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

Quarter Ending September 30, 1996

Greg Davis
Dan Johnson
Doug L. Mansur
Wayne D. Ruhter
R. Scott Strait

RECEIVED

DEC 09 1996

OSTI

DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED
LM

October 1996

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.

MASTER

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, makes 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 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.

This report has been reproduced
directly from the best available copy.

Available to DOE and DOE contractors from the
Office of Scientific and Technical Information
P.O. Box 62, Oak Ridge, TN 37831
Prices available from (615) 576-8401, FTS 626-8401

Available to the public from the
National Technical Information Service
U.S. Department of Commerce
5285 Port Royal Rd.,
Springfield, VA 22161

DISCLAIMER

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

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

Quarter Ending September 30, 1996

**Greg Davis
Dan Johnson
Doug L. Mansur
Wayne D. Ruhter
R. Scott Strait**

October 1996

Table of Contents

Preface	v
Safeguards Technology Program	STP-1
Introduction.....	STP-1
Summary of Major Accomplishments.....	STP-1
Task Description and Quarterly Progress.....	STP-2
I. Development of Advanced Isotopic Analysis Software.....	STP-2
II. Emission/Transmission Computed Tomography.....	STP-3
III. Implementation, Testing and Evaluation of LLNL Developed NDA Techniques.....	STP-4
IV. Monte Carlo Calculations of Gamma-Ray Spectra for Calibration	STP-5
V. Development of a Compton-Suppression Method Using Signal Processing Techniques	STP-5
VI. Publication of a Quarterly Report on Technology Development for OSS	STP-6
VII. Other Related Activities.....	STP-7
STP Appendix A: Summary of all Milestones and Deliverables for This Quarter.....	STP-8
STP Appendix B: List of all Publications Produced During This Quarter.....	STP-9
Safeguards and Material Accountability.....	SMA-1
Introduction.....	SMA-1
Summary of Major Accomplishments.....	SMA-2

Task Descriptions and Quarterly Progress.....	SMA-2
I. DISS - Electronic Transfer of Personnel Security and Personnel Security Database Modernization Technology Development.....	SMA-2
II. Risk Based Evaluation of Computerized Nuclear Materials Accountability Systems.....	SMA-6
III. Z-Lock Electro-Mechanical Lock for Administrative Control LLNL-438.....	SMA-7
SMA Appendix A: Summary of all Milestones and Deliverables for This Quarter.....	SMA-9
SMA Appendix B: List of all Publications Produced During This Quarter.....	SMA-12
 Computer Security - Distributed Systems	CSDS-1
Introduction.....	CSDS-1
Summary of Major Accomplishments.....	CSDS-1
Task Description and Quarterly Progress.....	CSDS-3
I. Computer Incident Advisory Capability (CIAC).....	CSDS-3
II. Network Intrusion Detector (NID).....	CSDS-3
III. AIS Alarm Project.....	CSDS-4
IV. Security Profile Inspector for Unix and VMS Operating Systems (SPI/UV).....	CSDS-4
V. Profiling and Vulnerability Analysis Project (VAP).....	CSDS-5
VI. DOE Information Security (DOE-IS) Server	CSDS-5
CSDS Appendix A: Summary of all Milestones and Deliverables for This Quarter.....	CSDS-6

**CSDS Appendix B: List of all Publications Produced
During This Quarter..... CSDS-7**

Complex-Wide Access Control System	CWAC-1
Introduction	CWAC-1
Summary of Major Accomplishments.....	CWAC-1
Task Description and Quarterly Progress.....	CWAC-2
I. Complete remaining procurement and assemble three CWAC enrollment/verification stations, one for development at LLNL, and two more for deploy- ment at DOE-OAK and DOE-HQ.....	CWAC-2
II. Modify Argus encoding/enrollment software for use as a CWAC enrollment/verification station with the ability to encode DOE Standard Badges, communicate enrollment information with the VADB, and verify visitor identity and access control information	CWAC-2
III. Develop the software required for the LLNL Argus ACS to communicate with the VADB	CWAC-3
IV. Provide installation requirements, support installation, test and activate an enrollment/ verification station at DOE-OAK	CWAC-3
V. Provide support for bug fixes and requested software enhancements for DOE-OAK enrollment/verification station	CWAC-4
VI. Provide Standard Badge policy and procedure support	CWAC-4
VII. Provide project management support.....	CWAC-4
VIII. Complete installation preparation, support installation, and activate an enrollment/ verification station at DOE-HQ	CWAC-5
CWAC Appendix A: Summary of all Milestones and Deliverables for This Quarter.....	CWAC-6

CWAC Appendix B: List of all Publications Produced During This Quarter.....	CWAC-6
--	--------

Standardization of Security Systems	SSS-1
Introduction.....	SSS-1
Summary of Major Accomplishments.....	SSS-1
Task Description and Quarterly Progress.....	SSS-1
Appendix A: Summary of all Milestones and Deliverables for This Quarter.....	SSS-3
Appendix B: List of all Publications Produced During This Quarter.....	SSS-3

Preface

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

- Safeguards Technology
- Safeguards and Materials Accountability
- Computer Security - Distributed Systems
- Complex-Wide Access Control
- Standardization of Security Systems

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

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

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

Safeguards Technology Program

**Wayne D. Ruhter, Program Manager
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 spectrometry techniques and to the development of computer codes for interpreting the spectral data obtained by these techniques.

The Safeguards Technology Program team presented a video conference review to members of the Planning and Technology Planning Branch on September 20, 1996.

SUMMARY OF MAJOR ACCOMPLISHMENTS

I. Development of Advanced Isotopic Analysis Software

- Development of a software code, CZTU, has begun to analyze uranium spectra obtained with cadmium-zinc-telluride detectors.

II. Emission/Transmission Computed Tomography

- The Pu-600 code is being implemented in the spectral tomographic scanner package to assay Pu isotopics of material deeper in the sample.

