UCRL-ID-106454-97-1

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

Quarter Ending December 31, 1996

Greg Davis
Doug L. Mansur
Wayne D. Ruhter
Mark S. Strauch

January 1997

Lawrence Livermore National Laboratory

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.

DISCLAIMER

This document was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor the University of California nor any of their employees, make any warranty, express or implied, or assume any liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its specific commercial products, process, or service by trade name, trademark manufacturer, or otherwise, does not necessarily constitute or imply its endorsement recommendation, or favoring by the United States Government or the University of California. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or the University of California, and shall not be used for advertising or product endorsement purposes.

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

Quarter Ending December 31, 1996

Greg Davis
Doug L. Mansur
Wayne D. Ruhter
Mark S. Strauch

January 1997

HH

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, make any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

DISCLAIMER

Portions of this document may be illegible in electronic image products. Images are produced from the best available original document.

Table of Contents

Preface

The Lawrence Livermore National Laboratory (LLNL) carries out safeguards and security activities for the Department of Energy (DOE), Office of Safeguards and Security (OSS), as well as other organizations, both within and outside the DOE. This document summarizes the activities conducted for the OSS during the First Quarter of Fiscal Year 1997 (October through December, 1996).

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
- Safeguards and Material Accountability
- Computer Security - Distributed Systems
- Physical and Personnel Security Support

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, 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
Isotope Sciences Division

INTRODUCTION

The Safeguards Technology Program (STP) is a program in LLNL's Isotope Sciences Division of the Chemistry and Materials Science Department 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 spectroscopy techniques and to the development of computer codes for interpreting the spectral data obtained by such.

SUMMARY OF MAJOR ACCOMPLISHMENTS

I. Development of Advanced Isotopic Analysis Software

- We applied for and were granted permission to release and license MGA++ technology.

II. Emission/Transmission Computed Tomography

- Approval received from DOE/OAK to measure a Pu button. Preparations are being made at LLNL to perform the measurement.

III. Implementation, Testing, and Evaluation of LLNL Developed NDA

- Support was provided to Westinghouse Hanford Company for a new Pu isotopic analysis system installed at the Plutonium Finishing Plant.

IV. Monte Carlo Simulation of Gamma-Ray Spectra for Calibration

- The SYNERGY user guide has been expanded to permit the user to easily modify the input without requiring a detailed knowledge of each component (i.e. GAMGEN, MCNP, POSTGL).

V. Development of a Compton-Suppression Method Using Signal Processing Techniques

- Testing continues on the test circuit (without detector) and has yielded improvements in the signal conditioning.

VI. Publication of a Quarterly Report on Technology Development for OSS

- Contributions have been received from most of the planned contributors and refinements have been made to the draft design and layout of the report.

TASK DESCRIPTIONS AND QUARTERLY PROGRESS

Accomplishments achieved during the first quarter of FY97 by STP are described below:

I. Development of Advanced Isotopic Analysis Software

B&R No.	Funding	Obligated
GD060402	$250K	$102K

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.

Uranium analysis using CdZnTe Detectors

DeLynn Clark, William Romine, M. N. Namboodiri, A. D. Lavietes, and James H. McQuaid,

Work on the CZTU code to increase the accuracy and versatility is progressing. CZT spectra are typically characterized by having low statistics and fairly wide (~2 keV) peaks. To minimize the statistical uncertainty in the analysis, the background fit of each peak has been found to be critical to the analysis. Deriving and implementing better algorithms to give significantly less dispersion in the results produced has been accomplished, but additional work remains. Both Ortec and Canberra have expressed an interest in licensing CZTU in the near future.

Enhancement of MGA++

William Romine .

Progress was made at understanding and extending the foundations of the server behavior in the Spec View Graphics Server. The graphics functionality is being enhanced to cover a wider class of Gamma Spectral related data.

Licensing of MGA++ based Software

William M. Buckley, Wayne Ruhter, Winifred Parker, and Robert Lanier

Licensing and CRADA negotiations are proceeding for MGA++ and CZTU. We applied for and were granted permission to release and license MGA++ technology. Given source code restrictions in the permission to release given by NN-50, we are reevaluating a potential license requested by a foreign vendor.

II. Emission/Transmission Computed Tomography

B&R No.	Funding	Obligated
GD060402	$150K	$38K

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 can 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 and with appropriate corrections for sample self-attenuation, one can identify the radioactivities detected and determine their abundance. Transmission or active CT is a nondestructive technique already widely used in medical and industrial applications that use 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

Approval was received from DOE/OAK to perform computed tomography (CT) measurements on a Pu button in Bldg 331. The approval limits the sample size to 300 g and arrangements are currently being made with the LLNL Materials Management to package the Pu button for measurement.

Improvements to the stage control program added the capability for the staging system to collect data at various positions continuously. This is a significant improvement over the previous control program which required information from the "home" position. The enhancement should reduce the required data collection time by as much as 10%.

Attenuation calculations as performed by MCNP for gamma-rays in high-Z materials such as Pu and U are inadequate for CT application. We are investigating the potential of a geometric progression build-up factor to the simulations of highly attenuated gamma-rays in high-Z materials to improve the technique. The geometric progression build-up factor is commonly used in shielding calculations and the study of this technique in CT applications will likely be submitted in a new lifecycle.

III. Implementation, Testing and Evaluation of LLNL Developed NDA Techniques

B&R No.	Funding	Obligated
GD060402	$75K	$52K

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, the LLNL Materials Management Division, and the LANL TA-55 facility. A brief description of activities under this task are given below.

Reduction of funding for this task from $90K to $40K for FY1996 resulted in suspending further activity in this task after April 1996. As a result, we could not address several issues until FY97 funding was available. Hence, the rapid use of FY97 funding in this area.

MGA Support to Westinghouse Hanford

William Buckley

Support was provided to Westinghouse Hanford Company (WHC) for a new Pu isotopic analysis system installed at the WHC Plutonium Finishing Plant. Adjustments were made to the code so that the Ortec-supplied system would provide essentially the same isotopic analysis results as the system being replaced. LLNL Safeguards Technology personnel modeled, modified and tested MGA to provide a code that met these requirements based upon a set of spectra provided by WHC (Rich Hamilton) and an additional test suite available at LLNL. The modifications were primarily changes to the gamma-ray branches, but these changes were well within the reported uncertainties of the branching ratios themselves. LLNL plans to incorporate the WHC test spectra into our continually growing MGA spectral test suite.

IV. Monte Carlo Calculations of Gamma-Ray Spectra for Calibration

B&R No.	Funding	Obligated
GD060402	$125K	$31K

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 and U 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 various geometric arrangements 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.

Simplification of the Monte Carlo Calculation of Gamma-Ray Spectra

Tzu-Fang Wang

The SYNERGY user guide has been expanded to permit the user to easily modify the input without requiring a detailed knowledge of each component (i.e. GAMGEN, MCNP, POSTGL). This represents a significant reduction in operational complexity of the system.

Histories are being generated from the MCNP simulation of a 5 mm x 5 mm x 5 mm CdZnTe detector. This 3-dimensional simulation will be compared to the 1-dimensional simulation to estimate the potential effects on electron and hole transport in a realistic electric field. This should improve our understanding of the charge transport mechanism in CdZnTe detectors.

