990, we presented a progress report for our work on the Quality Control Program for the Site Safeguards and Security Plans (SSSP). We also submitted two draft reports describing the Review Process and Review Guide.

In October, we were requested to serve as Technical Reviewer in support of the DOE Master Safeguards and Security Agreements (MSSA) Review Guide Project. In this quarter, two review meetings were held at Meridian Offices in Germantown, on November 6, 1990 and December 27, 1990. Written comments were also provided. On December 18 we received the latest draft of the guide, which we are currently reviewing.

Conferences, Papers, Reports, and Miscellaneous

- A paper entitled "Using ASSESS to support an Upgrade" was prepared and presented at the American Nuclear Society 1990 Winter meeting held in Washington D.C. on November 11-15, 1990. The paper was co-authored with Mark Snell.
- A draft report entitled "Technical Documentation for the Insider Evaluation Module of ASSESS" has been completed. The report provides a technical description of how the Insider module of ASSESS works and includes two appendices. the first appendix provides a list of assumptions supporting the Insider module databases, and the second appendix provides a complete listing of the databases.
- A draft report entitled "A Model for Evaluating the Effectiveness of Personnel Security Assurance Programs" has been completed and is undergoing internal review. The approach described is ready to be demonstrated at an operating facility. Discussion is underway to identify a potential site.
- A program review was held on October 17, 1990 at HQ. Following the program review an extensive overview of ASSESS, including the

development history, was presented to selected members from OSS and their contractors.

- Several meetings and extensive discussions have been held with the Central Training Academy to agree on the scope, schedule, and funding for the upcoming ASSESS workshop.
- We plan to participate in the upcoming Insider Protection Workshop to be held at Sandia National Laboratory in early February, 1991. LLNL is responsible for a 4-hour block addressing Safeguards evaluation methodologies.
- A Vulnerability Analysis Newsletter was put together and mailed to those who attended previous TVATP and ASSESS workshops. The newsletter included discussion of new features of ASSESS and tips on printing and other important features for the use of the Windows 3.0 version. We've also mailed a survey with the newsletter asking for user's feedback. We plan to provide a summary of responses to the users and incorporate, to the extent possible, these comments in the development of ASSESS and the new workshop training program.

COMPUTER SECURITY
DISTRIBUTED SYSTEMS
(CSS)

**Quarterly Progress Report
to the DOE Office of
Safeguards and Security**

Quarter Ending December 31, 1990

Charles E. Cole, Program Manager
LLNL Computer Security Manager

January 1991

COMPUTER SECURITY

DISTRIBUTED SYSTEMS

Charles E. Cole, Program Manager
LLNL Computer Security Manager

INTRODUCTION

The overall goal of this program is to conduct research and development into network security monitoring, computer virus and malicious code defensive mechanisms, system security maintenance software, distributed audit standards and requirements, a vulnerability reporting program, and system integrity concepts. In addition, the program continues to provide DOE and it's contractor community with computer security incident response through support of the Computer Incident Advisory Capability (CIAC).

I. Research Projects in Collaboration with U.C. Davis

- Network Security Monitor
- Virus and Malicious Code Research

II. System Security Maintenance Software

- SPI/VMS
- SPI/UNIX

III. Distributed Audit Standards and Requirements

- Defining standards for heterogeneous audit trails

IV. Computer Incident Advisory Capability (CIAC)

- Providing reactive and proactive computer incident response to DOE and it's Contractors

FUNDING

Funding is provided through B&R GD0601. The Defense Programs funding level for FY 1991 is \$775K. CIAC is also funded through Administration and Energy Research within DOE. The research program also receives funding from other federal agencies to expand the scope of work. DOE benefits directly from these collaborations through expanded products and shortened delivery times.

TASK DESCRIPTION AND SUMMARY OF ACCOMPLISHMENTS

The following is a summary of work performed during the first quarter of FY 1991 in support of this project.

I. Research Projects in Collaboration with U.C. Davis

- Network Security Monitor (NSM)

Efforts continue on development of version 0.2 of the NSM. This is approximately 80% complete with an expected release by January 31, 1991. The new version includes menus for ease of use, output files which can be processed by standard flat file databases, complete automation, and remote configurability. The NSM now has the capability to print troff reports at three levels of granularity: network overview, detailed summary, and transcript report. Also developed during the reporting period was a presentation style termed "playback". In this style a connection to the network is played directly to the screen exactly as the person being monitored would see it.

The NSM was partially installed on a system on the OutNet at LLNL. This test illustrated some minor differences between the LLNL network configuration and the one at U.C. Davis where development occurred. Minor modifications were installed and the monitor was successful in tracking security events of interest at LLNL. The research team continues to capture and analyze verified intrusions at both LLNL and U.C. Davis. Two papers have been completed and submitted to the upcoming DOE Computer Security Group Conference.

- Virus and Malicious Code Research

This effort is targeting the virus filter tool to a PC environment since there are many more PC viruses than UNIX viruses, and more binary viruses than source code viruses.

The team is also working on static analysis techniques to intelligently disassemble/decompile a binary program. The goal of this effort is to reconstruct enough of the data definition structure to allow the data flow analyzer and slicer to perform more detailed analysis.