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

- One copy of MGA has been transferred to Westinghouse Hanford for use in plutonium storage activities.

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

- A graphical interface has been developed for the GAMGEN transuranium gamma-ray generation software.

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

- A test circuit has been used to demonstrate real-time signal processing at rates up to 1 kHz.

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

- A call for papers for the report has been sent out, and a draft layout design has been developed.

TASK DESCRIPTIONS AND QUARTERLY PROGRESS

Accomplishments achieved during the fourth quarter of FY96 by STP are described below:

I Development of Advanced Isotopic Analysis Software

<u>B&R No.</u>	<u>Funding</u>	<u>Obligated</u>
GD060402	\$350K	\$351K

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.

U235 software for assay of Uranium *DeLynn Clark*

A computer program has been written that can non-destructively evaluate the percentage of ^{235}U in a uranium sample from the analysis of the emitted gamma rays. The program, U235, is operating and work continues to test and improve the accuracy of the assay for a variety of uranium samples.

Uranium analysis using CdZnTe Detectors

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

CdZnTe detectors and other room temperature detectors have the potential of being used widely in a variety of applications in safeguards technology as gamma-ray detectors with reasonably good energy resolution. To analyze the complex gamma-ray spectra of nuclear materials obtained with such a detector, it is necessary to characterize the detector's response as a function of gamma-ray energy. We have completed this work.

The results of this work is being incorporated into uranium analysis software being developed in part under a CRADA with EG&G Ortec, and in part under STP. This

software, CZTU, is being developed to analyze data taken with cadmium-zinc-telluride detector also under development at LLNL with the support of EG&G Ortec. CZTU operates within the MGA++ framework, and it can be included in a comprehensive software suite. It is built on some of the methods developed for the U235 code. In addition to EG&G Ortec, Euratom, and soon ISPO/IAEA are providing some support for this software development.

Enhancement of MGA++

William Romine

An effort has begun to integrate the latest networking and data communication facilities present in the Microsoft Window operating systems into the MGA++ system. Packaging this functionality as a standard part of each component will allow MGA++ to be extended both into the realm of instrument control and as originally envisioned to allow for iterative analyses. As side benefits, MGA++ will also be able to utilize future improvements in microprocessor technology, multiprocessor, and multinode desktop environments.

Licensing of MGA++ based Software

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

Discussions with vendors on the licensing of MGA++ based software are continuing. We are working licensing through CRADAs for the MGA and U235 components of MGA++ to EG&G Ortec and BNFL Instruments. We have also been contacted by Canberra Industries about these software packages. This license would probably proceed normally (without a CRADA). We are also licensing the CZTU software to EG&G Ortec. Canberra Industries has also requested a license on the CZTU software.

II. Emission/Transmission Computed Tomography

<u>B&R No.</u>	<u>Funding</u>	<u>Obligated</u>
GD060402	\$150K	\$142K

This technology combines the advantages offered by two well-developed, nondestructive assay techniques: gamma-ray spectrometry and computed tomography (CT). Coupled together these two techniques may be used to nondestructively and quantitatively measure uranium and plutonium in samples where the U and/or Pu are heterogeneously distributed, distributed in lumps of varying size, or the sample matrix varies in density and composition. This technology potentially offers significant improvements over current segmented gamma-scanning (SGS) techniques.

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

Emission and Transmission Computed Tomography Application

Tzu-Fang Wang

The Operational Safety Procedure for the use of the tomographic scanner was approved at the end of July for operation in Building 331. However, DOE/OAK has still not approved operation of the scanner as of September 1996, a year after we began preparations for operation in Building 331. Once we get approval, it will take about two months to complete a test scan of the MSE button.

We have started integrating of the Pu-600 code into the tomography program to get additional analyses of the Pu isotopics that use the high energy gamma rays. This analysis will give isotopics information for material deeper in the sample than can be obtained with MGA which relies on the 100-keV region.

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

<u>B&R No.</u>	<u>Funding</u>	<u>Obligated</u>
GD060402	\$40K	\$40K

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

Reduction of funding for this task from \$90K to \$40K for FY1996 results in suspending further activity in this task after April 1996.

Transfer of on Copy of MGA to Westinghouse Hanford *William Buckley and Wayne Ruhter*

One copy of the LLNL-developed MGA plutonium analysis software has been transferred, with the concurrence of DOE, to Westinghouse Hanford. This software will be applied to samples in plutonium storage activities. This work was paid for under the Development of Advanced Isotopic Analysis Software task.

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

<u>B&R No.</u>	<u>Funding</u>	<u>Obligated</u>
GD060402	\$175K	\$162K

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 up various geometries and transporting the gamma-rays of a known source through the material to a detector. Monte Carlo calculations may be used to calculate plutonium "standard" gamma-ray spectra that may be used to determine such characteristics as systematic biases in spectral data-analysis codes. With so many possible variations of the problems described above, the simulation of gamma-ray spectra from them is more efficient and cost effective than the development and measurement of various reference materials.

Simplification of the Monte Carlo Calculation of Gamma-Ray Spectra

Tzu-Fang Wang

We have completed the first step in integrating our gamma-ray simulation methodology in a software package, the "SYNERGY" suite. We have developed a graphical interface for the code GAMGEN, using the Tcl/Tk tool for the UNIX and PC platforms. A draft report has been completed entitled "Preliminary Report on the Usage of SYNERGY - a Monte Carlo Gamma-Ray synthesizing Suite for Transuranium Isotopes". This report contains a user guide to the suite and PC executables of GAMGEN and POSGL software with sample input files and output files on a floppy disk.