We are currently investigating the simulation of noise (either junction or thermal noise) in semiconductor detectors. The detailed examination requires a Monte Carlo simulation of the Boltzmann transport equation which depends heavily upon the material (semiconductor components, doping, etc.) and the temperature. Understanding the noise component is critical to any advanced digital signal processing.

V. Development of a Compton-Suppression Method Using Signal Processing Techniques

B&R No.	Funding	Obligated
GD060402	$177K	$39K

This task began in May 1996 with year-end startup funds. The previous concept development and proof-of-principle demonstration for this task were funded principally by the Isotope Sciences Division at LLNL and EG&G.

It is well known that the leading edge of signals from solid state detectors displays details that arise from the particulars of the interaction of the incident gamma-ray (amount of energy deposited and locations of deposition) and the properties of the detector (electric field, charge carrier traps, etc.). If the detector response is understood, which is the case for high purity germanium detectors (HPGe), these signal details can be used to correct individual signals, thus improving the measured spectrum.

We have already established the proof-of-principle that signals from conventional coaxial HPGe detectors can be unfolded with sufficient accuracy to determine the radial locations where energy is deposited with good resolution (about 2 mm). Our algorithms utilize this location information to perform Compton suppression without anticoincidence detectors. Monte Carlo predictions show that it should be possible to choose algorithm parameters that would actually allow nuclear assays to be performed in less time. We are applying our algorithm to measurements of gamma-rays from nuclear material samples of interest to materials control and nonproliferation to test the effectiveness of the algorithm and optimize the algorithm parameters. The signal processing algorithm has been successfully implemented in real time with a digital signal processor at a data rate of approximately 1 kHz. Improvement of the acquisition rate are in progress.

Signal Processing
Dean Beckedahl and Judith Kammeraad

In the first quarter of FY97 we continued testing and improving the "dummy circuit" so denoted because the actual detector is not yet present. However, the circuit is fully functional for the purposes of software development and testing.

The trigger system has been fully tested using a step pulser. The signal from the pulser is split between two processing paths. The first path performs the traditional signal shaping and integration while the other path filters the signal (high pass) and captures it in digital form. The trigger system consists of a discriminator and gate generating hardware. When the discriminator detects the leading edge of the pulse, a gate signal enables the waveform recorder and the ADC circuit in the Macintosh. The waveform recorder captures each signal and stores it until 1000 signals have been recorded and then transfers the buffered signals to the Macintosh. During the transfer the Macintosh disables the trigger system, thus preventing any further data from being collected. As a result this system has a significant dead time but improvements to reduce the dead time will be undertaken later in the year.

In addition, the signal conditioning hardware was improved after redesign of the filters and replacement of an amplifier. The analysis algorithm and software were tested for robustness with white noise of various amplitudes and we have created a Macintosh application of the algorithm. Preparations for assembly of the complete system (including the detector) have begun in the Dissolver Wing of Building 151 at LLNL. This location provides the opportunity to test the detection system with radiation sources of interest since the proper administrative controls are already present and the necessary safety precautions can be easily implemented.

VI. Publication of a Quarterly Report on Technology Development for OSS

B&R No.	Funding	Obligated
GD060404	$100K	$14K

The objective of this proposal is to provide NN-513.4 with a quality, and comprehensive report covering NN-513.4 technology development activities. The first report will cover material control and accountability, and closely related topics. Under this task, LLNL will provide scientific and technical editorial services, art and design capabilities, and other services as needed to provide a color report.

Report Planning and Preparation

Eugene A. Henry

During the first quarter of FY1997, seven contributions to the OSS technology development report were prepared and received by the editor at LLNL. Work on the additional fifteen contributions began after October 1, 1996 at LANL, but have not been received by LLNL as of the end of December. An introductory contribution and distribution list are also anticipated from DOE. Refinements have been made in the draft design and layout of the report.

Due to the lateness of input from the contributors, the publication of the report will not be early in 1997 as originally projected. Publication will take place approximately two to three months after the receipt of all contributions.

STP APPENDIX A: SUMMARY OF ALL MILESTONES AND DELIVERABLES FOR THIS QUARTER

I. Development of Advanced Isotopic Analysis Software

B&R No. GD060402

MGA++ with the Pu module was demonstrated to the OSS in mid 1996.

Development of extended Pu modules to improve the use of the high energy gamma-rays for isotopic assay is in progress. Estimated completion date is 4/97.

Demonstration of and report on the MGA++ module that analyzes high energy radiation of Pu. Work is progressing with an estimated completion date of 5/30/97.

An alpha version of MGA++ was released to EG&G Ortec for testing purposes. Canberra Nuclear has expressed interest in the same.

A report on the status of graphical user interfaces for MGA++ is in progress with an estimated completion date of 2/97.

II. Emission/Transmission Computed Tomography

B&R No. GD060402

Provide a digitized map of isotopic constituents of a hetergeneous Pu MSE Button. DOE approval for measurement received 12/96, 8 months after planned completion data. Preparations for measurement are now in progress. Estimated completion 6/30/97.

Report on the development of software necessary to convert CT data into isotopic information in progress. Estimated completion 5/30/97.

Interim report on studies of layered and shielded materials in progress. Estimated completion 9/30/97.

Study of complex hetergeneous samples which contain moderate amounts of SNM are in planning phase. Estimated completion 1/30/98.

III. Implementation, Testing and Evaluation of LLNL Developed NDA Techniques

B&R No. GD060402

Report on modifications to the uranium analysis software is in progress. Estimated completion date is 9/30/97.

Report on evaluation and testing of MGA analysis on Pu in DOE-approved thick-walled containers has been delayed due to the changing definition of a thick-walled container. Data taken by Westinghouse will be leveraged along with LLNL data for use in the report.

IV. Monte Carlo Calculations of Gamma-Ray Spectra for Calibration

B&R No. GD060402

Report on studies of simulated spectra of complex layered shielded SNM samples in progress. Estimated completion 6/30/97.

Interim report on the calculational study of charge collection phenomena in detectors in progress. Estimated completion 9/30/97.

V. Development of a Compton-Suppression Method Using Signal Processing Techniques

B&R No. GD60402

Complete assembly of hardware system. Dummy system assembled and tested. Real system assembly in progress at LLNL. Anticipated completion of assembly approximately 3/97.

Implement Compton-suppression algorithm of DSP. Software portion completely implemented. Hardware portion implemented in 1996 with event mode data collection. Hardware implementation in real time is the current task with anticipated completion approximately 6/97.

Interim report on equipment status, Compton-suppression algorithm implementation, and initial measurements. Expected completion approximately 9/30/97.

VI. Publication of a Quarterly Report on Technology Development for OSS

B&R No. GD60404

Call to contributors. Input from all contributors not received as of the time of this report. Anticipated receipt of all input anticipated by 4/97.

Report on MC&A technology. Due to the lateness of input from contributors, the publication of the report will not be early in 1997 as originally projected. Publication will take place approximately two to three months after the receipt of all contributions.

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

None this quarter.

Safeguards and Material Accountability

Mark S. Strauch, Assistant Deputy Associate Director
Fission Energy and Systems Safety Program

INTRODUCTION

Fission Energy and Systems Safety Program's Associate Program for Safeguards and Material Accountability works to ensure the security of the nation's nuclear material and supports U.S. efforts to prevent the global proliferation of nuclear weapons materials and technologies. We share this goal with the FESSP Associate Program for Security and Automation Technology and continually collaborate with them. Our technology base is in four areas.