II. System Security Maintenance Software

SPI/VMS

A new programmer (Jim Rothfuss) was hired during this reporting period. He has begun evaluation and test of a new module, the Integrity Checker Module. This module was written by the previous programmer on the project, but had not been completed or debugged. Jim is also looking into ways of creating a more secure distribution method for SPI/VMS.

SPI/UNIX

We are interviewing candidates for this position. Selection is expected by the end of this reporting period.

Requests continue to be met for both SPI/VMS and SPI/UNIX. Recent shipments include LANL, RICO, and Telnet. There is growing interest from organizations outside DOE, and outside the federal government.

III. Distributed Audit Standards and Requirements

SPARTA, Inc. presented current results of their work in the development of a distributed security audit management system. This effort is expanding the notion of a distributed auditing system providing protocols for collection of audit data and defining the concepts of a virtual audit trail.

This work fits well with the intrusion detection efforts and in other areas of this program by providing a basis for receiving audit information from heterogeneous hosts on a large-scale network.

IV. Computer Incident Advisory Capability (CIAC)

During the reporting period CIAC was involved in three major ongoing incidents involving hackers at DOE sites. The first involved attacks at several DOE sites from a hacker using the CERN network as an access path; the second was continuing activity related to the Wollongong intrusions; and the third, a set of attacks against systems on ESNET. The U.S. Navy asked for assistance in dealing with a hacker situation. CIAC installed a monitoring system for them, at their cost, and provided training on its usage. CIAC continues to interface with the FBI and other law enforcement agencies in these attacks.

CIAC responded to calls for assistance when several DOE sites detected apparent breakin attempts into their UNIX systems. CIAC discovered the "attacks" were originating in Italy, and were not attacks, but rather, a zealous computer security activity that got out of hand. CIAC published a bulletin describing the details to allay fears in the community.

The Incident Handling Workshop was expanded during the quarter to include a module on the insider threat. This module describes how to prevent such attacks, the kind of clues that indicate such an attack is occurring, how to gather evidence to identify the attacker, and how to eradicate bogus code and recover from such attacks. The workshop was also improved by expansion of the module on VMS security. The workshop now contains nine modules.

The Workshop was presented at LBL in October, and a half-day version was presented as part of the DOE computer security "Train the Trainer" program at the Training Academy in Albuquerque in December.

CIAC published 10 Bulletins during the reporting period. There were 43 separate contacts from 27 different sites in October; 23 separate contacts with 14 different sites in November; and 22 contacts with 11 sites in December.

CIAC continues to build a Patch Checking tool for UNIX-based systems. This activity will result in a security software product that can detect known vulnerabilities in computer systems and alert the system manager.

Began updating, and expanding, the CIAC bulletin Board computer (FELIX). This includes updating resident information.

Participated in evolving Cert-System organizational activities. Helped revise the charter to be acceptable to both DOE and LLNL. Also, participated on the Internet Engineering Task Force. Wrote a chapter for the Site Security Policy Handbook on incident handling. This effort is aimed at improving security on the Internet, thereby improving security to all connected sites (including DOE).

Began involvement with growing interest in the Cray Computer operating system (UNICOS). Attended a DOE contractor site meeting where system vulnerabilities were discussed. CIAC will interface with CRAY about repairs to these problems.

AVLIS Safeguards

RD&D

(LIS)

Quarterly Progress Report to the DOE Office of Safeguards and Security

Quarter Ending December 31, 1990

L. L. Thomas, Project Leader
Safeguards and Security Department

January 1991

AVLIS Safeguards RD&D

L. L. Thomas, Project Leader
Safeguards and Security Department

INTRODUCTION

The primary effort of this work is to ensure coordination of the AVLIS safeguards and security systems RD&D, to assure that it occurs at a pace commensurate with the overall AVLIS RD&D effort; to provide planning, support and independent review of safeguards and security system requirements to ensure they are cost effective and integrated into the AVLIS equipment and systems, design and operation; and, as needed, plan and support safeguards instrumentation technology to evaluate and develop the instrumentation for detection of HEU production in an AVLIS separator. LLNL will update the Long-Range AVLIS Safeguards Plan to reflect the current AVLIS deployment schedule.

FUNDING

The FY 1991 funding for this work is \$150K (B&R No.: GD-0604).

TASK DESCRIPTION AND SUMMARY OF ACCOMPLISHMENTS

- I. **Revise the Long-Range AVLIS Safeguards RD&D Plan to reflect current AVLIS deployment schedule.**

This effort was initially scheduled to be completed in November 1990. It was decided to postpone this update to start at the end of March 1991 to coincide with the completion of the AVLIS Plant Conceptual Design Report. This Conceptual Design Report will provide a definitive technical basis, scope and deployment schedule upon which to base rescheduling of the safeguards RD&D.

- II. **In conjunction with DOE/OSS, coordinate a meeting of the Enrichment Program Safeguards Review Group (EPSRG).**

In conjunction with the DOE/OSS Branch Chief for International Safeguards, an EPSRG meeting was set for January 8 and 9, 1991, at LLNL. All participants were contacted and arranged to attend. The agenda was set centering on presentations concerning the status of the AVLIS technology and conceptual plant design. The meeting was postponed because of a serious schedule conflict at DOE/HQ which made it impossible for anyone from DOE/OSS to attend. The EPSRG meeting has been tentatively rescheduled at LLNL in early March.

END

DATE FILMED

03 / 18 / 91