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

<u>B&R No.</u>	<u>Funding</u>	<u>Obligated</u>
GD060402	\$75K	\$76K

This task began in May 1996 with year-end startup funds. The previous concept development and proof-of-principle demonstration for this task have been 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. To test this hypothesis we propose to apply our algorithm to measurements of gamma-rays from nuclear material samples of interest to materials control and nonproliferation. We will test the effectiveness of the algorithm and optimize the algorithm parameters. We will implement our algorithm with a digital signal processor in order to perform the Compton suppression in real time. If successful, this work could lead to improved techniques for materials assay. When used with cryo-cooled HPGe detectors, our signal processing system and algorithm would enhance capabilities for remote assays.

Signal Processing

Dean Beckedahl and Judith Kammeraad

During the past five months we procured hardware needed for the real-time processing system and implemented a test circuit that does not contain a detector, but is otherwise fully functional for software development and testing the feasibility of real-time analysis. The test circuit and data acquisition computer have been used to process signals in real time at a rate of 100 Hz (with 9% dead time), and a rate of 1000 Hz (with 50% dead time). The dead time results from the processing time of the waveform recorder (faster waveform recorders are available). Other components of the system, including the signal processing algorithm, do not limit the count rate. Thus we have demonstrated the feasibility of performing the signal processing in real time.

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

<u>B&R No.</u>	<u>Funding</u>	<u>Obligated</u>
GD060404	\$25K	\$21K

The objective of this proposal is to provide NN-513.4 with a quality 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

A tentative schedule has been laid out leading to publication of the report in January 1997. A call for papers and instructions for their preparation have been made with the points-of-contact for the projects identified by the Planning and Technology Development Branch. A draft layout for the report has been developed, including a cover design and format for articles that will be included in the report.

VII. Other Related Activities

Eugene Henry, Winifred Parker, and M. N. Namboodiri are working with the AVLIS program on evaluation of non-destructive analysis methods for the assay of feed, product, and tails streams in a uranium enrichment plant.

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

I. Development of Advanced Isotopic Analysis Software

B&R No. GD060402

Continue development of MGA++, demonstration of integrated capabilities on test spectra completed 4/96.

Conclude development phase of MGA-like code for analyzing uranium spectra--prototype test program available 5/96, draft report completed 9/96.

Peak shape fitting methodology for CdZnTe spectra--concluded 5/96, draft report completed 9/96.

Design and integrate a graphical interface for developers, analysts, and users of MGA++ -- began 12/95.

II. Emission/Transmission Computed Tomography

B&R No. GD060402

Continue studies and analyses of layered and shielded SNM materials to optimize measurement parameters--Studies of the MSE button are delayed because of DOE/OAK approval has not been completed. The milestone, a report on a digitized map of Pu MSE button anticipated by 9/96 has not been concluded, pending DOE/OAK approvals. Approximately two months will be needed to complete a scan once operation is approved.

Use software assessment to begin development necessary to convert CT data into isotopic information--prototype software completed 2/96.

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

B&R No. GD060402

One copy of LLNL MGA has been transferred to Westinghouse Hanford for use in an EG&G Ortec system for plutonium storage.

Evaluation and testing of MGA analyses of plutonium samples in DOE-approved thick steel containers -- testing complete 3/96, report completed 8/96.

Implementation of MGA-like U235 program for analysis of uranium isotopes and uranium enrichment-- testing began 2/96, report completed 9/96.

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

B&R No. GD060402

Report summarizing the calculation of Pu spectra for selected heterogeneous materials – draft report completed 9/96.

A public library of simulated SNM spectra, and a manual on how to calculate these spectra – draft manual completed 9/96.

Implementation of MGA-like U235 program for analysis of uranium isotopes and uranium enrichment– testing began 2/96, report completed 9/96.

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

B&R No. GD60402

Assemble demonstration hardware; purchase digital signal processor–completed 9/96.

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

B&R No. GD60404

Start process leading to publication of OSS Technology Development report–completed 9/96.

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

"Using MGA to Analyze Pu Spectra Acquired with Thick Absorbers", Kenneth Raschke, and Eugene A. Henry, August 1996, STP961.

"Testing of the U235 Software: Analysis of Selected ²³⁵U Samples", DeLynn Clark, Kenneth Raschke, and Eugene A. Henry, September 1996, STP962.

"Status Report on Development of a Compton-Suppression Method using Signal Processing Techniques", J. Kammeraad, D. Beckedahl, J. Blair, and W. Payne, September 1996, STP963.

Safeguards and Material Accountability

**R. Scott Strait, Associate Program Leader
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. 2.0.3 installed at 10 of 11 operations offices and acceptance tested at 9.
- DISS Rel. 2.1 released to beta testing including additional functionality requested 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)

<u>B&R No.</u>	<u>Funding</u>	<u>Obligated</u>
GH-03	\$4,200K	\$4,129K
GH-03 carryover	\$ 895K	\$ 895K

These projects are modernizing the DOE Integrated Safeguards and Security (DISS) personnel security network and databases. They are part of an overall plan to modernize the computer systems of the OSS in order to form an integrated solution for the organization's needs. The product of this project will be a complex-wide system which incorporates modern software design and allows for easy enhancements, low maintenance costs, and growth in functionality. It will provide an integrated system for the electronic transfer of personnel security data between the DOE and the Office of Personnel Management (OPM) and between DOE Operations Offices. The modernized DISS will include most of the functionality provided by independent systems currently operated by many Operations Offices. The project uses existing hardware and software to the extent possible.

DISS Release 2.0.3 is completed and has been installed and acceptance tested at OAK, SR, RL, SNR, AL, PNR, HQ, NV, and OR and their contractor facilities. The system has been installed at ID and is awaiting acceptance testing. RF will be installed in October. The system did have several specification exceptions and problems, all of which are being addressed in subsequent bug fixes or formal releases. The Release 2.1 centralized personnel security database (PSDB) has been released to beta testing.

