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

Quarter Ending December 31, 1995

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

RECEIVED

APR 18 1996

OSTI

January 1996

DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED 85

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 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.

**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 December 31, 1995

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

January 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. NDA MC&A Measurement Technology R&D.....	STP-2
II. Emission/Transmission Computed Tomography.....	STP-3
III. Support to DOE Facilities in Implementation, Testing and Evaluation of LLNL Developed NDA Techniques.....	STP-4
IV. Monte Carlo Calculations of Gamma- Ray Spectra	STP-5
V. Other Related Activities.....	STP-6
Appendix A: Summary of all Milestones and Deliverables for This Quarter.....	STP-7
Appendix B: A List of all Publications Produced During This Quarter.....	STP-7
 Safeguards and Decision Support.....	 SDS-1
Introduction.....	SDS-1
Summary of Major Accomplishments.....	SDS-1
Task Descriptions and Quarterly Progress.....	SDS-2
I. DISS - Electronic Transfer of Personnel Security and Personnel Security Database Modernization Technology Development.....	SDS-2

II. Risk Based Evaluation of Computerized Nuclear Materials Accountability Systems.....	SDS-7
III. Z-Lock Electro-Mechanical Lock for Administrative Control LLNL-438.....	SDS-8
Appendix A: Summary of all Milestones and Deliverables for This Quarter.....	SDS-9
Appendix B: A List of all Publications Produced During This Quarter.....	SDS-12
Computer Security - Distributed Systems	CST-1
Introduction.....	CST-1
Summary of Major Accomplishments.....	CST-1
Task Description and Quarterly Progress.....	CST-4
I. Computer Incident Advisory Capability (CIAC).....	CST-4
II. Network Intrusion Detector (NID).....	CST-4
III. Security Profile Inspector for Unix and VMS Operating Systems (SPI/UV).....	CST-5
IV. Network Security Gateway (Firewall) Process and Tool Development.....	CST-5
V. Profiling and Vulnerability Analysis Project (VAP).....	CST-6
VI. DOE Information Security (DOE-IS) Server	CST-7
VII. Distributed Auditing System (DAS)	CST-7
Appendix A: Summary of all Milestones and Deliverables for This Quarter.....	CST-8
Appendix B: A List of all Publications Produced During This Quarter.....	CST-11

Complex-Wide Access Control System	CWAC-1
Introduction	CWAC-1
Summary of Major Accomplishments.....	CWAC-1
Task Description and Quarterly Progress.....	CWAC-1
I. Complete remaining procurement and assemble three CWAC enrollment/verification stations, one for development at LLNL, and two more for deploy- ment at DOE-Oakland 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-Oakland	CWAC-3
V. Provide support for bug fixes and requested software enhancements for DOE-Oakland enrollment/verification station	CWAC-3
VI. Provide Standard Badge policy and procedure support	CWAC-3
VII. Provide project management support.....	CWAC-4
VIII. Complete installation preparation, support installation, and activate an enrollment/ verification station at DOE-HQ	CWAC-4
Appendix A: Summary of all Milestones and Deliverables for This Quarter.....	CWAC-5
Appendix B: A List of all Publications Produced During This Quarter.....	CWAC-5

Standardization of Security Systems	SSS-1
Introduction.....	SSS-1
Summary of Major Accomplishments.....	SSS-1
Task Description and Quarterly Progress.....	SSS-2
I. Argus Homepage	SSS-2
II. Standardization of Federal Systems	SSS-2
Appendix A: Summary of all Milestones and Deliverables for This Quarter.....	SSS-3
Appendix B: A List of all Publications Produced During This Quarter.....	SSS-3
 Information Technology Support	 ITS-1
Introduction.....	ITS-1
Summary of Major Accomplishments.....	ITS-1
Task Description and Quarterly Progress.....	ITS-2
Appendix A: Summary of all Milestones and Deliverables for This Quarter.....	ITS-3
Appendix B: A List of all Publications Produced During This Quarter.....	ITS-4

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 1996 (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 six areas:

- Safeguards Technology
- Safeguards and Decision Support
- Computer Security
- Complex-Wide Access Control
- Standardization of Security Systems
- Information Technology Support

The remainder of this report describes the activities in each of these six 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 six 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.

SUMMARY OF MAJOR ACCOMPLISHMENTS

I. NDA MC&A Measurement Technology R&D

- A prototype graphical user interface and graphics server which can call the MGA, MGA-hi, and U235 analysis methodologies is being tested.

II. Emission/Transmission Computed Tomography

- The image reconstruction code RECON has been ported to the PC-NT computer and is being tested.

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

- The uranium analysis code U235 has been tested on LLNL Materials Management samples.

IV. Monte Carlo Simulation of Gamma-Ray Spectra

- Simulations of uranium layers contaminated with plutonium via Monte Carlo techniques has provided useful information to LLNL Materials Management on these samples.

TASK DESCRIPTIONS AND QUARTERLY PROGRESS

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

I. NDA MC&A Measurement Technology R&D

<u>B&R No.</u>	<u>Funding</u>	<u>Obligated</u>
GD060402	\$350K	\$104K

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.

Second Generation Software

William M. Buckley, William Romine, DeLynn Clark, and Joseph B. Carlson

The MGA++ framework for all our second-generation intelligent analysis and instrument control software is being developed. Coding is underway that provides a concrete realization of the MGA++ architecture described by Buckley and Carlson. The early software consists of five separate modules in a Win32 environment: executive capable of selecting between the three analysis methodologies, the MGA, the MGA-hi, and the U235 analysis methodologies, and a graphical user interface facade and graphics server. The system accepts spectra selected by the user from a list of spectra available on disk, pre-screens the spectra to select the appropriate analysis method, and simultaneously displays the spectra graphically. The analysis is performed and the isotopics report is written to a separate application window. The pre-screen portion of the executive has been designed. The intelligent pre-screen, graphics, and the analysis methodologies can all be enhanced independently under this scheme.

The system is designed to provide flexibility. As an example, the method codes were developed in the UNIX or DOS environments and moved easily to run under Windows NT. This is an important step forward as it combines the familiar, productive tools traditionally used by analysts with the up to date operating system and graphics tools. This ease of use is not available in any currently available system such as Visual Basic, or the tightly coupled commercial solutions.

