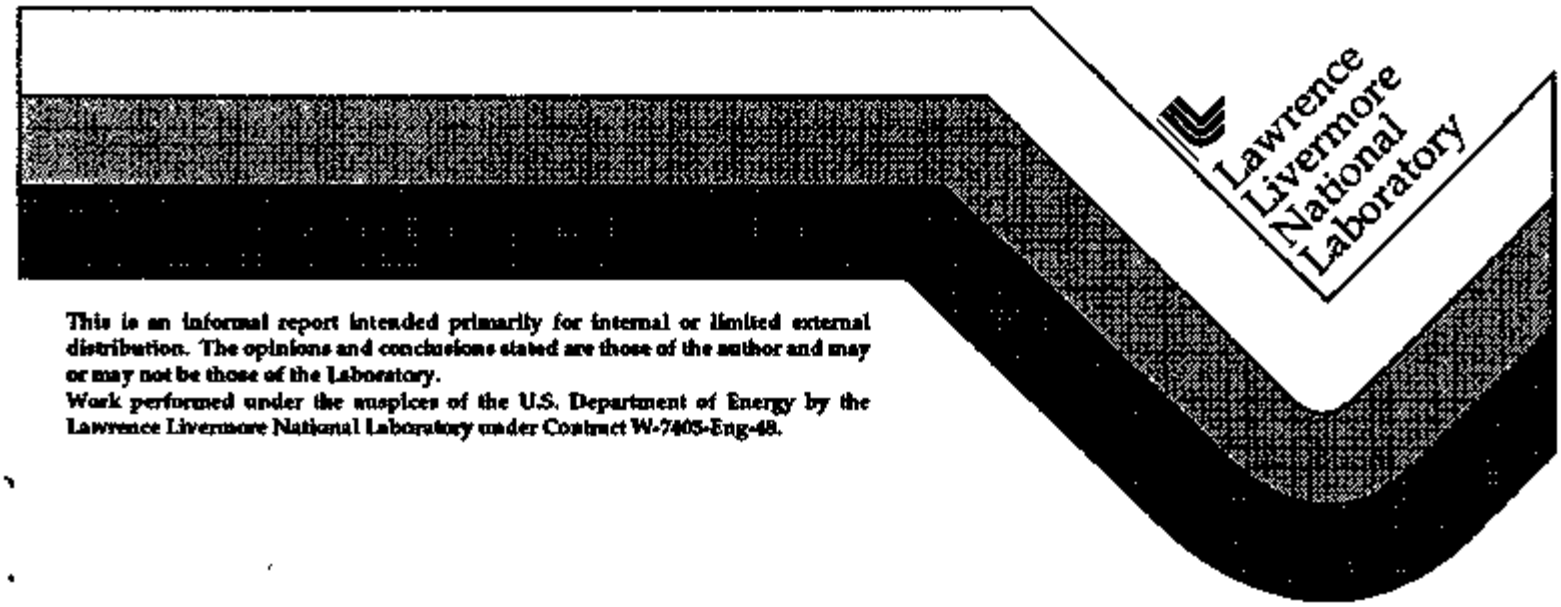
UCRL-ID-106454-96-2

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

Quarter Ending March 31, 1996

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

April 1996



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

UCRL-ID-106454-96-2

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

Quarter Ending March 31, 1996

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

April 1996

Table of Contents

Preface

The Lawrence Livermore National Laboratory (LLNL) carries out safeguards and security activities for the Department of Energy (DOE), Office of Safeguards and Security (OSS), as well as other organizations, both within and outside the DOE. This document summarizes the activities conducted for the OSS during the Second Quarter of Fiscal Year 1996 (January through March, 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 Materials Accountability
- Computer Security - Distributed Systems
- Complex-Wide Access Control
- Standardization of Security Systems
- Information Technology & Security Center

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

- The MGA++ executive has been developed and integrated with MGA, PU600, and U235.
- Studies of CdZnTe detector line shapes for detectors from a second manufacturer have be done revealing differences between detectors from different manufacturers..

II. Emission/Transmission Computed Tomography

- Methods for remote data taking, sample movement, and monitoring of the button scanner have been implemented.