Insider Protection

Insider protection is the safeguarding of nuclear material against theft or diversion by persons who, because of their job responsibilities, have facility access or have positions of authority. We develop protection technologies, operations procedures, and integrated systems to safeguard nuclear material while minimizing the impacts on operations.

Material Accountability

Accounting for nuclear material is necessary to detect material diversions, resolve real or alleged diversions or anomalies, and provide assurance of the effectiveness of other safeguards and security measures. Because modern accountability systems are highly automated, we draw heavily on FESSP's expertise in information systems and their security.

Planning and Evaluation

We believe that thorough planning and evaluation are necessary to ensure that safeguards systems, technologies, and procedures address security threats in the most cost effective manner. As a result, our scientists and engineers are experts in the tools of threat assessment, vulnerability analysis, and resource allocation and apply them whenever appropriate. We also realize that DOE, NRC, and IAEA rules and regulations provide important guidance in systems development and implementation.

Information Security

The national nuclear assets requiring protection for reasons of national security and to prevent global nuclear proliferation are not limited to nuclear material. In some ways classified and sensitive unclassified nuclear information is more valuable. Along with the FESSP Centers for Information Technology and Security and Computer Safety and Reliability, we provide technologies and expertise for protecting the national information assets.

SUMMARY OF MAJOR ACCOMPLISHMENTS

- DISS Rel. 2.0 installed and acceptance tested at all operations offices.
- DISS Rel. 2.1 completed beta testing; released to production by OSS.

TASK DESCRIPTIONS AND QUARTERLY PROGRESS

I. DISS - Electronic Transfer of Personnel Security and Personnel Security Database Modernization Technology Development

(Everett Wheelock, Project Leader)

B&R No.	Funding	Obligated
GH-03	$ 200K	$ 427K
GH-03 carryover	$ 197K	$ 197K

The DOE Integrated Safeguards and Security (DISS) modernization project is developing modernized databases and reengineered workflow for personnel security and weapons data access control systems. The resulting new system will be the focus of activities to track and manage the complex, interrelated set of information supporting clearance processing, access control, and weapons data access operations.

DISS employs a distributed, client/server architecture, utilizing ORACLE database servers running on UNIX platforms with client applications running on individual workstations (PC/Windows and Macintosh computers). The system is being deployed nationwide, with regional servers at DOE operations offices that can exchange data over public networks (Internet and DOEBIN) with the Office of Personnel Management (OPM). These regional databases also share distributed access with the new Personnel Security Database (PSDB) that hosts the Central Personnel Clearance Index (CPCI), Visitor Access Database (VADB), and Weapons Data Access Control (WDAC). The DISS project provides the integration of a new computer, communications, and information security infrastructure utilizing public-key encryption technologies and digital signature authentication of applicant data.

The DISS project completes the work initiated with Electronic Transfer of clearance information (DISS/ET) and development of the new Personnel Security Database (DISS/PSDB). The new DISS system bridges the gap from personnel security to physical security by additional interfaces to external systems including Complex-Wide Access Control System (CWACS) and Safeguards and Security Information Management System (SSIMS).

Production

The current production release status of the various DISS components are listed below. Documentation and release notes for individual items are available on the new secure DISS homepage (https://diss.llnl.gov) on the Released Project Documents Page.

DISS Release Status		
Component	**version**	**Status**
RPS Database	RPS version 2.0.3	
CDUI	2.1	
Admin Client	1.0.2	
Notary	2.05	
RPS/OPM Unix software	Build_2_0_2	

Deployment/Operations Support

Deployment of DISS 2.0 to all DOE Operations offices was completed this quarter.

Release 2.1 Development

- **PSDB standalone central server (WBS#2.2.2):**

The PSDB server v2.1b2 was released to DOE HQ for beta testing during the first week of September. Additional changes identified during the beta test have been identified and LLNL designers have prepared patches that will bring the PSDB server up to 2.1b6. This version will be the Release Candidate for DOE HQ acceptance testing.

- **CPCI User Interface (WBS#2.2.2.5):**

The CPCI user interface v1.0b3 was released to DOE HQ for beta testing during the week of 9-6-96. Additional changes identified during the beta test have been identified and LLNL designers have prepared CPCI Client 2.1b7. This will be the Release Candidate for DOE HQ acceptance testing.

- **WDAC (WBS#2.2.5):**

The WDAC DP Client version 1.0 and WDAC Web Client interface v1.0 are currently in beta testing at DOE HQ with acceptance and release to production anticipated for January, 1997.

- **VADB (WBS#2.2.6):**

The VADB Web interface v1.0 has passed testing at LLNL with release to production expected by January, 1997. This version is expected to be the Release Candidate for DOE HQ acceptance testing.

Web Infrastructure that supports both VADB and WDAC Web Clients has been placed under configuration control at version 1.0b3. Release to production will coincident with acceptance of the web clients.

- **VADB/CWAC Functions (WBS#2.2.6.3):**

VADB/CWAC support functions are in test at 1.0a8. This package will remain at integration test (alpha) designation pending release of CWAC software to beta testing.

- **AUI (WBS#2.2.8):**

Both Applicant User Interface (AUI) and Applicant Diskette Interface (ADI) have completed integration and beta testing. DOE HQ has approved the AUI/ADI for release to production beginning January 31, 1997.

Release 2.1 Deployment

- **DISS R2.1 Ready for Production Operations**

Before the R2.1 deployment can commence, the DISS R2.1 applications currently in beta testing at DOE HQ need to be approved for release to production and placed in an operational mode ready to support deployment of CPCI, VADB, and WDAC.

Details of specific application conditions that need to be established are:

- PSDB Operating with live data;
- CPCI approved for deployment;
- WDAC clients installed on DP 45 computers;
- VADB web operating with live data;
- WDAC web operating and ready to display DP 45 data;
- CPCI mainframe data feed operating with manual file transfer from mainframe;
- DISS production mirror webserver up at LLNL and pointing to HQ PSDB;
- Production mirror PSDB up at LLNL and ready to support training connections for CPCI deployment using sample training data (live data input of CPCI data in HQ PSDB must wait until VADB deployment completes);
- DISS firewall at HQ ready;
- SNS encryption on HQ PSDB enabled;
- Ready to start enrolling field users for CPCI, VADB web.

- **CPCI Data Sync**

The data sync operation is intended to provide one-way data transmission of all mainframe CPCI clearance data to the PSDB server. This will permit the R2.1 deployment planning to proceed. This synchronization will support old DAVAC and new VADB during the interim while some sites are still using the old mainframe and other sites are using the newly deployed R2.1. The data sync is expected to begin running as a nightly process to feed live clearance data into the PSDB server. The PSDB server will then be a mirror of live production data, thus permitting DAVAC and VADB produce same results (query same data), and so VADB cutover can begin.

- **VADB Deployment**

LLNL DISS team personnel with assistance from OSS have identified existing DAVAC users and are prepared to establish new PSDB accounts for them in preparation to begin deployment of VADB. Remaining tasks will include installing Netscape web browser software on PC's accessible to DAVAC users, (for those users that do not already have Netscape-many already do), and establishing net access where required for those DAVAC users without direct connection to the local site's network. VADB training can proceed once browser software is installed and operational. Cutover to VADB from DAVAC can proceed on a site-by-site basis.