One of the design goals of these deliverables is easy interfacing with other software systems. This should help facilitate technology transfer. We are continuing

technology transfer discussions with the Laboratory's licensing agent and with several potential technology partners.

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 is operating and work is underway to improve the accuracy of the assay, particularly at the high (>90%) and low (<0.7%) enrichments. The test version of the program has been made operable as one of the analysis methodologies of MGA++.

Gamma-Ray Line Shapes from CdZnTe Detectors

M. N. Namboodiri, A. D. Lavietes, 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.

Several new CdZnTe detectors have now become available and spectra taken with these detectors are being analyzed, and the resulting shape parameters compared with the results for the 5mm x 5mm x 5mm detector. A prototype uranium analysis code for use with cadmium-zinc-telluride detectors was enhanced, and is being prepared for commercial licensing along with the CdZnTe detector system developed under a CRADA with EG&G Ortec. [The study of gamma-ray line shapes from CdZnTe detectors is supported in part by a CRADA with EG&G Ortec.]

II. Emission/Transmission Computed Tomography

<u>B&R No.</u>	<u>Funding</u>	<u>Obligated</u>
GD060402	\$150K	\$41K

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

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

Emission and Transmission Computed Tomography Application

Tzu-Fang Wang

We have simulated a worst case scenario to understand what could happen to a 350 gm sample of weapons grade Pu in a sealed 0.25 in. sealed stainless steel container during an uncontrollable disaster. This effort is necessary to qualify our sample as a sealed source and move it to our scanner under the Operational Safety Procedure for Building 331.

We are porting the image reconstruction code RECON to the PC-NT platform, and are planning to port the image slicing code VIEW to the same platform. With these codes on the PC-NT computer, all measurement and data analysis can be handled by the PC platform. This will eliminate the extra data handling step of acquiring data with the PC and transferring it to a UNIX system for analysis.

While awaiting the start of Pu scanning, we are acquiring data from 200 gm uranium samples shielded by lead with the scanner. The uranium enrichments range from less than 1% to about 7%, while the lead thickness is varied from 1 to 13 mm. These data are helpful in development of uranium analysis codes, and a spectral region around 700 keV may offer the possibility of uranium enrichment determination.

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

<u>B&R No.</u>	<u>Funding</u>	<u>Obligated</u>
GD060402	\$90K	\$15K

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.

Evaluation of Spectra for Plutonium in Thick Containers

Kenneth E. Raschke

We have received an inquiry about the use of MGA for the analysis of spectra obtained from plutonium contained in thick containers. We have made an extended series of measurements of shielded samples to assure that statistics are sufficient to make precision fits of the spectra. We are studying the performance of MGA and evaluating the fitting process as a function of parameters such as the slope of the background and the efficiency model determination.

Evaluation of Uranium Spectra

DeLynn Clark, and Kenneth E. Raschke

A number of spectra from LLNL Materials Management uranium samples have been acquired with the IAAS. These samples are typical of some those that have non-standard isotopic composition, unusual geometries, or other characteristics that can cause problems in isotopic determination. We are evaluating analysis methodologies that may deliver good uranium enrichment values for these samples. A test version of the U235 code is being applied to some of these spectra.

Support of Savannah River Program

Kenneth E. Raschke

The Savannah River Laboratory has an LLNL designed and provided analysis system to analyze for ^{238}Pu . We consulted with them about the failure of this system's detector to help devise corrective action.

IV. Monte Carlo Calculations of Gamma-Ray Spectra

<u>B&R No.</u>	<u>Funding</u>	<u>Obligated</u>
GD060402	\$175K	\$37K

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.

Simulation of SNM Spectra

Tzu-Fang Wang

We have successfully recompiled the utility codes for the ENDL Library to the PC-NT/Win95 platform. These utility codes can extract information (extrapolation, interpolation, division, polynomial expansion, etc.) from the ENDL Library and present it in a visual way. We are also implementing the updated MCNP-6 library on both our UNIX and PC platforms. This new library contains the photon-electron interaction for material with Z higher than plutonium. We need such a library to be able to simulate gamma-ray scattering in high americium material such as MSE buttons or MSE residual salt.

Monte Carlo Calculation of Heterogeneous Materials

Tzu-Fang Wang

We have started to simulate the gamma rays from a uranium sample contaminated with plutonium, in response to measurements of spectra by LLNL Materials Management. They are interested in determining if the plutonium gamma rays are from a surface contamination, are from plutonium on the "back" or "inner" surface of the uranium that can not be observed directly, or from plutonium of the "back" of the uranium that penetrate plutonium principally along cracks. Simulations of this problem build on our previous simulations of spectra from pure plutonium and uranium materials. Our simulations show that the plutonium gamma rays penetrate the uranium layer, not along cracks, and that the uranium is not too thick.

V. Other Related Activities

M. N. Namboodiri and Eugene A. Henry are co-organizers of the American Chemical Society Symposium entitled Nuclear and Isotopic Methods of Analysis for Safeguards and Security to be held in New Orleans in March 1996. A two day program has been developed that includes sessions on gamma-ray spectrometry, neutron analysis methodologies, mass spectrometric methodologies, and nuclear forensics.

Detector systems and analysis software developed previously and presently under the NDA R&D task were demonstrated at two workshops during this period: "Nuclear Smuggling: In-Field Analysis and Assessment", held in Los Alamos in October; and the "International Conference on Nuclear Smuggling Forensic Analysis", held in Livermore in November.

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

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

I. NDA MC&A Measurement Technology R&D

B&R No. GD060402

Begin design and integration of graphical user interface for developers, analysts, and users of MGA++ -- began 10/95.

II. Emission/Transmission Computed Tomography

B&R No. GD060402

Begin development of software necessary to convert CT data into isotopic information -- began 10/95

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

B&R No. GD060402

No milestones or deliverables for this quarter.

IV. Monte Carlo Calculations of Gamma-Ray Spectra

B&R No. GD060402

Begin development of the use of particle histories in Monte Carlo studies -- began 10/95

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

"Modification to the Klein-Nishina Cross Section for Ge Electrons at the High Statistics Limit", T. F. Wang, UCRL-ID-122484.

"Gamma-Ray Line Shapes from Cadmium Zinc Telluride Detectors: An Interim Report", M. N. Namboodiri, UCRL-JC-122451.