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	DOE HQ production approval received.
Admin Client	1.0.2	DOE HQ production approval received.
Notary	2.05	
RPS/OPM Unix software	Build_2_0_2	

Deployment/Operations Support

Although operations support for deployed sites has consistently exceeded the planned level designated for these activities, the LLNL design staff has made necessary adjustments. Multiple, parallel deployment, operations, and design activities are still frequently placed in competition for limited design team resources, sometimes necessitating weekly or even daily reprioritization of directed support. This will hopefully ease with the completion of R2.0 deployment activities, especially if R2.0 deployment can complete before R2.1 deployment starts up in earnest.

The DISS team continues to perform daily direct monitoring of the OPM gateway to insure correct production operations.

Maintenance activities continue on various components of DISS Release 2.0. These include the Unix utilities with bug fixes to Validator error messages, and various patches to improve and streamline the RPS database installation.

Release 2.1 Development

- **CDUI 2.1 (WBS#2.2.1):**

CDUI 2.1 represents an interim software release of the CDUI application that include some of the items that were originally deferred in order to meet Release 2.0 delivery deadlines. The CDUI 2.1 incorporates bug fixes that include items of concern to Schenectady, namely bugs that would allow data to be inadvertently saved from read-only mode if printing or validator functions were selected, improvement in local office search function and contractor access to requests. The CDUI 2.1 also includes functions that permit viewing and printing of scanned documents stored in the RPS database as part of the Clearance Request packet items.

DCUI 2.1 has successfully passed testing and is released to production pending approval from DOE HQ. The RPS Admin Client was upgraded to match the deployment DLL's contained with the CDUI installation package, and is also awaiting DOE HQ approval for release to production.

- **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 2.1b4. This version is currently in testing with release expected by October 18, 1996. This 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 2.1b4. This version is currently in testing with release expected by October 18, 1996. This will be the Release Candidate for DOE HQ acceptance testing.

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

The WDAC DP Client version 1.0b4 and WDAC Web Client interface v1.0b3 are currently in beta testing at DOE HQ.

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

The VADB Web interface v1.0b3 is in testing at LLNL with release to production expected by October 21, 1996. 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 1.03b.

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

VADB/CWAC support functions are in test at 1.0a6. 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 testing. Release to pre-production at selected sites is planned, with advance copies installed at HQ.

Release 2.1 Deployment

- **CPCI Data Sync**

Initial operation of the CPCI Data Sync utility is underway at DOE HQ. A member of the LLNL Data Management team was on-site to assist in the initial data load during the week of 9-16-96. This utility 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 personnel are working to assist OSS to identify existing DAVAC users and 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, 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 2.0 deployment, and/or VADB deployment, or as a separate tasking. CPCI can be installed on the same workstations as the CDUI application. CPCI will initially be pointed as a 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.

- **CWAC 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.

Release 3.0 Development

- **OPM Oracle Database**

A task is underway to develop the OPM Oracle database (part of R3.0 functionality) which will replace much of the current PEM data transmission with SQL*Net Secure Network Services, as well as providing a return channel for OPM investigation results.

- **Scanned Document Viewer - Notary replacement**

The scanned document viewer/binary image loader is under development. This is intended to provide a replacement for the current Notary. This capability has been previously identified as part of Release 3.0, but may be incorporated earlier, potentially as part of a new version of the CDUI.

A subset of the document viewer/printer functionality has been incorporated into CDUI 2.1.

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

<u>B&R No.</u>	<u>Funding</u>	<u>Obligated</u>
GD-05-08-03	\$300K	\$158K
GD-06-02-02	\$24K carryover	\$24K

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 this quarter, we focused on disseminating more detailed information about two aspects of our methodology for evaluating computerized material accountability (MA) systems against insider threats. The two aspects are

- i) the methodology model for quantitatively evaluating the desirability of different combinations of safeguards control options MA system planners could consider when implementing MA software applications for different system tasks
- ii) insights from applying the methodology concepts to local area network material accountability system prototypes (e.g., LANMAS)

The methodology model for evaluating safeguards options uses a multiattribute utility (MAU) function. Value judgment information is assessed to calibrate an MAU model which takes as input assigned levels for each of the methodology's six criteria (access controls, automated controls, human oversight, auditing scrutability, resolution and responsiveness). The MAU model produces as output a single number or utility suitable for logically comparing alternatives for a subsystem task. A specific numeric example was used to show the variety of ways a facility might achieve a high utility or assurance against the insider threat for a task without requiring every possible safeguards control to be implemented at its highest possible level.

We also described the methodology application to a LANMAS prototype implementation in terms of the methodology's six criteria. For each criterion, LANMAS features and implementation options reflecting client-server system safeguards concerns were discussed. These concerns covered topics such as Trojan horses, source code and core procedure modifications, decentralized customized report writing, and the possibilities of proactive automated-assisted triggering of audits.

Both aspects discussed above along with an overview of the methodology were documented in a paper for the Institute of Nuclear Materials Management's (INMM) 37th annual meeting held in Naples, Florida on July 28 to August 1. A talk based on the paper was presented at the conference and copies of the paper were sent to attendees associated with the LANMAS effort at Los Alamos and other facilities looking at local area network material accountability systems.

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

<u>B&R No.</u>	<u>Funding</u>	<u>Obligated</u>
GD 06-04-01	\$73K	\$31K

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 placed a contract with TESA for modification of the CT-20 to

meet DOE requirements. TESA is committed to delivering these modifications by the end of October. We have submitted a revised project lifecycle plan for OSS approval with our recommendations to pursue modifying the CT-20 rather than design and build an original system.