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

- Support has been provided for the Plutonium Stabilization and Packaging Program.

IV. Monte Carlo Simulation of Gamma-Ray Spectra

- Data bases have been extended to include photon-electron interactions on americium.

TASK DESCRIPTIONS AND QUARTERLY PROGRESS

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

I. NDA MC&A Measurement Technology R&D

B&R No.	Funding	Obligated
GD060402	$350K	$198K

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, and DeLynn Clark

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 first version of MGA++ (ISO-S) if ready for demonstration. This is a Win32 version running under Windows95 or WindowsNT, and has been developed using five separate modules: an executive capable of pre-screening spectra and selecting between three computation paths - MGA, PU600, and U235 - with a graphical user interface and the SpecVu graphics server. The LLNL version of MGA, the U235 code developed under this task, and the PU600 code developed for mutual-reciprocal-inspection (MRI) have all been ported to the Win32 environment, and are accessible from ISO-S. The controller portion of the executive is completed. The "pre-screen" portion of the executive is functioning and will route spectra for Pu (MGA), shielded Pu (PU600), and U(U235) analysis. The complexity of the decision process, and the number of analysis choices can be increased as the code evolves.

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++.

This program uses measured branching ratios explicitly so that as improved data becomes available, it can be incorporated into the code. This method also avoids "fitted" values that may not be valid for all geometries and sample types. The program is modular, with algorithms that model physical processes, not "black boxes" that generate results with no apparent physical process foundation.

A method has been developed to analyze very low enrichment uranium using the uranium and daughter gamma rays in the 130-190 keV region. It successfully obtains the enrichment of a 0.017% ^{235}U standard to about 1%. The accuracy of the program, as determined by analyzing standards, is steadily improving over the entire enrichment range. Overall, the accuracy of the program is about $\pm 2\%$ over the enrichment range of 0.17% to 99% for known uranium standards.

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 production prototype CdZnTe detectors have now become available from the manufacturer of the first 5mm x 5mm x 5mm detector that was used in the initial analysis of peak shapes from these detectors. The energy dependence of the shape parameters for these detectors is very similar to what we reported earlier for the first detector. We have also studied spectra taken with detectors made by a second manufacturer. The long term tailing is much less significant in these spectra. However, at least in the spectra studied so far, the short term tailing (covering a range of several keV below the peak for a 122-keV gamma ray) appears to be larger in magnitude than for detectors from the first manufacturer. The spectrum also is different as the maximum of the gamma-ray peak is approached, with the peak cutoff parameter being significantly larger for detectors of the second manufacturer than those of the first. These results suggest that one generalized shape parameterization may not apply well to detectors from different manufacturers at this time. 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.] We are starting to examine the practicality of Pu measurements using CZT detectors.

II. Emission/Transmission Computed Tomography

B&R No.	Funding	Obligated
GD060402	$150K	$86K

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 upgraded the stage design for our scanner platform to reduce wobble (about 1 mm) when the staging is moved in all three axes. The redesigned and rebuilt stage system now has a straightness of less than 0.01 mm in 30 cm travel, allowing for reliable combining of the emission and transmission data for a sample. We have installed a small CCD camera for remote monitoring of the stage system for both safety and security purposes.

We are acquiring data remotely for Pu standards samples, and excising the stage control software and data acquisition software, while awaiting final DOE approval of our Operating Safety Procedure (OSP). This delay in obtaining this approval, now more that 6 months in total, has delayed finishing the scan of our Pu molten-salt extraction (MSE) button. Nevertheless, progress made in the operation of the scanner on test samples and the experience being gained in the use of the software will allow for rapid progress of the measurement of the Pu MSE button upon OSP approval.

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

B&R No.	Funding	Obligated
GD060402	$90K	$36K

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 made an extended series of measurements of Pu samples shielded by up to 12.7 mm of stainless steel 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. For a 1 kg Pu oxide standard, we get $\pm$0.5% accuracy for material shielded by 6 mm of stainless steel (a four hour count), and $\pm$1% for 1 kg of Pu oxide measured through 12.7 mm of stainless steel (an eight hour count). Thus MGA will perform well for samples of Pu oxide contained in stainless steel containers now being considered by DOE.