Safeguards and Decision Support

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

INTRODUCTION

The Fission Energy and Systems Safety Program (FESSP) Safeguards and Decision Support program area provides support to the DOE and other government sponsors in two related areas: (1) development and application of systems approaches for improving the security of nuclear and other critical facilities; and (2) decision analysis and risk management to support policy and decision making processes. The purpose of the program is to integrate advanced analytic methods with an understanding of technologies, economics, and the policy making process. We develop systematic approaches and analytic tools for enhancing the effectiveness of safeguards and security systems, including MC&A, physical protection, and personnel security. We transfer the technology developed through workshops and field consultations, and we evaluate available tools to determine their applicability to DOE safeguards and security interests. We also provide technical support to OSS on program planning, assessment and integration, and implications of arms control treaties.

SUMMARY OF MAJOR ACCOMPLISHMENTS

- DISS Rel. 2.0 in production at LLNL
- DISS Rel. 2.0 installed at SR and RL

TASK DESCRIPTIONS AND QUARTERLY PROGRESS

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

<u>B&R No.</u>	<u>Funding</u>	<u>Obligated</u>
GH-03	\$3,500K	\$1,118K

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 is completed and is now in production at DOE OAK and their LLNL and SNLL contractor facilities. The system did have several specification exceptions and problems, all of which are being addressed in subsequent bug fixes or formal releases. The specification exceptions are detailed in our letter of October 31, along with other problems and behavior characteristics of user significance, and suggestions for good user practices in using DISS Release 2.

The DISS Quality Panel met at Livermore on November 7-9. In conjunction with that meeting, SR, RL and AL representatives received user training and were able to perform system testing. These users were provided with the latest version of Release 2.0 for installation on their PCs to allow continued user testing against the DISS User Test RPS server from their home office.

Production at OAK

Training of the last DOE OAK, LLNL, and SNLL users was conducted October 10-12. Release 2.0 of the DISS system was deployed to DOE Oakland in November. Acceptance testing of the system began during the week of November 6, 1995. The system began production use on December 4, 1995. The current production release of DISS is the baseline DISS Release 2.0.1d. Version of components of this baseline are listed below. Release notes for 2.0.1d are still in preparation and will be made available at the earliest opportunity.

DISS Release 2.0.1d Baseline	
module	version
CDUI	2.0.1d
Admin Client	1.0 (Release Candidate)
Notary	2.05
RPS/OPM Unix software	Build_95
RPS Database	RPS_2_0_1d.tar

Implementation at SR

The Savannah River RPS system was deployed and configured with DISS Release 2.0.0. Due to the scheduled deployment at DOE OAK and the Quality Panel meeting, actual installation of the SR systems did occur until the week of November 13. User training was conducted at Savannah River during the weeks of November 27 and December 4, 1995. Savannah River acceptance testing has been rescheduled to the week of January 15, 1996. The Savannah River RPS system is planned to be upgraded from DISS Release 2.0.0. as configured at LLNL to the current production DISS Release 2.0.1d prior to the start of SR's acceptance testing.

Implementation at RL

The hardware for the Richland RPS server was received at LLNL and configured with server components of DISS Release 2.0.0. The hardware was shipped back to RL and received there during the week of December 4, 1995. RL technical staff had installed the system and it was up and working for LLNL and DynCorp personnel visit to RL during the week of December 11, 1995. Training for the Richland operations office is currently scheduled for the week of February 12, 1996, with acceptance testing the following week.

Implementation at NV

Nevada Operations Office's RPS hardware has not yet been delivered to LLNL. This hardware is currently scheduled to be configured at LLNL during the week of January 29, 1996. The Nevada RPS deployment will need to be rescheduled for at least one month later unless this hardware is received at LLNL by Friday, January 26, 1996.

Release 2.0 Maintenance

Maintenance and enhancements are continuing on the DISS Release 2.0 software suite. The new baseline was prepared and submitted to integration testing as Release 2.0.1d. Upon successful completion of testing, this upgrade will be ready for deployment to those sites that have not yet received an RPS system. This release is the first routine maintenance release of the DISS system. A "patch" to upgrade a site from R2.0.0 to R2.0.1d will be prepared. This patch will be made available to those sites choosing to upgrade.

The next maintenance baseline currently in development will be 2.0.2. This maintenance release will upgrade the CDUI to use the current versions of the Powerbuilder Dynamic Link Libraries (DLLs). This modification is expected to correct several printing problems in the CDUI and result in more stable overall operation due to enhanced memory management. DISS Release 2.0.2 is expected to be released to integration testing in the latter half of January, 1996.

The Identicator fingerprint software has not been able to meet our requirements for printing on two types of fingerprint stock. To overcome this we have procured new personal computers for OPM, each of which will drive a separate printer. Minor software changes were required.

The DISSCNVRT utility will be incorporated into the RPS/OPM Unix utility software. This utility will be used to convert old, existing data from legacy systems into the model used in the RPS databases from an intermediate format. The updated RPS utilities including DISSCNVRT were released to integration testing on January 12, 1996. DISSCNVRT will be initially released as a "patch" that may be applied to in-situ DISS Release 2.0.1d production systems. Thus, Operations offices that have 2.0.1d may apply the patch (or have it applied by the LLNL DMT) in order to use DISSCNVRT. This patch will also be incorporated into the next production release of the system (currently planned to be 2.0.2).

Our first help desk person from Sciencetech came on board. This person has been a member of the test team, and simply has a new title and new duties. A second help desk person is starting in January.

Release 2.1 Development

- PSDB standalone central server (WBS#2.2.2): An internal DISS design review was held for the PSDB standalone central server design. As a result of the review, the PSDB server design was placed into formal configuration management on October 31, 1995. Ongoing design changes to the PSDB server are documented in developer change requests for weekly database builds. Incremental changes to the PSDB standalone central server that are currently in the queue to support client software development will continue up to the week of January 22nd, at which time

the PSDB database design will be frozen in preparation for release to testing. Any additional requests for changes and/or new features will be deferred to production maintenance and new development following the DISS 2.1 production release.

As of this writing, the design definitions needed to support integration of unclassified SSIMS data into the PSDB database have not been received by the PNL designers. Therefor SSIMS connectivity cannot be included in DISS release 2.1 planned for April, and must be deferred to follow-on releases.

Clearance state transition diagrams for workflow processing in the CPCI application have been refined based upon comments stemming from the November Quality Panel and also from a detailed code review of the legacy CPCI COBOL program on the existing DISS mainframe.