- **CPCI Deployment**

This task can be performed concurrent with VADB deployment, or as a separate tasking. CPCI can be installed on the same workstations as the DISS R2.0 CDUI application. CPCI will initially be pointed at a "production mirror" training server located at LLNL, not the headquarters PSDB production server.

- **CPCI cutover**

CPCI cutover can be performed site-by-site with no need for mass system-wide coordination. Each site will stop using the mainframe to process clearances, and start using new CPCI/PSDB. This will prevent any sync problems from arising. Once CPCI and VADB are fully deployed and in operation, operations can move off mainframe.

- **WDAC Data Sync**

Synchronization of data between the existing mainframe-based S2000 WDAC application and the new DISS/WDAC is in preparation at DOE HQ. This synchronization will be accomplished by a nightly dump of visit and channel information into temporary files, transfer of these files to the PSDB server, where the data will be finally imported into the WDAC tables of the PSDB server. Both the mainframe dump and the PSDB import programs have been written and are working. The only remaining task falls to the DP support staff (DynCorp) to establish either automated or manual file transfer between the mainframe and the PSDB server.

- **WDAC Web Interface Deployment**

Deployment of the WDAC Web interface to field personnel for read-only querying of information established by DP-45 will be conducted as part of the VADB deployment. Approximately 50 WDAC field users have been identified and accounts on the DISS/PSDB Webserver will be generated accordingly.

LLNL Tasks for FY97

The goal for FY97 DISS Project tasking is to provide a complete, operating system out of the existing DISS Release 2.0 components deployed to the field and the DISS Release 2.1 components currently in beta-test at DOE HQ.

This DISS Project tasking scenario endeavors to maintain key developers, the "core" team, while working within the following budget constraints:

Assumed FY97 budget:

	$200K	GH03 carryover from FY96 at LLNL
	$500K	GD0508030 carryover at LLNL
	$1600K	GH03 additional FY97 funding to be sent
	$2300K	subtotal
less	$140K	Amount of GD0508030 carryover requested to be returned to HQ
	$2160K	Total FY97 funding available for DISS at LLNL

The major tasks that the LLNL DISS team can undertake immediately and continuing for the remainder of the fiscal year include the following:

- **PowerBuilder Application Maintenance**

This is the incorporation of routine enhancements, bug fixes, ad-hoc reports, etc. into the following existing DISS applications:

Admin Client

CDUI

CPCI

AUI (Windows)

AUI (Mac)

ADI

WDAC DP Client

- **OPM Integration**

This activity entails fielding an oracle database for OPM along with modifications to RPS database. This will serve as a necessary "maintenance retrofit" of the existing PEM mail transmission to OPM. Benefits are expected to be a savings in maintenance effort of approx. 2 FTE of combined sys-admin, DBA, and help desk support that will be otherwise occupied with monitoring and maintaining OPM PEM mail. This task is expected to resolve all open integration issues with OPM, thus allowing OPM to fully adopt the electronic transfer concept and eliminate their reliance on paper transmission.

- **Network Maintenance and Field Support**

LLNL will provide support for complex network operations and maintenance problems that that local site support organizations cannot solve. This includes Unix troubleshooting, firewall maintenance, DOEBIN issues and other network issues. This task allows some travel for on-site troubleshooting if needed.

- **Database Administration**

The DISS team will continue to utilize manpower provided by the in-house LLNL Data Management Team. As with network support, DBA efforts will focus on complex database maintenance and support issues that cannot be resolved by local site resources.

- **Testing**

The DISS team will provide testing of all bug fixes, patches, and utilities developed as part of maintenance. This will also include test case development and testing of the OPM DB system.

- **Documentation and Training**

The DISS team will provide focused documentation updates and development of specific classes such as the infomaker ad-hoc reporting class just presented in Albuquerque. Routine CDUI, CPCI, and AUI training are not covered in this task.

- **Help Desk**

An active help desk presence is deemed essential to the early identification of maintenance problems that will be addressed by the DISS developers. The help desk serves as the "early warning system" for potential production problems. Help desk coverage will be provided over an 8-hour period from 10am East Cost to 2pm West Cost, 5 days/week. This will concentrate efforts on the period in which most requests currently arrive. We will increase reliance on email, voicemail, and the DISS homepage for submission of help requests.

- **VADB/CWAC/Web Maintenance and Support**

The DISS team will work closely with the CWAC team to provide support needed to field CWAC. Routine modifications to web pages for VADB and WDAC would be included as part of maintenance activities.

- **Deferral and Prioritization of DISS Release 3.0 Tasks**

Some DISS 3.0 tasks will be worked as time and resources permit. The prioritization of R3.0 items will be (1) OPM integration, (2) Albuquerque issues.

Completion of these FY97 DISS tasks within the identified funding is contingent on OSS to support placing all DISS Release 2.1 items into production (ready to begin operation). Planning for operation of CPCI, WDAC and VADB can then proceed with field input. The management and development team is committed to the successful fielding and proper operation of this system.

II. Risk Based Evaluation of Computerized Nuclear Materials Accountability Systems (Edwin Jones, Project Leader)

B&R No.	Funding	Obligated
GD-06-04-02	$115K	$ 0K
GD-05-08-03	$142K carryover	$28K

This project uses the methodology developed under OSS R&D task LLNL94005. We access current materials accounting applications to identify information flows representing insider activities with potential serious consequences. In particular, we will evaluate the implementations of latest Local Area Network Materials Accountability System (LANMAS).

During the first quarter of FY97, we worked on revisions of our draft report, "Analysis of Insider Threats Against computerized Nuclear Materials Accountability Applications," incorporating developments and results from FY96. We also began the planning and preparation for a complete analysis of at least one implemented LAN-based accountability system, developed approaches for incorporating cost and operational considerations into extensions of the methodology for evaluations of other information-based systems, started the development of spreadsheet-based tools to aid evaluations and training, and initiated research into anti-gaming (the methodology) procedures.

III. Z-Lock, Electro-Mechanical Lock for Administrative Control LLNL-438 (Michael O'Brien, Project Leader)

B&R No.	Funding	Obligated
GD 06-04-01	$46K	$8K

This project is developing and demonstrating an electro-mechanical "Z Lock" for standardized use in multiple administrative access control applications to compliment existing and future access control systems. The Z Lock will provide economical and accessible graded access control devices/systems for all security interests. We have received the completed software revisions and necessary locking and badging hardware from TESA. The locks were installed in preparation of functional testing and a familiarization of the software began. Actual testing of the hardware and software will be conducted in the next quarter with results being coordinated with TESA in preparation for a DOE HQ demonstration.