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. In particular, the U235 program has performed somewhat better than another often used program, MGAU, for a material with non-standard uranium enrichment of about 80%. Also for uranium material with slight Pu contamination, a situation that is intractable for the MGAU program, the U235 program gives results to within 10%. Work is being done to improve these results.

Support of the Interim Plutonium Storage Activity
William M. Buckley, Kenneth E. Raschke, and Eugene A. Henry

Support has been provided to the interim plutonium stabilization and packing project (PuSAP) in several areas. We have provided input specifications to a proposal for instrumentation based on the IAAS instrument funded in part by OSS at LLNL. This proposal included rapid data acquisition and analysis using methods embodied by MGA and MGA++. We attended a recent DOE/HQ working group meeting to discuss instrumentation. It was decided that standardized instrumentation would not be used at all sites, but that standards and requirements would be instituted to assure that all sites obtain the same analysis for these samples. LLNL, Westinghouse Hanford, and possibly Westinghouse Savannah River will use MGA-based approaches. We have volunteered our assistance in generating or refining requirements, and evaluating proposals for MGA based analysis systems at Westinghouse Hanford.

IV. Monte Carlo Calculations of Gamma-Ray Spectra

B&R No.	Funding	Obligated
GD060402	$175K	$74K

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 completed the installation and testing of the new data base MCNPDAT6 for the MCNP program for simulating gamma ray spectra. This new data base has multigroup cross section table for neutron interactions with various elements. The gamma rays that induced neutron interactions are included in this new data base, allowing a more accurate simulation of special nuclear materials that contain neutron emitters.

The photon interaction data base (mcnplib02) and the electron table (el1) have been extended to Z=95. These extensions have been tested, and give the capability to simulate materials that contain significant amounts of americium correctly. This capability, not available with the usual MCNP libraries which extend only to Z=94, is necessary for simulating spectra of materials like Pu (MSE) buttons that contain significant amounts of americium.

Monte Carlo Calculation of Uranium Spectra
Tzu-Fang Wang

We continue to develop the method to accurately simulate uranium spectra. Excellent agreement has been obtained for a simulation of a 75% enriched uranium standard for the 100-keV region. However, extensive measurements are continuing to establish the overall spectrum of uranium to complete development of simulated spectra of enriched uranium standards.

V. Other Related Activities

M. N. Namboodiri and Eugene A. Henry were co-organizers of the American Chemical Society Symposium entitled Nuclear and Isotopic Methods of Analysis for Safeguards and Security held in New Orleans on March 27-28, 1996. Approximately 24 papers were presented during a two day program that included sessions on gamma-ray spectrometry, neutron analysis methodologies, mass spectrometric methodologies, and nuclear forensics.

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: A SUMMARY OF ALL MILESTONES AND DELIVERABLES FOR THIS QUARTER

I. NDA MC&A Measurement Technology R&D

B&R No. GD060102

Continue development of MGA++, including coding of the decision making executive, integration of SpecVu capabilities, and integration of MGA with the executive--Began 9/94, coding of executive began 1/96, integration of SpecVu and MGA began 2/96.

Conclude development of MGA-like code for analyzing uranium spectra--prototype test program available 5/96, report to be available 6/96.

Conclude study of peak shape fitting methodology for CdZnTe spectra--draft report available 5/96, final report to be available 8/96.

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

II. Emission/Transmission Computed Tomography

B&R No. GD060202

Continue studies and analyses of layered and shielded SNM materials to optimize measurement parameters--Studies of the MSE button are delayed because of the need to requalify the MSE button containment, and to obtain OSP approval. Report on digitized map of Pu MSE button anticipated by 9/96 (previously estimated as 4/96).

Use software assessment to begin development necessary to convert CT data into isotopic information--began 1/95, design determined 6/95, prototype software in place 2/96.

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

B&R No. GD060302

Evaluation and testing of MGA analyses of plutonium samples in DOE-approved thick steel containers - testing complete 3/96, report to be available 6/96.