- CPCI User Interface (WBS#2.2.2.5): The Software Design Description (SDD) which documents user interface to the Central Personnel Clearance Index (CPCI) segment of the PSDB server has been written. The design utilizes the same internal inheritance structure as the current CDUI. This should facilitate merging the CPCI user interface with the CDUI for Release 3. The Software Design Description (SDD) which documents user interface to the Central Personnel Clearance Index (CPCI) segment of the PSDB server will be updated as development progresses. The CPCI user interface will be a PowerBuilder application that is intended to be run from the same user workstations as the CDUI application. Development of an internal prototype CPCI user interface application was completed during December, 1995. This internal prototype establishes an application shell for the CPCI interface. Finalization of "look and feel" datawindow design and workflow processing will continue in January.
- WDAC (WBS#2.2.5): With the establishment of an internal configuration baseline for the PSDB server, the WDAC DP-312 interface will now proceed with modifications needed to utilize the PSDB server design intended for DISS Release 2.1. Modifications to the WDAC DP-312 interface needed to utilize the PSDB server design for DISS Release 2.1 are substantially complete. The design will undergo internal review during the week of January 15, 1996 in preparation for release to integration testing.
- VADB (WBS#2.2.6): Version 1.0 of the VADB interface control document was released October 5, 1995 to the CWAC project team and DOE HQ. A prototype web interface to the VADB has been developed that supports the standard query functions presently performed by the DAVAC process. This web-browser interface will be refined to work with commercial secure webserver technology. The Netscape Commerce server has been selected as the initial secure web platform for the VADB interface. This will establish a development environment for conversion of the existing

prototype web interface to the VADB into a production version for inclusion with the DISS Release 2.1 software suite.

- AUI (WBS#2.2.8): The development of the standalone Applicant User Interface (AUI) is proceeding ahead of internal schedule. The AUI is being developed as a standalone Powerbuilder application connecting to a local Watcom database that can be installed on an applicant's PC. Existing forms from the CDUI were ported to the AUI with only minor internal modifications. The portion of the RPS database that supports the forms was successfully ported from Oracle to Watcom, again with only minor modifications.

The AUI is anticipated to require between 3 and 5 high-density diskettes for installation, and will be capable of placing applicant data in a secure format for transmission via email or placement on a diskette for transmission to the RPS. Release of the AUI to testing is expected for late January or early February, 1996.

Incorporation of PEM into the AUI concurrent with an April deadline for R2.1 is not presently achievable with current resource limitations, therefore the April release will include the AUI without PEM (but with data encryption). Planning for use of PEM encryption with the AUI is underway for a post-April upgrade.

Release 3.0 Development

Development for the Release 3.0 Distributed Database has been placed on hold as reflected in the August 18 release of the DISS Project Management Plan. Work is proceeding instead on the standalone Central PSDB server design (WBS#2.2.2) that will support CPCI, WDAC, and VADB. A Statement of Work for FY96 DISS Release 3.0 functions was prepared and delivered to DOE HQ.

II. Risk Based Evaluation of Computerized Nuclear Materials Accountability Systems

<u>B&R No.</u>	<u>Funding</u>	<u>Obligated</u>
GD-05-08-03	\$300K	\$6K
GD-06-02-02	\$24K carryover	\$16K

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 continued to develop, document and report on our method to analyze insider threats against computerized nuclear materials accountability (MA) applications. To provide insight to regulators and MA system design decision makers, we have developed a systematic and manageable aggregation assessment approach for 'scoring' the effectiveness of different system designs against insider threats. This approach is based on the use of multi-attribute utility preference functions, and its details, with exemplifications, have been included in the methodology draft report.

We have prepared a paper on the method for the LLNL Computer Security Practitioner's Conference, February 6-7, 1996. An abstract/paper was also prepared for submission to the 12th Annual American Defense Preparedness Association (ADPA) Symposium on Security Technology. The ADPA paper focuses on how the methodology can assist managers and policy makers to logically and pragmatically trade off competing design options for accountability applications. We also plan to submit a paper for the 1996 INMM Annual Meeting.

We began to prepare for an evaluation, utilizing the developed methodology, of the SRS beta-LANMAS against potential insider threats. It is anticipated that the unclassified SRS beta-LANMAS will be available for evaluation in the January-February 1996 time frame. In preparation, we modified some of the method templates to focus on modern network-based systems and began to develop structured questions for performing assessments and tradeoffs of the beta-LANMAS security features.

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

<u>B&R No.</u>	<u>Funding</u>	<u>Obligated</u>
GD 06-04-01	\$96K	\$0K

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.

During this quarter, we developed the Z Lock functional requirements. A commercial product, the CT-20 produced by TESA Inc., that meets many of these requirements was identified. A preliminary evaluation of the CT-20 was performed. Based on this evaluation we are entering into discussions with TESA on the possible modification of the CT-20 to meet DOE requirements. If the discussions are favorable, then we will submit a revised LCP for OSS approval with our recommendations to pursue modifying the CT-20 rather than design and build an original system.

Because of the late receipt of funding (December) and the scoping nature of our work this quarter, no funds were obligated.

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	Awaiting NV hardware
1/15/96	Begin RL Acceptance Test	Scheduled for 2/12/96
2/12/96	Begin SR Acceptance Test	Beginning 1/15/96
2/26/96	Begin SNR Acceptance Test	Hardware shipping to LLNL
4/22/96	Begin CPCI/WDAC/VADB Acceptance Test	
5/20/96	Begin AL Acceptance Test	
6/17/96	Begin OR Acceptance Test	
7/8/96	Begin HQ Acceptance Test	
7/22/96	Begin ID Acceptance Test	
7/29/96	Begin RF Acceptance Test	
8/19/96	Begin PNR Acceptance Test	

<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. Operational Readiness Review	10/30/95
11/30/95	Standalone HQ server and network operational	Awaiting server
12/31/95	CPCI Oracle-mainframe synchronization demonstrated	Expected 1/31/96
2/1/96	WDAC beta test begins	Awaiting HQ server
3/15/96	Integration testing of all standalone centralized system components (CPCI/WDAC/VADB/MFRS)	
4/30/96	AUI ready for deployment	
4/30/96	Standalone centralized system ready for deployment	
6/30/96	Mac ports ready for deployment	

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	
3/96	Report on extension to other computerized safeguards and security systems	
4/96	Technology transfer tools, documentation, and training materials	
7/96	Management evaluation approach to evaluate all aspects of MC&A systems	
9/96	Evaluations of risks of LANMAS (or sooner depending on when implementation of LANMAS is complete)	
9/96	Report on evaluations of risks of LANMAS (or sooner depending on when implementation of LANMAS is complete)	

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	

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

DISS Personnel Security Networks and Databases Concept of Operations, Version 4, October 19, 1995

DISS Encryption Key Management Plan, Version 1, October 11, 1995

DISS VADB Interface Control, Version 1, October 5, 1995.