SMA APPENDIX A: SUMMARY OF MILESTONES AND DELIVERABLES FOR THIS QUARTER

I. DISS Personnel Security Network and Databases Modernization

B&R No. **GH-03**

<u>Date</u>	<u>Implementation Milestones</u>	<u>Status</u>
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	Installation completed 10/3/96
7/29/96	Begin RF Acceptance Test	Configuration underway 10/14/96
8/19/96	Begin PNR Acceptance Test	Complete

<u>Date</u>	<u>Development Milestones</u>	<u>Status</u>
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	One-way 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	Pre-production release
4/30/96	Standalone centralized system ready for deployment	Beta - awaiting start of DOE HQ acceptance testing
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

<u>Date</u>	<u>Milestone or Deliverable</u>	<u>Status</u>
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

<u>Date</u>	<u>Milestone or Deliverable</u>	<u>Status</u>
10/31/95	First level project review	12/7/95 with Darryl Toms
4/30/96	Mechanical and electrical design drawings	TESA contract placed. Delivery expected 10/31/96

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

Jones, E. and Sicherman, A., "Assessing the Integrity of Local Area Network Materials Accountability Systems Against Insider Threats", Lawrence Livermore National Laboratory, Livermore, CA, UCRL-JC-123327, presented at 37th Annual Meeting, Institute of Nuclear Materials Management on July 28-August 1, 1996.

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 and 7 cases, where cases are incidents that involve more than one DOE site. These incidents and cases generated 38 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 also created a new incident tracking system that will be in use starting Oct. 1st.

The team responded to numerous viruses: Concept, Good Times (the hoax continues to pop up), WAZZU, and PKZIP300V. While PKZIP300 is a real Trojan program, it has not been seen for quite some time, but the warning about the Trojan is starting to take on urban legend status. Intrusion attempts via the Internet continue. CIAC handled incidents involving ftp, e-mail spamming, SATAN scans, suspicious port scans and finger requests, and unauthorized Telnet attempts.

CIAC actively participated in and supported the following conferences and seminars: Marcey Kelly attended a Windows NT Seminar, John Fisher attended the Information Security Officer's Forum, Sandy Sparks attended the DOE Information Warfare Workshop, the 13th Office Information Technology Conference where she presented information on computer security, and the Forum of Incident Response and Security Teams Conference. Bill Orvis delivered the presentation "Computer Virus Operation and New Directions" from the DOE Computer Security Group Training Conference to Sandia security personnel and two groups at LLNL.

II. Network Intrusion Detector (NID)

We developed a graphical user interface that integrated packet capture, analysis, and playback. The ability to switch between capture modes in real-time was also added. To validate the system, we included automated tests to exercise all of the back-end tools and their options.

III. AIS Alarm Project

The LANL/LLNL/SNL team completed the Alarms Functional Design Document and Interface Control Documents for its functional subsystems. LLNL supplied the source code for multiple sensors and the communications interface in a complete development framework. With contributions from the other labs, we continued development of the Phase 0 Alarms system and demonstrated its operation from intrusion detection sensors through assessment and response.

IV. Security Profile Inspector for UNIX and VMS Operating Systems (SPI/UV)

This quarter marks the close of the successful SPI project. The SPI team conducted a DOE Computer Security Tools Usage Survey to assess the degree and effectiveness of information security tools and technologies in use by DOE computer system administrators. Progress continued in SPI/SPI-NET Technology Transfer efforts.

V. Profiling and Vulnerability Analysis Project (VAP)

We continued to load the database with known vulnerabilities and intrusion methods. There are currently 74 vulnerabilities and 70 intrusion methods detailed in the database.

The secure web server has arrived and is being installed. As soon as it is available, we will implement the connection between an Oracle database and the server, test the connection, move the database to the Oracle server and make it available to select outside users.

VI. DOE Information Security (DOE-IS) Server

We continued to populate the server as an ongoing activity. Highlights include: the conference papers for the DOE Computer Security Group Training Conference, a page of computer use policies from several hundred organizations, and the User Needs survey pages.

This quarter we created a special project area on the server to use for the User Needs survey and the AIS Alarm Project. This special access area allows multi-site projects to share their administrative data and to coordinate their projects.

Two other groups are now using special access areas on the server: Advice and Assurance (A&A) and National INFOSEC Technical Baseline (NTTB).

TASK DESCRIPTION AND QUARTERLY PROGRESS

I. Computer Incident Advisory Capability (CIAC)

<u>B&R No.</u>	<u>Funding</u>	<u>Obligated</u>
GD060603	\$444K	\$444K

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: Marcey Kelly attended a Windows NT Seminar, John Fisher attended the Information Security Officer's Forum, Sandy Sparks attended the DOE Information Warfare Workshop, the 13th Office Information Technology Conference where she presented information on computer security, and the Forum of Incident Response and Security Teams Conference. Bill Orvis delivered the presentation "Computer Virus Operation and New Directions" from the DOE Computer Security Group Training Conference to Sandia security personnel and two groups at LLNL.

II. Network Intrusion Detector (NID)

<u>B&R No.</u>	<u>Funding</u>	<u>Obligated</u>
GD060403	\$263K	\$250K

We completed the graphical user interface (GUI) and ramp-up milestones this quarter. The GUI integrated packet capture, analysis, and playback using Tcl/Tk by combining the tools developed earlier this year and then supplying any missing functionality. For automated ramp-up, iWatch begins saving packets upon recognition of a user-supplied threat signature. In addition, in real-time, an end user may also switch between capture modes while using iNid.

Automated tests now exercise all of the back-end tools and their options to check their output against verified test data. This check is available to both developers and end users who only have a binary release.

III. AIS Alarm Project

<u>B&R No.</u>	<u>Funding</u>	<u>Obligated</u>
GD060403	\$500K	\$441K

LLNL completed its two Alarms milestones for this quarter. In concert with SNL and LANL, we completed the Phase 0 Functional Design Specifications and merged sensor components into the Integrated Release 0.0 prototype software. In addition, LLNL developed Interface Control Documents describing the message formats allowed between sensors and assessment components.

We developed three sensors for the initial prototype to span the three phases of a network attack. For the attack preparation phase, the Gabriel sensor detects SATAN scans of a host's network ports. In the second phase, entry, a hacker attempting to log in to a trapped account with an easily guessed password (a Joe account), will alert the central assessment component. If the intruder actually modifies selected files in the third exploitation phase, the Odo sensor will detect the change using MD5 checksums.