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

IV. Monte Carlo Calculations of Gamma-Ray Spectra

B&R No. GD060102

General use library of simulated spectra, and a suite of codes and input modules to use with MCNP for spectral simulation--report and library available 9/96.

Study of the simulation of selected heterogeneous materials--began 10/95, report due 9/96.

Development of techniques and capabilities to use the histories provided by MCNP simulations for coincidence and detector charge collection studies--began 1/96.

Continue to generate and study spectra of layered and shielded samples, and explore limitations of these spectra for interpretation of sources--began 2/96

Explore the use of MCNP for the design of complex NDA instruments--not yet begun.

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

"Gamma-Ray Line Shapes from Cadmium Zinc Telluride Detectors", M. N. Namboodiri, presented at the ACS Symposium on Nuclear and Isotopic Methods of Analysis for Safeguards and Security, March 27-28, 1996, New Orleans.

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 installed and acceptance tested at SR, RL, and SNR
- DISS Rel. 2.1 released to integration testing

TASK DESCRIPTIONS AND QUARTERLY PROGRESS

I. DISS - Electronic Transfer of Personnel Security and Personnel Security Database Modernization Technology Development
(Everett Wheelock, Project Leader)

B&R No.	Funding	Obligated
GH-03	$4,200K	$2,323K

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 has been installed and acceptance tested at DOE OAK, SR, RL, and SNR and their 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 Release 2.1 centralized personnel security database (PSDB) has been released to integration testing.

Production

The current production release of DISS is the baseline DISS Release 2.0.1d. Versioned components of this baseline are listed below. Release notes for 2.0.1d have been prepared and are available on the DISS homepage (http://diss.llnl.gov) on the Released Project Documents page.

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

Savannah River

LLNL and DynCorp support for Savannah River acceptance test was completed during January. The Savannah River RPS system was upgraded to the current DISS production Release 2.0.1d. Although numerous difficulties were encountered prior to and during the testing, the deployment team was able to successfully support SR to complete testing of the system. LLNL support staff are continuing to provide assistance to SR and are working with DynCorp to schedule the upgrade of the SR RPS database to include the DISSCNVRT data conversion utility.

Richland

Training for the Richland operations office was completed during the week of February 5, 1996. Acceptance testing for the Richland operations office was completed and the system accepted by RL on February 16, 1996. Richland intends to operate the system in parallel with existing operations for a period of several weeks prior to cutover.

Schenectady

Configuration of the Schenectady systems at LLNL took place in February. A failed internal (system) disk drive caused a setback in the configuration effort. Acceptance testing for the SNR system was performed during March. SNR identified two previously reported bugs that they feel are critical to their application. They are in the CDUI application and are related to Contractor access to data after release to DOE and potential for a read-only user to change data under some circumstances. The fixes for these bugs are currently planned to be incorporated into the next maintenance release of DISS, 2.0.3.

Oakland

In January, DOE Oakland experienced the accidental erasure of a key directory (/etc) on the RPS unix server by the Oakland system administrator. DOE OAK requested DISS team support to restore the system. Restoring the system required in excess of a person-week of effort by the DISS team. In March, DOE Oakland experienced a hardware failure (hard disk). We have loaned them a replacement and have reconfigured their system.

HQ

Hardware for the DOE HQ Firewall, RPS database, and PSDB database was received in March. The PSDB server was configured with operating system and Oracle database; the PSDB database will be installed as soon as it is released to production. The HQ RPS server was configured with both an RPS database for DOE HQ and an RPS database for the Chicago Operations Office. The equipment was shipped back to HQ on April 12, 1996.

OPM

A problem has been identified with the OPM firewall that is believed to be related to insufficient system resources on the AIX computer (memory and disk space). Symptoms include occasional garbling of PEM email at an unacceptable rate for production usage. This problem has been temporarily alleviated by modifying the OPM firewall (with DOE HQ concurrence) to pass PEM mail through to the OPM gateway computer that has sufficient resources for processing. The DISS team is planning to dedicate two weeks in April to analyze OPM firewall load requirements and make recommendations for a permanent solution.