SMA APPENDIX A: SUMMARY OF MILESTONES AND DELIVERABLES THIS QUARTER

I. DISS Personnel Security Network and Databases Modernization

B&R No. GH-03

Date	Implementation Milestones	Status
11/13/95	Begin NV Acceptance Test	Complete
1/15/96	Begin RL Acceptance Test	Complete
2/12/96	Begin SR Acceptance Test	Complete
2/26/96	Begin SNR Acceptance Test	Complete
4/22/96	Begin CPCI/WDAC/VADB Acceptance Test	Beta testing - awaiting start of DOE HQ acceptance testing
5/20/96	Begin AL Acceptance Test	Complete
6/17/96	Begin OR Acceptance Test	Complete
7/8/96	Begin HQ Acceptance Test	
7/22/96	Begin ID Acceptance Test	Complete
7/29/96	Begin RF Acceptance Test	Complete
8/19/96	Begin PNR Acceptance Test	Complete

Date	Development Milestones	Status
9/30/95	Release 2.1 standalone centralized system requirements approved	9/21/95
10/15/95	Release 2.1 Operational Readiness Review	10/30/95
11/30/95	Standalone HQ server and network operational	5/9/96
12/31/95	CPCI Oracle–mainframe7 synchronization demonstrated	Complete
2/1/96	WDAC beta test begins	5/27/96
3/15/96	Integration testing of all standalone centralized system components (CPCI/WDAC/VADB/MFRS)	3/22/96
4/30/96	AUI ready for deployment	Complete
4/30/96	Standalone centralized system ready for deployment	Beta - awaiting DOE HQ release to production

6/30/96	Mac ports ready for deployment	AUI port in process

II. Risk-based Evaluation of Computerized Nuclear Materials Accountability Systems

B&R No. GD 05-08-03

Date	Milestone or Deliverable	Status
2/96	Extension to other computerized safeguards and security systems	Completed
3/96	Report on extension to other computerized safeguards and security systems	With Tech Editor
4/96	Technology transfer tools, documentation, and training materials	Delayed at OSS Request
7/96	Management evaluation approach to evaluate all aspects of MC&A systems	With Tech Editor
9/96	Evaluations of risks of LANMAS (or sooner depending on when implementation of LANMAS is complete)	FY1997
9/96	Report on evaluations of risks of LANMAS (or sooner depending on when implementation of LANMAS is complete)	FY1997

III. Z-Lock, Electro-Mechanical Lock for Admin Control LLNL-438

B&R No. GD 06-04-01

Date	Milestone or Deliverable	Status
10/31/95	First level project review	12/7/95 with Darryl Toms
4/30/96	Mechanical and electrical design drawings	TESA contract placed. Received software 11/1/96.
11/1/96	Testing of revised software and lock	In progress

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

Various DISS User Guides and Training Materials

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)

Incident handling remained relatively constant throughout the quarter. The team dealt with 17 incidents that generated 136 actions which include both phone and e-mail correspondence that is required to track the cause of the incident and assist sites in responding appropriately.

CIAC actively participated in and supported the following conferences and seminars: FIRST Technical Colloquium attended by John Fisher presenting information on "Internet Solutions for Tracking Incidents"; Sandy Sparks gave presentations at the CCIRN Meeting on FIRST and FedCIRC; Sandy Sparks attended the NIISC Conference; David Crawford participated in the Trade-Secret Theft and Network Intrusion training and the Sacramento Valley Security – Real Threats seminar; Lauri Dobbs represented CIAC at the ESCC Meeting and presented information on the latest threats in addition to discussing the SSDS project; Paul Mauvais attended an Internet IPV6 Standards Meeting; and Sandy Sparks and Tom Christian attended the SANS Conference and Training session.

CIAC is proposing to present the following topics at the upcoming Computer Security Group Training Conference: DOE-IS Security Information Source (W. Orvis), Using the VAP Vulnerability Database (W. Orvis), and CIAC Threat Update (S. Sparks). In addition, the CIAC team is proposing tutorials on: Unix Security for Network Administrators, Securing Public Web Servers, Computer Virus Operation and New Directions, and Hacker Tools and How Do They Do It.

CIAC provided DOE with an outline of the Scope and Rules of Engagement in preparation for a White Hat activity in addition to a list of requests for Advice & Assistance efforts. The recent White Hat at Lawrence Berkeley National

Laboratory was found to be extremely beneficial and plans are in progress for addressing the various recommendations made by CIAC.

CIAC provided DOE Headquarters with the following: a summary of responses to the Internet Hoaxes, a summary of CIAC's specific efforts to help INEL in FY96, information on Irina, multiple requests regarding ISRC advisory notices, posted the Classified Computer Security Program manual on the DOE-IS server, posted information on the DOE Computer Security Group Training Conference, commented on DOE's Computer Security Incident Reporting form, and provided a copy of "cleansed" incident cost data generated from a previous incident.

II. Network Intrusion Detector (NID)

We implemented and tested the ability to capture packets on FDDI based networks. We completed and tested the port of NID to the HP-UX 10 system for TAC-4 machines. The ability to use a simplified pattern matching model was implemented and tested.

III. AIS Alarm Project

The LANL/LLNL/SNL team released the Phase 0 (Proof-of-Concept) Alarms system to the LANL test network and demonstrated the capability to detect suspicious events, assess them, and issue appropriate responses. The project plan for the Phase 1 (Production) Alarms system was completed and submitted.

IV. Security Profile Inspector for Networks (SPI-NET)

This quarter marks the start of the SPI-NET Distributed Security Inspection Project. This quarter saw refinement of the SPI-NET work (co-sponsored by DoD) leading to a major field test release (SPIN 0.96) on December 20, 1996, as announced through the SPI-ANNOUNCE mailing list.

V. Profiling and Vulnerability Analysis Project (VAP)

We continue to load the database with known vulnerabilities and intrusion methods. There are currently 114 vulnerabilities and 97 intrusion methods detailed in the database.

The Netscape secure web server has a problem that prevents it from reliably running CGI scripts on our system. Instead of waiting for a new version of the server, we are switching to the Microsoft Internet Server that runs under Windows NT 4.0. Switching to a different web server will not only get around the problem with running server scripts, but will make the web pages and database much easier to maintain.

VI. DOE Information Security (DOE-IS) Server

We continued to populate the server as an ongoing activity. Highlights include: Conference call for the 1997 DOE Computer Security Group Training Conference, the CIAC Internet Hoaxes page, and the DOE User Needs Management tool.

We completed an informative brochure describing how to use the server and how to get new information placed on the server.

TASK DESCRIPTION AND QUARTERLY PROGRESS

I. Computer Incident Advisory Capability (CIAC)

B&R No.	Funding	Obligated
GD060603	$450K	$191K

The Computer Incident Advisory Capability (CIAC) team members continued to assist DOE sites with computer intrusions, vulnerability assessments, security tools, evaluations, education, training, and awareness. Incident handling included intrusions which crossed country borders, new clandestine techniques, and spamming of inappropriate messages.

CIAC actively participated in and supported the following conferences and seminars: FIRST Technical Colloquium attended by John Fisher presenting information on "Internet Solutions for Tracking Incidents," and Sandy Sparks gave presentations at the CCIRN Meeting on FIRST and FedCIRC. Sandy Sparks attended the NIISC Conference, David Crawford participated in the Trade-Secret Theft and Network Intrusion training and the Sacramento Valley Security - Real Threats seminar, Lauri Dobbs represented CIAC at the ESCC Meeting and presented information on the latest threats in addition to discussing the SSDS project, Paul Mauvais attended an Internet IPV6 Standards Meeting, and Sandy Sparks and Tom Christian attended the SANS Conference and Training session.