These sensors were updated and merged into the integrated source and tested from detection through assessment and response. Real-time results are displayed in a test graphical user interface developed by Sandia and in the prototype Netscape Java interface developed by LANL. This source code is now version controlled using DES-secured CVS on the Internet between the three sites.

IV. Security Profile Inspector for UNDX and VMS Operating Systems (SPI/UV)

<u>B&R No.</u>	<u>Funding</u>	<u>Obligated</u>
GD060503	\$222K	\$222K

This quarter marks the close of the successful SPI project. The SPI team conducted a DOE Computer Security Tools Usage Survey in September. This survey, announced at the DOE Computer Security Group Training Conference in Seattle, sampled scores of computer system administrators at the major DOE sites, to assess the degree to which various computer security tools and technologies are deployed and utilized throughout the DOE, and to gauge their perceived effectiveness.

In the SPI Technology Transfer effort, negotiations with several firms that have expressed interest in commercialization continue. According to the LLNL Technology Transfer Office, the first of several non-exclusive licenses will be awarded around December, 1996.

V. Profiling and Vulnerability Analysis Project (VAP)

<u>B&R No.</u>	<u>Funding</u>	<u>Obligated</u>
GD060503	\$222K	\$221K

We are continuing to load the database and currently have 74 vulnerabilities and 70 intrusion methods detailed.

We have designed the external access around a Netscape Enterprise server linked to an Oracle database. Sessions will use the Secure Sockets Layer (SSL) encryption mechanism to give the link end-to-end protection. DOE access to the database will be granted by a local site CFPD who will have the authority to add a user name and password to the system.

The Netscape Enterprise server has arrived and we are currently installing it. Once installed, we will build the connections between the server and an Oracle database. The database will eventually hold the VAP data. When the secure web server is in place and connected to the database, we will test the connection and then move the VAP database to the Oracle server and make it available.

VI. DOE Information Security (DOE-IS) Server

<u>B&R No.</u>	<u>Funding</u>	<u>Obligated</u>
GD060503	\$150K	\$150K

We continue to add new and updated information to the server. New items this quarter include the conference papers of the DOE Computer Security Group Training Conference, a page of computer use policies from several hundred organizations, and the User Needs survey pages.

The special access areas we started last quarter are starting to interest more groups. Using a combination of a web server and the secure shell connection protocol, we give a project a protected area to work in that is convenient to access from any platform attached to the Internet. Each special area is *chrooted* into its own area of the file system, and is not given access to any files outside of that special area. Users with a need to write to the special area must use secure shell (SSH) to make the connection. Authentication is cryptographic in nature and the link is encrypted, making it very difficult for intruders to intercept the data or to spoof the link. People who need read access to the special area use a web browser. Web access to directories in the special areas can be either public or restricted to people with a particular user name/password.

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

I. Computer Incident Advisory Capability (CIAC)

B&R No. GD060603

Issued 20 Bulletins/Advisories:

- G-29: dip Program Vulnerability
- G-30: DEC Software Security Kits
- G-31: FreeBSD Security Vulnerability (ppp, rdist, rz)
- G-32: HP-UX Vulnerabilities in expreserve, rpc.pcnfsd, rpc.statd
- G-33: rdist Vulnerability
- G-34: HP-UX Vulnerabilities (netttune, SAM remote admin)
- G-35: SUN Microsystems Solaris vold Vulnerability
- G-36: HP-UX Vulnerabilities in elm and rdist Programs
- G-37: Vulnerability in Adobe FrameMaker (fm_fls)
- G-38: Linux Vulnerabilities in mount and umount Programs
- G-39: Vulnerability in expreserve
- G-40: SGI admin and user Program Vulnerabilities
- G-41: Vulnerability in BASH Program
- G-42: Vulnerability in WorkMan Program
- G-43: Vulnerabilities in Sendmail
- G-44: SCO Unix Vulnerability
- G-45: Vulnerability in HP VUE
- G-46: Vulnerabilities in Transarc DCE and DFS
- G-47: Unix FLEXlm Vulnerabilities
- G-48: TCP SYN Flooding and IP Spoofing Attacks

Reissued CIAC 2301, the Virus Update document.

II. Network Intrusion Detector (NID)

B&R No. GD060403

Completed the graphical user interface (GUI) and ramp-up milestones this quarter.

III. AIS Alarm Project

B&R No. GD060403

Completed two milestones this quarter. In concert with SNL and LANL, we completed the Phase 0 Functional Design Specifications and merged sensor components into the Integrated Release 0.0 prototype software.

IV. Security Profile Inspector for UNIX and VMS Operating Systems (SPI/UV)

B&R No. GD060403

Completed the DOE Computer Security Tools Usage Survey milestone this quarter.

V. Profiling and Vulnerability Analysis Project (VAP)

B&R No. GD060403

Completed the milestone to have a populated database in place this quarter.

VI. DOE Information Security (DOE-IS) Server

B&R No. GD060403

No milestones or deliverables to report for this quarter.

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

None.

Complex Wide Access Control (CWAC) Project Safeguards Technology Program

Dan Johnson, Principal Investigator

INTRODUCTION

The purpose of this project is to develop an approach that will allow visitors to use their DOE standard badge in access control systems throughout the DOE complex. The overall goals include:

- Define the interfaces and develop the standards necessary to implement access control on a DOE complex-wide basis.
- Demonstrate the enrollment (registration) of a standard badge at one site and the use of that badge in the access control system of another site.
- Develop a hardware/software system (enrollment station) that will allow any site to create and enroll (register) access control data in the central CPCI data base for use by the site or any other site.