Installation at OPM of the PC's to support gray-scale printing of two types of fingerprint cards was tentatively forecast for late March, however, the staff needed to travel to OPM to perform this function will be occupied with the DOE HQ equipment configuration. Installation of these items at Boyers will need to be deferred until staff can complete HQ's configuration–which will be in May. This is consistent with HQ's latest guidance to the field on electronic transmission of fingerprints until Identicator software problems are overcome.

Other Sites

Albuquerque equipment has been shipped to LLNL, Nevada equipment has not been received. Because of this, deployment to Nevada Operations Office will be rescheduled to follow sometime after Albuquerque. Equipment has been received at LLNL from Oak Ridge and Pittsburgh Naval Reactors.

Release 2.0 Maintenance (WBS#2.1.5)

DISS maintenance baseline 2.0.2 has experienced delays in testing, but is expected to be released to production in April. This maintenance release upgrades 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. Upon completion of integration testing baseline 2.0.2 will be submitted to DOE HQ for approval to release to production.

The DISSCNVRT utility (which is part of 2.0.2) has been released to production. Pending approval by DOE HQ, this utility can be made available as an upgrade patch to RPS v2.0.1d databases.

Release 2.1 Development

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

Clearance state transitions for workflow processing in the CPCI application were reviewed at DOE HQ during the week of January 15, 1996. The PSDB server v2.1a1 was released to test for schema validation and client application testing on March 7, 1996. The v2.1a2 which includes triggers and stored procedures was released to test on March 29, 1996.

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

The CPCI user interface v1.0a1 was release to test on March 29, 1996.

- **CPCI Data Sync (WBS#2.2.4)**

Problems have been encountered in "cleaning up" inconsistent or erroneous data on the existing CPCI mainframe so that it is internally consistent with existing mainframe business rules. This is necessary to ensure that data can be successfully converted to the new DISS. Portions of this cleanup process can be performed on both the mainframe as well as on the PSDB server, however it is the identification of the specific data inconsistencies that is taking longer than originally forecast. Development of the code needed to perform cleanup on the PSDB server is underway. This is intended to permit parallel operation of the existing CPCI mainframe with the new DISS PSDB server for a limited period of time while deployment of DISS Release 2.1 is completed at all sites. It will provide a temporary means of synchronizing a limited subset of essential information (primarily needed by the DAVAC and VADB processes) while cutover to the new DISS is occurring.

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

The WDAC DP-312 interface was release to LLNL integration testing during the week of February 5th. Initial test run was performed against the PSDB server release March 8, 1996. Initial testing uncovered a few bugs which are being re-worked. Re-submittal to test is expected by April 12, 1996, along with the WDAC web client.

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

In February, the environment for web development has been finalized with the receipt and installation of the Netscape Commerce server and Oracle Web Agent as the initial secure web platform for the VADB interface. The VADB interface completed its internal design review on March 14, 1996. Minor design changes resulting from the review were incorporated and released to integration testing April 5, 1996.

- **CWAC Server Support (WBS#2.2.6.3):**

The PSDB server will support Complex-Wide Access Control (CWAC) by including a package of stored procedures and views that provide read-write access to VADB information. These stored procedures are ready to be released to test.

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

Development of the standalone Applicant User Interface (AUI) is proceeding. The AUI is being developed as a standalone PowerBuilder application connecting to a local Watcom database that can both be installed on an applicant's PC. The user interface portion (forms and local database) are largely complete. A companion application, the Applicant Diskette Interface (ADI) is largely complete. This application will permit an Operations Office user to prepare an applicant data diskette containing the most recent applicant data extracted from the RPS database. This application will also provide a means to load the completed applicant data back into the RPS to resume processing. The Validator function of the AUI has completed development.

Incorporation of digital signatures (such as used with "PEM" or equivalent) for data authentication into the AUI has been estimated to require approximately 8 weeks, and could not be included into an April deadline for R2.1. The need for this capability was identified to be driven by the Albuquerque deployment, which has been revised to begin sometime in early June. Completion of development and release to test is forecast for May 13, 1996, with release to production forecast for June 12, 1996.