The CIAC Web server is now set up and continuously updated as new bulletins are released. The server also contains information on the FIRST Conference, DOE Computer Security Group Training Conference, and a newly created CIAC Internet Hoaxes page.

CIAC's 2301 - *Computer Virus Information Update* document was updated and released in December 1996. A draft of the *Windows NT Network Security* document is in review. The goal is to create a more defined and usable document for a larger scale design by breaking the "Securing Windows NT Server and Workstation" document into four separate papers to provide DOE sites with a comprehensive reference for systems administrators servicing NT networks and systems.

CIAC has provided financial reports on a monthly basis and an annual listing of existing equipment, plus a list of FY97 needs is in progress. CIAC is currently working on collecting data for the annual report.

II. Network Intrusion Detector (NID)

B&R No.	Funding	Obligated
GD060403	$225K	$26K

We completed the ability to capture packets from an FDDI network. The FDDI option was implemented to allow users to seamlessly use NID on FDDI based networks as well as Ethernet based ones. The FDDI networks have much higher bandwidths so the quantity of data can be greatly increased. This requires the NID machine to be a relatively fast machine. Also, the increase in the amount of data requires increased disk storage to capture all the data. This system was successfully tested on LLNL's FDDI network.

We completed the port of NID to the HP-UX 10 operating system. This was done because the DoD already has a substantial procurement of these systems, namely TAC-4. The port was successfully completed and tested with one minor caveat. This caveat is that HP-UX 10 systems do not currently support the **bufmod** libraries, which keep track of packets and packet statistics. As a result, there are no statistics as to the number of dropped packets. We are hoping that our customers who have TAC-4 systems will encourage Hewlett Packard to add this support to upgrades of the HP-UX 10 system.

We completed the implementation of an optional simple pattern matching threat signature to the system. After performing a normal capture run, the resulting data were processed with the analyze code which uses the UC Davis threat model. An option was added to the analyze code to allow the user to process the data with a simple pattern matching model instead of the UC Davis model.

Finally, two new people were hired to support NID. They have been trained and have taken over full support of the system.

III. AIS Alarm Project

B&R No.	Funding	Obligated
GD060403	$800K	$156K

LLNL completed both of the Alarms project milestones scheduled for this quarter. Working closely with SNL and LANL, the Phase 0 (Proof-of-Concept) release of the Alarms system was successfully installed on the Alarms development test network at LANL and was demonstrated to Carl Piechowski and Ray Holmer. The Phase 0 system sensors successfully detected suspicious actions in three different attack scenarios and reported them to the Assessment engine, which correctly interpreted these actions as attacks and issued response actions. This successful demonstration was a crucial step toward validating the technical approach.

Following this success, the project plan for the Phase 1 (Production) release was developed and submitted for review and approval. Lessons learned from the Phase 0 development were incorporated into this plan.

Technical meetings with LANL and SNL were held as work began on the Conceptual Design Document for Phase 1 with a submittal deadline of late January, 1997.

IV. Security Profile Inspector for Networks (SPI-NET)

B&R No.	Funding	Obligated
GD060403	$225K	$38K

The Security Profile Inspector for Networks (SPI-NET) project builds upon work conducted for the DoD in producing a secure, distributed inspection system. The prototype has been demonstrated to conduct convenient multi-host security inspections and reporting.

A major effort this quarter revised the entire package installation procedures, leading to a product that is both more easily and more flexibly installed. In particular, in addition to the standard source-code distribution, there are now available pre-compiled (binary) SPI-NET packages for selected platforms.

The user interface now contains a snapshot specification editor for the SPI-NET Change Detection Tool (CDT). This facility allows an administrator to easily select subsets of users, groups, files and directories from the file system that are to be recorded for the purpose of intrusion change detection. For each subset specified, checkboxes are provided so that the administrator may indicate exactly which attributes of the subset are to trigger change detection reporting entries. The SPI-NET Security Domain host table is incorporated into this screen, allowing the user to deploy and retrieve the specification parameters for each host in the domain, allowing customization on a system-by-system basis.

V. Profiling and Vulnerability Analysis Project (VAP)

B&R No.	Funding	Obligated
GD060503	$225K	$32K

We are continuing to load the database and currently have 114 vulnerabilities and 97 intrusion methods detailed.

We have redesigned the external access around a Microsoft Web Server running on a Windows NT 4.0 platform. The Web server will link to an Access database and provide external sessions using the Secure Sockets Layer (SSL) encryption mechanism. The SSL protocol gives the session end-to-end protection. DOE access to the database will be granted by a local site CPPM who will have the authority to add a user name and password to the system.

The change to the Microsoft server will overcome a problem with the Netscape server. The change will also make it much easier to maintain the database-web interface.

VI. DOE Information Security (DOE-IS) Server

B&R No.	Funding	Obligated
GD060503	$100K	$24K

We continue to add new and updated information to the server. New items this quarter include the DOE User Needs survey pages and the CIAC Internet Hoaxes page.

We completed a draft of a brochure describing how to use the server and how to get information added to the server.

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

I. Computer Incident Advisory Capability (CIAC)

B&R No. GD060603

Issued 19 Bulletins/Advisories:

H-01: Vulnerabilities in bash
H-02: Sun's TCP SYN Flooding Solutions
H-03: HP-UX_suid_Vulnerabilities
H-04: HP-UX Ping Vulnerability
H-05: Internet Hoaxes: PKZ300, Irina, Good Times, Deeyenda, Ghost
H-06A: Sun libc/libnsl vulnerabilities (Sun Bulletin #00137a)
H-07: Sendmail SIGHUP-smtpd Vulnerability
H-08: lpr Buffer Overrun Vulnerability
H-09: HP 9000 Access Vulnerability
H-10: HP-UX Security Vulnerabilities (passwd, fpkg2swpkg, newgrp)
H-11: Sendmail Group Permissions Vulnerability
H-12: IBM AIX(r) 'SYN Flood' and 'Ping o' Death' Vulnerabilities
H-13: IBM AIX(r) Security Vulnerabilities (gethostbyname, lquerypv)
H-14: SGI IRIX Vulnerabilities (systour, OutOfBox, cdplayer, datman)
H-15: Korn Shell (ksh) suid_exec Vulnerability
H-16: HP-UX Security Vulnerabilities (chfn, Remote Watch)
H-17: cron/crontab Buffer Overrun Vulnerabilities
H-18: Denial-of-Service Attack via ping
H-19: HP Software Installation Programs Vulnerability

Reissued CIAC 2301, the Virus Update document.

II. Network Intrusion Detector (NID)

B&R No. GD060403

No milestones or deliverables to report for this quarter.

III. AIS Alarm Project

B&R No. GD060403

Completed demonstration of Phase 0 Alarms system to sponsor.
Completed and submitted to sponsor Project Plan for Phase 1 development.

IV. Security Profile Inspector for Networks (SPI-NET)

B&R No. GD060403

The SPI-NET Change Detection Tool Meta-Specification Editor milestone was successfully completed this quarter. In addition, a product deployment plan has been prepared and is being utilized in promoting a broad field-test deployment to DOE system security personnel.

V. Profiling and Vulnerability Analysis Project (VAP)

B&R No. GD060503

No milestones or deliverables to report for this quarter.

VI. DOE Information Security (DOE-IS) Server

B&R No. GD060503

A draft brochure describing how to access the server and how to get new information placed on the server was delivered to DOE.