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 43 incidents and 28 cases—cases are incidents that involve more than one DOE site. CIAC is attempting to tighten up its incident tracking to better support the needs of DOE Headquarters. These incidents and cases generated 312 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.

The team responded to numerous viruses: Microsoft Prank, Good Times (the hoax continues to pop up as real), MacGyver, Junkie, AntiCMOS, and AOLGOLD. Intrusion attempts via the Internet continue: CIAC handled incidents involving ftp, e-mail spamming including a forged hate mail message, SATAN scans, a compromised rhost file, suspicious port scans and finger requests, attempted root logons utilizing captured passwords, and unauthorized telnet attempts. A number of incidents involved intrusion attempts by individuals from outside of the U. S. including the former Soviet Union and involved agencies beyond the DOE.

CIAC has submitted several session and training proposals for the 1996 DOE Computer Security Group Training Conference. And as a result of a conversation at DOE Headquarters involving CIAC team members and Bob Caldwell, CIAC has been asked to participate in a track aimed at helping sites utilize the guidance in the new DOE security manual which complements the existing classified and unclassified orders.

CIAC also received the first annual DOE IM award for technical excellence. The project leader and one team member flew to Pittsburgh to receive this award.

II. Network Intrusion Detector (NID)

NID was converted to the Solaris 2 operating system. A new operating model (evidence gathering) was added to NID. A draft of the new user's guide was completed. A white paper on monitoring ramp-up was completed.

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

The SPI team released a beta version of the SPI-NET multi-host security inspections package to select beta testers.

IV. Network Security Gateway (Firewall) Process and Tool Development

We completed a write-up on Firewalls using CIAC Notes as a method of getting the information to the field. This is currently being reviewed for release by CIAC. We prepared abstracts and started on presentations for the Security Practitioners Conference at LLNL and the DOE Computer Security Group Training Conference. We also continued exploring the possible development of an advanced firewall system.

V. Profiling and Vulnerability Analysis Project (VAP)

We prepared a preliminary Operations and Management document for the VAP archive, including the archive hardware and network design, security plan, access types, and options for external access. We presented and revised that document at a meeting in Germantown. We visited with the CERT team and obtained operational documents concerning their vulnerability lists and the layout of the documents containing those lists. We discussed the project with Gene Spafford at Purdue University and obtained an operational document for his vulnerability database. We also discussed cooperation with the ASSIST team.

VI. DOE Information Security (DOE-IS) Server

The CIAC archive was successfully moved to the new server and made operational. The old CIAC server has been retired and all current requests for information to the CIAC server are being handled by the new server. The improvement in response times and overall accessibility are very noticeable.

A preliminary Operations and Management document has been produced concerning the types of access to be allowed to the server, security plan, external access options and design of the DOE-IS home page. This document

was discussed at a meeting in Germantown to finalize the access types and the precautions necessary to maintain the integrity of the server.

The DOE-IS home page and page hierarchy were completed and a new IP address is being obtained to logically separate the DOE-IS server from the CIAC server that was its predecessor. The CIAC archive IP address will be maintained to assure continued access for those who already maintain pointers to it.

VII. Distributed Auditing System (DAS)

During this quarter, Dr. Matt Bishop and his students at the University of California at Davis, analyzed the problem of correlating logs at the same level of abstraction but on different hosts. They determined that, short of some indication of interaction, no such correlation could be done (or was meaningful). They then decided to focus on the interaction (since that would be what is of interest).

TASK DESCRIPTION AND QUARTERLY PROGRESS

I. Computer Incident Advisory Capability (CIAC)

<u>B&R No.</u>	<u>Funding</u>	<u>Obligated</u>
GD060603	\$464K	\$117K

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 response continues to be the primary mission of CIAC. This is reflected in the FY96 Project Plan which was discussed and amended at the video conference in December 1995.

Incident handling included intrusions which crossed country borders, new clandestine techniques, and spamming of inappropriate messages. Intruders were using DOE systems to cross country borders in hopes of covering their tracks.

CIAC was also called in to assist DOE Headquarters with their own internal information security program. As part of a trip to NIST, a team member stopped by Germantown to evaluate the NID server that had been given to NN to help secure their network. The system was not being used and hence was several revisions behind. Working for one day, CIAC was able to get the system operational, NID updated, secure the operating system, and train the contract employee who would be monitoring NID. CIAC will also be working with the unclassified security manager on their security issues.

CIAC continues to secure its firewall and other file servers. It is making extensive use of the power of html and perl to develop applications to facilitate the configuration management of its systems and to automate routine tasks, such as bulletin formatting.

CIAC continues to participate in the FIRST organization. The project leader attended a steering committee meeting in December in Santa Clara where the 1996 Workshop and Conference will be held. CIAC continues to collaborate with other teams in an effort to train and educate all response teams on the correct use and analysis of penetration scripts.

II. Network Intrusion Detector (NID)

<u>B&R No.</u>	<u>Funding</u>	<u>Obligated</u>
GD060403	\$297K	\$64K

We continued distribution and customer support via telephone, fax, and U.S. mail for the NID 1.4 release.

We completed the task of converting the NID code for use on the Solaris 2 operating system. In addition, we created a new operating model for NID. This model, known as evidence gathering, is analogous to being under surveillance. We also produced a white paper describing our upcoming efforts to add automatic monitoring ramp-up to certain NID modes.

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

<u>B&R No.</u>	<u>Funding</u>	<u>Obligated</u>
GD060403	\$223K	\$50K

We released the SPI-NET 0.9-beta multi-host security inspection package for field testing. The system employs an extensive graphical user interface based upon tcl-tk. The remote inspection system has been successfully tested on SunOS 4.1.2, SunOS 5.4 (Solaris 2.4), IRIX 5.3 and HP-UX 9.05.