SUMMARY OF MAJOR ACCOMPLISHMENTS

1. Completed development and formal software QA testing of CWAC software for the stand-alone enrollment/verification station. This software provides the capability to enroll people, badges, PINs, and biometrics in the Visitor Access Data Base.
2. Coordinated with DOE-OAK personnel regarding CWAC E/VS installation, and completed system installation at the Oakland Federal Building.

TASK DESCRIPTIONS AND QUARTERLY PROGRESS

Accomplishments achieved during the third quarter of FY 96 are described below:

<u>B&R No.</u>	<u>Funding</u>	<u>Obligated</u>
GD 060501	477K	453K

- I. **Complete remaining procurement and assemble three CWAC enrollment/verification stations, one for development at LLNL, and two more for deployment at DOE-Oakland and DOE-HQ.**

Quarterly Progress: Complete. All enrollment stations have been procured and assembled. After discussions at DOE Germantown in July with personnel responsible for the DOE Germantown badge enrollment system, we have ordered a 2' x 2' scale to replace the 4' x 4' scale originally specified. This is due to space limitations in the room reserved at DOE Germantown for the CWAC Enrollment/Verification Station.

- II. **Modify Argus encoding/enrollment software for use as a CWAC enrollment/verification station with the ability to encode DOE Standard Badges, communicate enrollment information with the VADB, and verify visitor identity and access control information.**

Quarterly Progress: Complete. We previously demonstrated the ability to encode badges, communicate with a developmental version of the VADB to enroll badges and biometrics, and retrieve information for identity verification. We also demonstrated the ability to enroll badge and biometrics information for a worker with a standard badge that was encoded by another system, which is required for locations such as DOE HQ, where badges have been encoded but not enrolled in VADB.

We completed implementation of a transaction file for enrollment data. If the connection to VADB is lost, enrollment transactions can be logged to a file for later playback when VADB communication is re-established.

The ability to update and maintain badge status information has also been provided. When complex wide access control is implemented, there must be a means of keeping the badge status information current in VADB. Since this capability will not be provided by a VADB end-user client, as first expected, this functionality has been implemented in the enrollment/verification station.

A comprehensive test procedure was developed to exercise enrollment and verification functions with and without VADB, with DOE standard badges and LLNL format badges, for different enrollment stations configurations. This test procedure has been successfully completed for the stand-alone enrollment/verification station.

- III. Develop the software required for the LLNL Argus ACS to communicate with the VADB. Demonstrate the ability to extract access control data from the VADB to facilitate visitor passage through the LLNL Argus ACS. Work with SNL to provide interface requirements for commercial ACS systems.**

Quarterly Progress: The software required for the Argus to communicate with the VADB has been developed and successfully demonstrated between the LLNL Argus Test System and a developmental version of the VADB operating on the LLNL Open LabNet. This software is being modified to ensure compatible operation with other Argus software processes which are being revised to merge Argus ACS and IDS configuration and communication functions. A formal test procedure has been prepared, and QA testing of this software should be initiated in October.

A firewall has been designed and installed to ensure appropriate security is provided for connection of the LLNL Argus production system to DOEBINET or the Internet. This firewall will ensure that only VADB processors are allowed to communicate with the Argus processors, and that all other attempts to connect to Argus processors will be precluded. The firewall connection between the Argus Test system and the developmental VADB system has been successfully demonstrated. The computer security plan for the LLNL Argus production system has been updated to reflect the addition of the firewall, and we are documenting the firewall test results and the firewall configuration. All of these must be approved before the firewall will be allowed to connect to the LLNL Argus production system.

- IV. Provide installation requirements, support installation, test and activate an enrollment/verification station at DOE-Oakland. Demonstrate the ability of the enrollment/verification station to collect enrollment and access control information and transmit it to the VADB, using Oracle SQL*Net client software. Develop and provide enrollment operator training.**

Quarterly Progress: Equipment layouts were provided to DOE-OAK personnel to establish the location of CWAC E/VS hardware. We provided an integrated layout which optimized location of the DOE-OAK badge production hardware in conjunction with the CWAC E/VS hardware. Information was provided to DOE-OAK to allow installation of the enrollment enclosure, conduit, electrical power, and data connections. This is all complete.

The installation of enrollment station hardware, consisting of operator workstation, RAP, hand geometry unit, and scales has been completed.

In preparation for operator training at DOE-OAK and DOE Germantown, Argus Enrollment Operator Training has been updated to reflect the new functions added to support CWAC.

V. Provide support for bug fixes and requested software enhancements for DOE-Oakland enrollment/verification station.

Quarterly Progress: No activity this quarter, since the DOE Oak enrollment verification station is not yet operational. However, we have used personnel files provided by DOE-OAK to pre-load pre-enrollment records for individuals that are to be enrolled. This will relieve the operator of the time-consuming and error-prone chore of entering enrollment data such as badge serial number, name, SSN, clearance level, contractor, user identification number, etc. It is intended that this same approach will be used at DOE Germantown.

VI. Provide Standard Badge policy and procedure support. Identify policy and procedure issues which hinder effective implementation of CWAC concepts, research solution alternatives, and develop policy/procedure recommendations.

Quarterly Progress: At the request of Darryl Toms, we provided a presentation to attendees at an ASQP meeting on the importance of the DES key encoded on the standard badge, and outlined restrictions regarding how the DES key should be generated and implemented. We have recommended that this information be included in the next issue of the DOE Standard Badge Functional Requirements Document.

VII. 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, and quad chart updates.

Quarterly Progress: A status update for the CWAC project was presented at a video teleconference held with NN-51 personnel on September 20, 1996.

A CWAC Quad chart was prepared at the request of NN-513.4. This Quad chart summarizes the CWAC project objectives, and FY97/98 funding and major tasks.

Project change proposals were prepared and submitted related to milestones impacted by VADB non-availability and resource shortages.

A revised Life Cycle Plan was prepared and submitted to propose scope changes related to FY97 funding reductions.