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

None.

Physical and Personnel Security Support

Greg Davis, Program Manager

INTRODUCTION

The purpose of this set of projects is to support the standardization of security systems in the Department Of Energy to meet DOE orders and requirements while reducing costs, and also to support the DOE in offering relevant security technology and capabilities to Federal standardization efforts. The DOE appears to be unique with its integrated approach to physical and personnel security on a nation-wide scale. These projects are carаried out as part of the Laboratory's Fision Energy Systems Safety Program.

SUMMARY OF MAJOR ACCOMPLISHMENTS

I. Argus Home Page

The Argus Webpage security was upgraded to RC4-128 encryption standard. Other security enhancing steps were taken.

II. Neutron Chip Based Sensor Integration

- Upgraded Echelon development system to vendor's current release.
- Began selection of third party sensors and design of required hardware modifications.
- Developed preliminary design of sensor neuron chip software.

III. Low Cost Enrollment Station

- Completion of software for all functionality except Batch Enrollment.
- Completion of a draft version of QA test procedures.

IV. DOE Proprietary Security Sensor Development

- Project funding became available in late October and was allocated at a level 44% less than requested. Significant revisions to project plans, budgets, and schedules, based on the allocated funding, were completed.
- A project kickoff meeting was held on December 11 at LLNL to introduce all project team members, describe the project, its goals, schedule, and deliverables, outline the project team organization and describe the proposed sensor development effort.

- A video teleconference was held on December 12 with Darryl Toms and Carl Pocratsky to review the project plan, schedule, and proposed sensor development activities.

- Procurement of MIR motion sensors to be used in early deployment on the ARGUS test system was completed.

V. Advanced Training Simulator for Security Dispatch

- With the availability of project funding, the project design team was assembled and work on the Advanced Training Simulator began in early December.

- The basic design concepts and system architecture for the Advanced Training Simulator system was developed. A unique and innovative system solution was developed with the detailed design now underway.

VI. Complex Wide Access Control Project

- Completed update CWAC and VADB documentation and incorporated into CWAC Web page

- Established a VADB platform for DOE/Contractor sites to use for CWAC development and testing. Reached agreement with DISS project team for them to support this platform.

- Established information package to be provided to sites beginning CWAC implementation. Started providing CWAC implementation assistance.

- Began development of a draft CWAC Certification Program.

TASK DESCRIPTIONS AND QUARTERLY PROGRESS

I. Argus Home Page

B&R No.	Funding	Obligated
GD 06057-SF50	$57.2K	$5.6K as of 12/31/96

The Argus webpage continued to operate (24 hours a day, 7 days a week) in secure mode throughout the 1st quarter, providing the DOE complex with valuable information about standard DOE security systems. We have continued to receive and honor requests for access throughout the quarter. There are currently 29 off-site and 27 LLNL on-site Argus webpage users. This quarter we initiated a review of all current users to evaluate their need for continued access to the webpage.

In a further effort to enhance the protection of the information on the Argus webpage, we upgraded the encryption algorithm to RC4-128 (with a 128 bit key). This effectively prevented access to the Argus webpage by any webbrowser software available for international export, regardless of the username or password. US-only versions of webbrowsers are required to access the Argus Webpage.

The Documentation section has been updated and reorganized. There are currently 58 titles of released Argus documentation available on the webpage, 19 of which are new or updated in the last six months.

II. Neutron Chip Based Sensor Integration

B&R No.	Funding	Obligated
GD 060401	$236K	$11K

This project requires several internal deliverables:

10 Argus type sensors modified to incorporate neuron chips
Sensor neuron chip software
Sensor network protocol definition
Sensor network host software

We have preliminary designs for the sensor Neuron Chip software and for the hardware modifications required to the selected sensors to incorporate the Neuron Chips.

Definition of the network protocol is the next priority.

III. Low Cost Enrollment Station

B&R No.	Funding	Obligated
GH 03 - FY 97	$21.6K	$21.6K
GD 0605	$185K	$143K

Development

Development of LCES has continued on schedule and within budget. Brian Ciepriesz, our Sybase/Powerbuilder consultant, has written all software to date, and has done an excellent job. All software with the exception of batch enrollment has been completed and is ready for QA testing. Batch enrollment functionality is on schedule, and will be ready for QA testing by 31 Jan.

Testing

Rita Benedict, who has been the test coordinator for DISS, will be the tester for LCES.

We be installing software on the target test PC in January. An initial draft of the test procedures was written in September. A current, edited version of the procedures will be supplied to Rita on 23 Jan. She will begin the QA test process immediately following receipt and review of the procedures.

We are anticipating that testing will be completed on schedule.

Documentation

Brian's next task will be completion of all required documentation. This includes:

Developer documentation
Installation guide
User guide

System Demonstration

LCES will be ready for demonstration in mid-February as planned. It was expected that the demonstration would be held in conjunction with the ASQP meeting that was to be held at LLNL. With cancellation of the meeting, a new date for demonstration of LCES needs to be set.

IV. DOE Proprietary Security Sensor Development

B&R No.	Funding	Obligated	Liens
GD 06 04	$400K	46K	5K as of 12/31/96

Project re-planning

Funding for the project became available late in October. The allocated budget was $400K, while the requested budget was $710K. This large shortfall in funding necessitated significant re-planning and redefinition to bring the project into line with available funds. The scope of the project was reduced from an effort to develop and deploy several prototype sensors and sensor systems in year one, to one in which a few sensors would be developed and field tested. Additional re-planning was undertaken to modify the project scope to conform with agreements made during the video teleconference on December 12, which is discussed below.

MIR Security Sensor Project Kickoff Meeting

The purpose of the meeting was to introduce project team members, describe the project, its goals, schedule, and deliverables, outline the team organization and describe the proposed sensor development effort. Copies of the Project Plan and a document describing Planned Sensor Development of FY-97 were distributed to meeting attendees. The technical approach for the new sensor development was also discussed at the meeting. To minimize technical risk, new sensors will be developed using existing MIR sensor designs from the MIR modular family, in particular the RF receiver and transmitter designs which have been fully prototyped and tested. New design, with low technical risk, is required to satisfy the goals of the project, particularly in low frequency signal processing circuits to address the unique capabilities which will be integrated into these sensors.

MIR Security Sensor Project Kickoff Video Teleconference

The purpose of the meeting was to review the project plan, scope and schedule. Copies of the meeting presentation materials, the Project Plan and a document describing the Planned Sensor Development of FY-97 were available to meeting attendees at Germantown. The overall scope of the project for year one was discussed. The discussion included projections of shortfalls in out-year budgets which would likely have a negative impact on the project as originally proposed. Based on those talks, the participants agreed that the project should focus on the development of a single sensor with the goal to fully develop that sensor in FY-97. In addition, the proprietary nature of information which will be produced in the project and the need to protect that information was discussed.

Procurement of MIR motion sensors

MIR motion sensors were procured in the first quarter. These sensors will be deployed early in the project in the ARGUS test system to provide a means early evaluation of MIR technology. In the next quarter, these sensors will be modified, as needed, to make them compatible with the ARGUS test system and they will be installed and tested in realistic environments. Test results will be used, as appropriate, in the new sensor design.