A VMS version of the SPI-NET Remote Inspection System has been released to a limited set of beta testers. This has uncovered problems related to system calls with two of the six executables, and work is underway to add the necessary functionality to the VMS support library.

A tech-transfer plan for the SPI and SPI-NET products is on schedule for release on 1/31/96. Six responses to the SPI Commerce Business Daily announcement are being evaluated to develop the selection criteria.

IV. Network Security Gateway (Firewall) Process and Tool Development

<u>B&R No.</u>	<u>Funding</u>	<u>Obligated</u>
GD060103	\$221K (FY95)	\$218K

A firewall focused edition of CIAC Notes was prepared to get some firewall information to the field. This includes the paper *Firewall Products Today* with updates on things learned since the paper was presented at the last DOE Computer Security Group Training Conference. The Notes material is being reviewed by CIAC for release. This edition also includes requests for feedback from DOE sites regarding firewall use.

We are preparing a pilot presentation on firewalls for the LLNL Computer Security Practitioners Conference to be held in February. This is to help develop the workshop to be presented at the next DOE Computer Security Group Training Conference, as well as at other sites upon request.

We are working with Sandia to determine who to team with and how best to update our proposal for an advanced firewall system. This is in response to feedback from ARPA. We hope to update the proposal and re-submit it for a new BAA. We believe that the type of technology we are exploring would be very useful for the national laboratories.

V. Profiling and Vulnerability Analysis Project (VAP)

<u>B&R No.</u>	<u>Funding</u>	<u>Obligated</u>
GD060403	\$259K	\$35K

We completed the installation of the Oracle database software on the server and installed the front-end development software on a PC workstation. Network access of the database server has been achieved and development of the front-end is in process.

We wrote a preliminary operational document concerning the operation of the database server, security precautions, and methods of access for the server. The document served as a straw-man operations document for a day of discussions in Germantown. During those discussions, many questions were answered concerning the type of access needed and how that access can be achieved and still maintain adequate security for the database. The operations document is currently being revised to show the results of that meeting, and the access methods are being implemented.

One task is to coordinate the database with other response teams and to institute sharing among the teams. We visited CERT to setup methods for exchanging vulnerability information and to obtain the design of the CERT vulnerability database to ensure that it is compatible with the one being developed at the CSTC. The CERT database currently consists of single files, with each containing the description of a single vulnerability. There is no database engine used to maintain the database or to provide a structured search capability.

Members of the ASSIST team were able to attend the meeting in Germantown, to discuss sharing of the database information and the state of the ASSIST database. At this time, nothing has been done on the ASSIST database.

We discussed the database and sharing with Gene Spafford at Purdue University and obtained a description of the Purdue database. The Purdue vulnerability database was developed as part of a Masters thesis by Taimur Aslam (T. Aslam, *A Taxonomy of Security Faults in the UNIX Operating System*, Masters thesis, Purdue University, Aug. 1995). A copy of the thesis is

available online at the Coast archive at Purdue (<http://www.cs.purdue.edu/coast/>). The archive consists of a flat database, with a single record per vulnerability. There are about 45 vulnerabilities catalogued, with information obtained from CIAC and CERT bulletins.

VI. DOE Information Security (DOE-IS) Server

<u>B&R No.</u>	<u>Funding</u>	<u>Obligated</u>
GD060403	\$150K	\$11K

We completed a preliminary Operations and Management document for the server and presented that document at a meeting in Germantown. Numerous questions were answered and the procedures were revised to support those answers. A revised document is in process.

The server hardware and software are installed and operational. The CIAC archive has been transferred to the server and is currently available. The DOE-IS home page and page hierarchy are complete and being populated with information. The CIAC home page is available at <http://ciac.llnl.gov>. The DOE-IS home page is currently available at <http://ciac.llnl.gov/doe>, and will be available at <http://doe-is.llnl.gov> as soon as the new address is assigned and available.

We are developing methods to use the security features of the new system, including the lockable hard disk, the CD-ROM drives and the MLS system to enhance the security of the server without impacting its access.

We are actively seeking information from other DOE sites to use to populate the server.

VII. Distributed Auditing System (DAS)

<u>B&R No.</u>	<u>Funding</u>	<u>Obligated</u>
GD060103	\$75K (FY95)	\$75K

During this quarter, Dr. Matt Bishop and his students at the University of California at Davis, analyzed the problem of correlating logs at the same level of abstraction but on different hosts. They determined that, short of some indication of interaction, no such correlation could be done (or was meaningful). They then decided to focus on the interaction (since that would be what is of interest). In order to determine what log entries spring from the interaction, one needs to mark the communication or interaction in some way; and their report, "Reconciling Applications and Kernel Logs," discusses how to do this, along with some simple experiments.

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

I. Computer Incident Advisory Capability (CIAC)

B&R No. GD060603

6 Bulletins/Advisories

- G-01: Telnetd Vulnerability
- G-02: SunOS 4.1.X Loadmodule Vulnerability
- G-03: AOLGOLD Trojan Program
- G-04: X Authentication Vulnerability
- G-05: HP-UX FTP Vulnerability
- G-06A: Win95 Vulnerabilities

Changes to CIAC Project Management Plan have been agreed to and document is being revised for delivery.

Discussions continue to refine format and content of annual CIAC incident statistics report.

We completed the update of the CIAC Project Management Plan in November of 1995.

Changes in the format and content of the yearly report on incident stats were given to the OSS Project Manager in December 1995.

II. Network Intrusion Detector (NID)

B&R No. GD060403

We completed converting NID for use under the Solaris operating system. We met the 12/31/95 milestone and deliverable for a white paper on our monitoring ramp-up task.

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

B&R No. GD060403

We met the 10/31/95 milestone and deliverable for the beta release of SPI-NET for distributed mode operation across an installed base of UNIX systems from a UNIX command client.

We met the 11/30/95 milestone and deliverable for the beta release of SPI-NET for distributed VMS inspections from a UNIX command client.

IV. Network Security Gateway (Firewall) Process and Tool Development

B&R No. GD060103

We delivered a firewall focused edition of CIAC Notes. This edition also includes requests for feedback from DOE sites regarding firewall use. We are also preparing a pilot presentation on firewalls for the LLNL Computer Security Practitioners Conference to be held in February. This is to help develop the workshop to be presented at the next DOE Computer Security Group Training Conference, as well as at other sites upon request.