In collaboration with NN-51 personnel, we prepared and presented a paper at the July meeting of the Institute of Nuclear Materials Management. The paper described DOE's ongoing efforts to improve physical and personnel security by a careful implementation of DOE Standard Badges, computer databases, and networks of automated access control systems at DOE facilities.

VIII. Complete installation preparation, support installation, and activate an enrollment/verification station at DOE-HQ. Provide enrollment operator training.

Quarterly Progress: Installation requirements were prepared and transmitted to DOE HQ. We visited DOE Germantown in early July to survey the candidate installation site and provided recommendations regarding revising the current equipment arrangement and installing the CWAC equipment.

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

MILESTONES STATUS TABLE

**Milestone
Date**

Description of Milestone

Status

8/15/96	CWAC enrollment station installed at DOE-Oakland (but not tested)	Complete
7/31/96	After production VADB is operational, install ACS/VADB software on LLNL Argus production ACS	CWAC Change Proposals* 4 and 5 submitted to change date to 11/15/96 due to VADB being in beta test
7/30/96	At DOE-OAK, enroll individual in VADB; demonstrate visitor passage through CAIN booth at LLNL	CWAC Change Proposals* 4 and 5 submitted to change date to 11/20/96 due to VADB being in beta test

* Change Proposal 4: LLNL FESSP Letter 96-0725, dated 7/22/96
Change Proposal 5: LLNL FESSP Letter 96-0862, dated 9/25/96

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

UCRL-JC-124698, DOE's Nation-Wide System for Access Control Can Solve Problems for the Federal Government, Samuel Callahan & Darryl Toms - US DOE, Gregory Davis, Daniel Johnson, and Scott Strait - LLNL, July 1996

Standardization of Security Systems

Greg Davis, Program Manager

INTRODUCTION

The purpose of this project is to support the standardization of security systems in the Department Of Energy to meet DOE orders and requirements, and also to support the DOE in offering relevant security technology and capabilities to Federal standardization efforts.

SUMMARY OF MAJOR ACCOMPLISHMENTS AND ISSUES

- I. Presentation of "Evolving a Mature System with New Technologies" presentation for a CTA Interactive Television class held July 18, 1996
- II. Presentation of paper "DOE's Nation-Wide system for Access Control Can Solve Problems for the Federal Government" for presentation at the 37th Annual INMM Conference.
- III. The Argus Homepage continued operation. It operated without problems throughout the quarter with secure sockets and secure registration enabled. There were no enhancements over the period, however, new user requests were evaluated and implemented.
- IV. The "Standardization of Security Systems" task has been completed

TASK DESCRIPTIONS AND QUARTERLY PROGRESS

<u>B&R No.</u>	<u>Funding</u>	<u>Obligated</u>	
GD 06 0201	\$100K	\$99.4K	as of 9/30/96

Participation in CTA class

A presentation was made at the CTA Interactive Television class held on July 18, 1996 in Albuquerque N.M. titled "Emerging Technologies". The presentation given was titled "Evolving a Mature System with New Technologies". Information was presented about the new technologies developed for the DOE Integrated Safeguards and Security system and the Complex-Wide Access Control system and how they are being integrated into DOE's Argus system. CTA reports that the presentation was well attended by security personnel across the DOE complex.

Presentation of Paper at INMM conference

A paper was submitted for publishing in the proceedings, and a presentation given at the 37th annual INMM conference in Naples, Florida on July 27, 1996. The paper and presentation were titled "DOE's Nation-Wide System for Access Control Can Solve Problems for the Federal Government". The paper outlined DOE's creation of the DOE Integrated Safeguards and Security system and the Complex-Wide Access Control system and suggests that access control challenges facing the federal government might be addressed by systems analysis and tools available from the Department of Energy. Ten copies each were sent to co-authors Darryl Toms and Sam Callahan of OSS.

Argus Homepage

The Argus homepage continued to operate (24 hours a day, 7 days a week) in secure mode throughout the 4th quarter. We have continued to receive and honor requests for access throughout the quarter. There have been approximately 230 visits to the webpage in the last quarter. No new features were added or updated made to the homepage this quarter.

We have received requests from multiple sites to continue to update information on the Argus homepage. In particular sites have requested that the latest documents be converted to PDF format and made downloadable from the webpage, and that the latest "Tech Notes" be added. There has also been a request for access to the System Performance (SPR) database through the web. We believe that the first two requests should be honored immediately, but have security concerns regarding the third.

This Task is Complete

The "Standardization of Security Systems" task is complete. All required tasks have been successfully completed approximately on schedule and within budget. It has been a pleasure and an honor to work with DOE's Office of Safeguards and Security on these tasks.

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

**MILESTONE & DELIVERABLE
STATUS TABLE**

Original Deliverable	Description of Deliverable	M/D	Status
12/1/95	Argus Internet Homepage with user registration required	D	Complete
2/14/96	Presentation to and report on Argus Advisory group meeting	D	Complete
3/9/96	Draft report on DOE contribution to the Federal Standardization of electronic security systems	M	Complete
5/1/96	Report on DOE contribution to the Federal Standardization of electronic security systems	D	Complete
6/30/95	Demonstration of DOE's electronic security systems concepts	D	Complete
7/10/96	Presentation of paper at the INMM's physical protection section.	D	Complete
7/18/96	Presentation at CTA ITV Course on "Emerging Technologies"	D	Complete
9/1/96	Argus Advisory Group meeting support	M	Complete
9/13/95	Host DOE community at an Argus Technical Interchange Meeting	D	Complete

M=Milestone
D=Deliverable

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

UCRL-JC-124698 "DOE's Nation-Wide System for Access Control Can Solve Problems for the Federal Government".

Presentation at the 37th annual INMM meeting in Naples Florida titled "DOE's Nation-Wide System for Access Control Can Solve Problems for the Federal Government".

Presentation at the July 18, 1996 CTA ITV class on emerging technologies titled "Evolving a Mature System with New Technologies".