- **Low Cost Enrollment Station:**

Work on the CWAC low cost enrollment station was funded and begun this quarter. We have determined that LCES will be developed using PowerBuilder for a PC. A Web based alternative was seriously considered, but the current state

of Web technology for interfacing to local PC serial devices (RAP and HGU) was determined to be not yet satisfactory. A transition to Web technology at some later point when the technology is more stable and capable may be worthwhile. The target (user) platform for LCES will be a Pentium PC (any processor speed) with 16 Mbytes of memory, 2 serial ports, ethernet interface, modest hard disk (IDE based, 300-500 Mbytes), and a 15" color monitor. Less capable machines may be able to run the software but will not be tested. The system will require Windows 95, Oracle SQL*Net client, and Oracle SNS client. The Oracle clients and PowerBuilder executable have no associated costs for the PC.

The first LCES deliverable will be a Requirements and Functional Specification document. We are targeting for a draft of this document by end of April, 1996. We are planning site visits to LLNL, SNL-Livermore, and ORNL. The results of these visits will be reflected in the specification.

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

B&R No.	Funding	Obligated
GD-05-08-03	$300K	$55K
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).

This quarter, we carried out internal review on draft report "Analysis of Insider Threats Against Computerized Nuclear Materials Accountability Applications." This report explicates the risk-based evaluation method, including the scoring aggregation algorithm for providing figure-of-merits for system effectiveness. We believe the method and scoring system are now so constructed to be able to extend the approach to other information based S&S systems. The review indicated the need for re-writing parts of the report for more clarity and simplicity.

We prepared for the evaluation of installed beta LANMAS systems at SRS, Pantex, and INEL (SIMS). SRS is the first choice as it is farthest along in development, although it has been delayed for use since January till April.

We also began developing training and guidance materials for transfer of the evaluation methodology to DOE elements. These include briefing/tutorial materials, templates and protocols, and computerized spreadsheet calculation tools.

We presented a paper on the method for the LLNL Computer Security Practitioner's Conference, February 6-7, 1996. We submitted an abstract for the 1996 INMM Annual Meeting.

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

B&R No.	Funding	Obligated
GD 06-04-01	$73K	$4K

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 entered into discussions with TESA on the possible modification of the CT-20 to meet DOE requirements. 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.

APPENDIX A: SUMMARY OF ALL MILESTONES AND DELIVERABLES THIS QUARTER

I. DISS Personnel Security Network and Databases Modernization

B&R No. GH-03

Date	Implementation Milestones	Status
11/13/95	Begin NV Acceptance Test	Awaiting NV hardware
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	HQ Server shipped
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	

Date	Development Milestones	Status
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	Server shipped
12/31/95	CPCI Oracle–mainframe synchronization demonstrated	Expected 5/15/96
2/1/96	WDAC beta test begins	Server shipped

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	
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

Date	Milestone or Deliverable	Status
2/96	Extension to other computerized safeguards and security systems	Completed
3/96	Report on extension to other computerized safeguards and security systems	Draft
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

Date	Milestone or Deliverable	Status
10/31/95	First level project review	12/7/95 with Darryl Toms
4/30/96	Mechanical and electrical design drawings	

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

DISS VADB Interface Control, Version 1.02, January 6, 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 57 incidents and 24 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 161 actions, which include both phone and e-mail correspondence, that are required to track the cause of the incident and assist sites in responding appropriately.

The team responded to numerous viruses: Microsoft Word Macro, Good Times (the hoax continues), PKZip, Junkie, AntiCMOS, Monkey, Michaelangelo, Da'Boys, and the Joker. Intrusion attempts via the Internet continue: CIAC handled incidents involving ftp, e-mail spamming that forged a DOE site as the originator, sniffers, suspicious port scans, fingering, and unauthorized telnet and ftp attempts. A number of incidents involved intrusion attempts by individuals within the U. S., and involved agencies beyond the DOE.

The CIAC team will be participating in the 1996 DOE Computer Security Group Training Conference in Seattle, Washington. CIAC will be addressing several security topics which include: Annual State of CIAC, Status of the Threat, Securing Internet Connections, Secure Architecture, VAP Database, and Computer Viruses (Identifying, Handling, and the Cleanup Process).