V. Advanced Training Simulator for Security Dispatch

B&R No.	Funding	Obligated
GD060401	$94K	$5.6K

The Integration of Security Alarm Systems with Advanced Simulation

An innovative design concept for the Advanced Training Simulator system was developed and carefully examined. This new concept makes use of LLNL's powerful conflict simulation system known as the Joint Tactical Simulation (JTS) model. It was determined that the JTS system can be used by training directors to create and execute the life-like intrusion detection scenarios needed for this effort. It was further determined that the JTS system itself can be directly interfaced to Argus so that alarm events within the simulation can be used to actually trigger Argus Console system incidents.

The powerful integration of Argus and JTS capabilities was successfully determined to be feasible. The design work for the effort was initiated. A review of the JTS communications protocol was completed and the basic structure of the Argus/JTS interface was determined. An initial training scenario was selected that uses JTS simulation work that was previously initiated by the LLNL Safeguards and Security Department in cooperation with Sandia National Laboratory.

The detailed design of the training simulation system will be undertaken during the next quarter. The securing of the remaining necessary hardware and software resources for this effort is also underway.

VI. Complex Wide Access Control Project

B&R No.	Funding	Obligated
GD 060501	726K	95K

Task 1: Complete work to install, activate, and provide training for Enrollment/Verification Stations at DOE Oakland and DOE Germantown

Quarterly Progress: All installation work associated with a CWAC Enrollment/Verification Station at Oakland was completed in October. Software was installed, but operator training and system activation have been deferred pending availability of the production Visitor Access Data Base and official personnel clearance records on the HQ DISS server.

Task 2: Provide CWAC consulting support and implementation assistance to ACS vendors and other DOE facilities.

Quarterly Progress: The CWAC Functions and Requirements Document and the VADB Interface Control Document, which are the critical technical documents for CWAC implementation, were revised to reflect the "as-built" condition after initial CWAC development. A new CWAC Web page layout was developed, and the CWAC and VADB documents were incorporated in the Web page and are now available for download by authorized users. An overview of CWAC covering the DOE-OSS vision, project objectives, CWAC/VADB interface, CWAC accomplishments, and near term plans has also been incorporated into the web page.

Information essential for sites beginning CWAC implementation has been developed. Since specific Oracle software is required for CWAC clients to communicate with the VADB server, we are coordinating with Oracle to obtain the required client SQL*Net and Secure Network Services software and documentation. This software is available without charge to clients, based on the VADB server licensing agreement, but must be requested by LLNL, since we purchased the server licenses.

Information has been provided to Sandia to assist them in developing a CWAC gateway which will support CWAC objectives. We have provided accounts and passwords on the VADB production mirror to Sandia for development and testing purposes.

A meeting has been scheduled with Savannah River Site personnel in February to discuss implementation of CWAC at SRS.

Task 3: Prepare for and conduct a CWAC workshop. The workshop will be open to all DOE contractors, and will provide a forum to communicate CWAC concepts and design information, and allow attendees to identify issues and seek help with specific implementation questions

Quarterly Progress: Initial plans were developed to hold a workshop in conjunction with a Classified Visit Control workshop sponsored by Defense Programs. We had coordinated with Glen Tayler of DOE/HQ-DP to host this workshop at LLNL in early February. However, issuance of a revised DOE Order related to Classified Visits has been delayed, and Mr. Tayler now anticipates that the Classified Visit Control workshop will be held in April. Because of the broad attendance at this workshop, we have proposed to delay the CWAC workshop accordingly. Holding the workshops together will also eliminate some sites from having to make separate trips for the two workshops.

Task 4: Provide support for bug fixes and requested software enhancements for DOE-OAK and DOE-HQ enrollment/verification stations.

Quarterly Progress: No activity. These systems have not yet been activated.

Task 5: Establish a VADB platform to be used by DOE sites to develop, test, and qualify the software they intend to implement for CWAC enrollment/verification and access control authorization retrieval.

Quarterly Progress: Complete. A PSDB production mirror server has been established at LLNL which will duplicate the HQ-DISS server hardware and software at DOE-HQ. This platform is intended for use by sites developing CWAC software. The DISS project team has agreed to provide system management and account management support for this platform.

Task 6: Develop a program to qualify and certify the hardware/software interface and procedures developed by DOE sites implementing CWAC. The program will ensure that appropriate security measures are in place to protect information, to ensure enrollment procedures and data are appropriate and accurate, that access control data is maintained in VADB and in local sites databases, and access control information retrieved is properly utilized.

Quarterly Progress: Work has begun to determine the structure of the certification program. At present we envision development of a list of critical features with accompanying assessment criteria. As sites complete development of a CWAC interface capability, but before they are allowed access to the HQ-DISS server for CWAC enrollment, we will request that they perform a self assessment against a CWAC Certification instrument. Results of this self-assessment will be evaluated to ensure personnel security and access control information will be appropriately utilized and protected.

Task 7: Provide project management support. Activities include budget planning, liaison with DOE-HQ Technical Monitor and Project Manager, quarterly report preparation, quarterly project review preparation/conduct, project control functions, final project report preparation, and Quad chart updates.

Quarterly Progress: One change proposal has been submitted to delay three project milestones dependent upon activation of a production Visitor Access Data Base at DOE -HQ.

A Quad chart update was prepared and submitted as requested by OSS.

An overview of CWAC and DISS, including detail concerning the Enrollment/Verification Station awaiting activation at the Oakland Federal Building, was presented to DOE-OAK Information Management Division (IMD) and Safeguards and Security Division (SSD) personnel.

PPSS APPENDIX A: SUMMARY OF ALL MILESTONES AND DELIVERABLES FOR THIS QUARTER

I. Argus Home Page

Original Deliverable	Description of Deliverable	M/D	Status
2/14/97	Presentations to and report on Argus Advisory group meeting	D	
4/97	Participation in Federal Interagency meetings	M	
9/1/97	Presentations to and report on Argus Advisory group meeting	D	
9/31/97	Conduct the FY97 Argus Workshop	D	
9/31/97	Delivery of Source Code to the Argus Homepage	D	

II. Neutron Chip Based Sensor Integration

There were no scheduled deliverables for this quarter.

III. Low Cost Enrollment Station

Original Deliverable	Description of Deliverable	M/D	Status
Jul 96	LCES Functional Specification	D	Complete
Jan 97	Complete software development	M	On schedule
Jan 97	Deliver software to QA for testing	M	On Schedule
Feb 97	User Guide, System Installation Guide	D	On Schedule
Feb 97	LCES Demonstration	D	On Schedule**

** May be delayed due to delay of ASQP meeting to Apr 97. LCES will be ready for demo in February.

IV. DOE Proprietary Security Sensor Development

Original Deliverable	Description of Deliverable	M/D	Status
1/23/97	Quarterly report	D	Complete

V. Advanced Training Simulator for Security Dispatch

Original Deliverable	Description of Deliverable	M/D	Status
6/97	Simulator design review	M	
9/97	Simulator research/design report publication	M	In draft
9/97	Prototype demonstration		

VI. Complex Wide Access Control Project

Milestone Date	Description of Milestone	Status
12/15/96	CWAC WWW Page updated	Complete

M=Milestone
D=Deliverable

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

CWAC Functions and Requirements Document, Version 1.2.1, December 18, 1996