V. Profiling and Vulnerability Analysis Project (VAP)

B&R No. GD060403

The repository hardware and software are in place and operating, along with operational procedures.

VI. DOE Information Security (DOE-IS) Server

B&R No. GD060403

The DOE-IS server is installed and online.

VII. Distributed Auditing System (DAS)

B&R No. GD060103

Tasks completed (cumulative):

1. Develop a standard audit log format that can provide enough information to trace breaches of security in a heterogeneous environment. At a minimum, the format will apply to a UNIX-type system and a non-UNIX type system.
2. Determine what high-level and low-level events should be logged, and the current state of logging mechanisms.
3. Analyze the problem of mapping low-level logs from a single computer system to high-level events.
4. Analyze the problem of correlating low-level (or high-level) logs from networked systems (or components of a distributed system) to obtain a high-level picture of attacks upon the system.

Deliverables completed (cumulative):

1. A paper presenting the standard audit log format, including a rationale for each component ("A Standard Audit Trail Format," submitted to the 1995 NISS Conference, successor to the NCSC).
2. Tools to convert logs from at least two existing systems into this format.
3. A paper presenting what should be logged for each of several types of auditors (financial, criminal, etc.).
4. A description of techniques to map low-level log entries to high-level log entries.
5. Software to do the mapping, or to aid the auditor in doing the mapping.
6. A description of techniques to correlate low-level log entries from multiple systems with one another.
7. Software to do the correlation, or to aid the auditor in doing the correlation.

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

Dr. Matt Bishop, "Reconciling Application and Kernel Logs."

Complex-Wide Access Control System (CWAC) 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:

- 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

- I. Completed hardware assembly and checkout for two enrollment stations (CWAC development and DOE-Oakland). Completed hardware fabrication and all procurement and receipt of hardware (except for computer workstation hardware) for the DOE-HQ enrollment station.
- II. Updated the definition of the interface between CWAC elements and the Visit Authorization Data Base (VADB).
- III. Completed design of enrollment/verification station software; development is continuing.

TASK DESCRIPTIONS AND QUARTERLY PROGRESS

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

<u>B&R No.</u>	<u>Funding</u>	<u>Obligated</u>
GD 060501	477K	158K

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: Specification and procurement have been completed for all hardware and vendor-supplied software for all enrollment/verification stations, with the exception of the Oracle software used to encrypt SQL*Net communication between the enrollment/verification station client and the VADB data base server. Quotations are being solicited for this software. Two enrollment/verification stations have been assembled and all components verified operational. Due to a delay in capital funding authorization, the computer workstation hardware for the third enrollment/verification station was ordered later than other hardware, and was not received until the week of January 8.

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: Software design has been completed and software development continues. The design will incorporate the functions currently provided by the Argus enrollment station in the CWAC Enrollment/Verification Station. These functions include:

- Encoding/Reencoding Badges
- Enrolling/Reenrolling Users
- Enrolling with the Hand Geometry Unit
- Reinstating Badges
- Badge Verification
- Biometrics Verification
- Display User/Badge/Access/Preenrollment Information
- Validate User by Biometrics Template

As a result of CWAC design criteria reviews, it was determined that Argus enrollment station functionality will be expanded in two areas. The first is to allow enrollee weight values to be input by the enrollee, rather than measured by a weight measurement system. The second is to provide the ability to insert "person" records in VADB for uncleared workers who will be issued standard badges and who are not being processed for clearances. This is required because VADB does not contain "person" information for workers who are not being processed for clearances. This will allow VADB to provide badge accountability for all standard badges.

- 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: An initial software design has been developed for the Argus ACS/VADB interface. The need to provide software processes to accomplish such functions as download of visitor access control information in advance of site visits, reconciliation of local access control databases versus VADB data base content, and "hot stop" checks for badges and clearances has been identified. It is planned to incorporate these functions after the development of the basic ACS/VADB interface has been completed and correct operation demonstrated.

- 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: DOE-Oakland Security personnel were briefed on the current status of the CWAC project, and they visited the staging location for the DOE-Oakland Enrollment/Verification Station. Here they were briefed on the physical installation requirements for the E/VS components. It was explained that LLNL will ship E/VS hardware to the Federal Building in Oakland and provide installation consulting and support, but will not perform the actual installation, which must be arranged by DOE-Oakland.

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

Quarterly Progress: No activity this quarter

- 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: A review was performed on a draft revision to the DOE Standard Badge Implementation Guide, and several comments were developed. Issues related to enrollment and maintenance of standard badge and access control information in VADB were also identified and described. As a result, draft "principles" related to security and standardization of the processes which enroll and maintain information in VADB were developed. It

is intended that these principles, when finalized, will be included in a future release of the DOE Standard Badge Implementation Guide.

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: Progress reports summarizing significant project accomplishments, issues, and milestone status were issued each month. We coordinated with Wendy Smoot of DOE-HQ to obtain required capital funding authorization for the workstation hardware for the third enrollment/verification station. Presentations concerning CWAC objectives, status, and design criteria were given at a November DISS Quality Panel meeting, and a December Security Systems Quality Panel meeting.

At the request of DOE-HQ OSS we prepared a proposal to develop a low cost enrollment/verification station which will allow non-Argus users a relatively inexpensive option (<\$10K per unit) to enroll CWAC information in VADB. This low cost enrollment/verification station would be based on the VADB end user client hardware/software platform, and would provide the capability to enroll badge (including PIN and weight), person, and biometrics information in VADB. It would not encode badges, and would support weight entry by the enrollee, rather than automatic weight measurement.

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

Quarterly Progress: No activity this quarter

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

Original Milestone	Description of Milestone	Status
10/95	Complete hardware fabrication of first CWAC enrollment/verification station for development use	Complete
11/95	Demonstrate enrollment/verification station communication with developmental version of VADB over unencrypted communication lines.	Complete
12/95	Complete hardware fabrication of 2nd and 3rd CWAC enrollment/verification stations for future deployment at DOE-Oakland and DOE-HQ	Complete

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

None.

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, and also to support the DOE in offering relevant security technology and capabilities to Federal standardization efforts.

SUMMARY OF MAJOR ACCOMPLISHMENTS AND ISSUES

- I. The Unclassified Argus Internet Homepage with password protections was activated at LLNL at an address of [HTTP://argus.llnl.gov](http://argus.llnl.gov). The Homepage was significantly enhanced beyond the prototype produced last quarter.
- II. As a part of the Federal standardization effort, presentations were created and given to the Facility Protection Committee in Washington on November 8, 1995 and to the Director of Security Police for the Air Force Space Command on November 16, 1996.
- III. Final note on the CRADA closeout. All material has been returned to its owner. Computer disks were returned to Martin last quarter and Argus Demo System equipment was returned to LLNL this quarter. There have been no further demands, clarifications, or communications between LLNL and Martin on the subject of the Argus CRADA. At this point we consider this subject completely closed.

TASK DESCRIPTIONS AND QUARTERLY PROGRESS

B&R No.
GD 06 0201

Funding
\$150K

Obligated
\$53K as of 12/30/95

I. Argus Homepage

The Unclassified Argus Internet Homepage with password protections was activated at LLNL at an address of HTTP://argus.llnl.gov. As an added security measure, the Argus Homepage has been set up to only accept browsers located on the LLNL site, pending a content and security plan review from DOE HQ. A server which implements secure communications links has been obtained and installed. It will be activated as soon as testing is complete. The activation of the secure server will ensure privacy of the communication session. A description of the prototype Argus Homepage was provided last quarter. This quarter has seen steady improvement to the webpage as internal reviewers provide comments and suggestions for content modification and additions. The photo, documentation, and software release sections were enhanced. A new Argus Futures section was created, along with a form-based software enhancement request section.

II. Standardization of Federal Systems

The DOE is participating in the ongoing efforts to reduce the cost and improve the operation of the physical and personnel security systems of the Federal Government. The Department of Energy appears to be the only agency with an integrated approach on a nation-wide scale. The DOE has been working towards implementing this approach through the careful funding and deployment of computer-based systems over the last few years. An overview presentation on this approach was given to the Facilities Protection Board in November. A more detailed discussion of elements of this approach was provided to the U.S. Space Command in November. The DOE standard badge was a particular interest of the Space Command.

APPENDIX A: 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
1/15/96	Update of Argus Functional Description	D	
2/14/96	Presentation to and report on Argus Advisory group meeting	D	
3/9/96	Draft report on DOE contribution to the Federal Standardization of electronic security systems	M	
5/1/96	Final report on DOE contribution to the Federal Standardization of electronic security systems	D	
6/30/95	Federal Govt. Workshop on DOE's electronic security systems concepts	D	
9/1/96	Argus Advisory Group meeting support	M	
9/13/95	Argus Workshop	D	
9/30/95	Argus Homepage report	D	

M=Milestone
D=Deliverable

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

Argus Homepage HTML files

Information Technology Support

Barbara C. Davis, Deputy Associate Program Leader
Fission Energy and Systems Safety Program

INTRODUCTION

The Fission Energy and Systems Safety Program (FESSP) Information Technology Support program area provides support to the DOE and other government sponsors in two related areas: (1) the integration of an organization's information technologies to create a collaborative work environment; and (2) the integration of information security into an organizations information technologies. The purpose of the program area is to integrate advanced information technologies through a structured approach. This approach begins with requirements, including threat, defense-in-depth, and graded protection. System robustness is a key issue when developing the requirements. Most major information security breaches are the result of a lack of robustness, rather than individual vulnerabilities. The integration of information security into an organizations electronic information infrastructure makes security a core feature rather than a separate function.

SUMMARY OF MAJOR ACCOMPLISHMENTS

- Development of the Advanced Information Management System (AIMS) for the Nuclear Regulatory Commission (NRC) Advisory Committee on Reactor Safety (ACRS) and the Advisory Committee on Nuclear Waste (ACNW).
- Development of the Geographical, Environmental & Siting Information System (GEN&SIS) for the Nuclear Regulatory Commission (NRC) Office of Nuclear Reactor Regulations (NRR).
- Development of the U.S. Business Advisor for the Small Business Administration (SBA) and the National Performance Review (NPR).
- Development of the Acquisition Reform Network for the Executive Office of the President (EOP) Office of Federal Procurement Policy (OFPP), the National Performance Review (NPR), and the Department of Energy (DOE) Office of Safeguards and Security (OSS).
- Development of RuleNet for the U.S. Nuclear Regulatory Commission (NRC) Office of General Council (OGC).
- Development of SARNet for the Department of Energy (DOE) Office of Defense Programs (DP).

TASK DESCRIPTIONS AND QUARTERLY PROGRESS

Electronic Open Meeting Methodology Development - EOM (Kristian Chubb, Project Engineer)

B&R No.

Funding
\$200K

Obligated
\$200K

No quarter activity on the Electronic Open Meeting Methodology. Funds were expended on getting the June EOM pilot system operational. The pilot project on Federal Acquisition Reform did occur. The necessary reports to close the project have not been generated; they are in process.

This pilot project did result in follow-up on work by NRC and DOE-DP. DOD has formally requested the source code developed in the pilot for use in DOD Acquisition Reform efforts. The FAA, GSA, NRC, and DOE-ER are discussing with us the possibility of follow-on work using the EOM System.

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

<u>Date</u>	<u>Milestone or Deliverable</u>	<u>Status</u>
7/31/95	Conduct first EOM	Milestone Met
9/30/95	Provide DOE with results of initial prototype along with lessons learned	Milestone not met - revised delivery 2/15/96
9/30/95	Provide DOE with requirements detailing the functionality of the web-based methodology	Milestone not met - revised delivery 2/15/96
9/30/95	Provide DOE with plan for convening a second EOM	Milestone not met - revised delivery 2/15/96
9/30/95	Provide DOE with the design of the enhanced prototype expert-based system and interface; and a training plan for discussion facilitator for the second EOM	Milestone not met - revised delivery 2/15/96
9/30/95	Present to DOE a program plan for conducting a second prototype meeting using the enhanced export-based tool. The program plan will also discuss where name development is required to enhance the expert-based EOM methodology. The program plan will also include discussions on development of a tool kit which can be used to easily configure the interface for convening an EOM on any topical issue. The program plan will also provide a detailed plan for developing, implementing and evaluating the proposed EOM and how the methodology might lend itself to other uses, such as an emergency response meeting or an EOM which must accommodate a mixed access level information environment. This program plan will also provide a detailed plan for the training of discussion facilitator on the use of the expert-based system with interface.	Milestone not met - revised delivery 2/15/96

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

None this quarter.