II. Network Intrusion Detector (NID)

The NID iWatch evidence gathering operating model was used in the first court-ordered wiretap of a computer network.

III. AIS Alarm Project

We formed the initial project team and defined the joint project plan. We also set up the password-protected AIS Alarm Project web site on the DOE IS Server.

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

The SPI team continued gaining experience with the beta version of the SPI-NET multi-host security inspection package. Progress continued with the Tech Transfer planning process and documentation enhancements.

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

We presented a paper for the Security Practitioners Conference at LLNL and prepared materials for a presentation at the DOE Computer Security Group Training Conference. We developed a proposal for the development of an advanced firewall system.

VI. Profiling and Vulnerability Analysis Project (VAP)

We completed the database design, and have a working schema in place.

We installed an initial load of 25 vulnerabilities to test the design, and get a feel for the user interface.

VII. DOE Information Security (DOE-IS) Server

We continued to populate the server as an on-going activity. Highlights include: added all CSTC projects to the tools page (e.g., SPI, NID, etc.); added the Oak Ridge National Laboratory workstation day lock project to the tools section; added the CIAC Virus Database as an on-line database accessible from the web; and added pointers to the CTA and HR pages.

TASK DESCRIPTION AND QUARTERLY PROGRESS

I. Computer Incident Advisory Capability (CIAC)

B&R No.	Funding	Obligated
GD060603	$464K	$281K

The CIAC team members continued to assist DOE sites with computer intrusions, vulnerability assessments, security tools, evaluations, education, training, and awareness. Incident response continued to be the primary mission of CIAC.

The team responded to numerous viruses: Microsoft Word Macro, Good Times (the hoax continues), PKZip, Junkie, AntiCMOS, Monkey, Michaelangelo, Da'Boys, and the Joker. Intrusion attempts via the Internet continue: CIAC handled incidents involving ftp, e-mail spamming that forged a DOE site as the originator, sniffers, suspicious port scans, fingering, and unauthorized telnet and ftp attempts. A number of incidents involved intrusion attempts by individuals within the U. S., and involved agencies beyond the DOE.

CIAC continued to receive publicity and questions about the macro viruses. We were referenced in USA Today, Federal Computer Week, local TV Channel 30, The Times (local paper), and Computerworld. CIAC remains the focal point for macro virus information.

CIAC continued to improve its internal capabilities. CIAC enhanced its capabilities for managing incoming e-mail. The virus database continued to be updated. The CIAC virus database is now available on-line as a web page.

CIAC continued to participate in the FIRST organization. CIAC continued 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)

B&R No.	Funding	Obligated
GD060403	$297K	$117K

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

The NID iWatch evidence gathering operating model was used in the first court-ordered wiretap of a computer network. This generated very positive reviews of our capabilities.

Work continued on the development of an integrated graphical user interface for the NID product suite.

III. AIS Alarm Project

B&R No.	Funding	Obligated
GD060403	$500K	$21K

We formed the initial project team and defined the joint project plan. In conjunction with this, we developed reporting methods to DOE HQ and a detailed milestone schedule. We also set up the password-protected AIS Alarm Project web site on the DOE IS Server.

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

B&R No.	Funding	Obligated
GD060403	$223K	$128K

The SPI team continued gaining experience with the beta version of the SPI-NET multi-host security inspection package through field testing. The remote inspection system continued to be successfully tested in SunOS 4.1.2, SunOS 5.4 (Solaris 2.4), IRIX 5.3, and HP-UX 9.05 environments.

The VMS version of the SPI-NET remote inspection system continued to be tested with necessary enhancements and fixes.

Progress continued in the Tech Transfer planning process, with the submission of the plan and the drafting of a new SPI Commerce Business Daily announcement. SPI documentation continued to be improved in anticipation of the eventual Tech Transfer.

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

B&R No.	Funding	Obligated
GD060103	$221K (FY95)	$218K

We gave a presentation on firewalls for the LLNL Computer Security Practitioners Conference in February. We submitted an abstract to present the paper at the upcoming DOE Computer Security Group Training Conference.

We did not get on the schedule, but we integrated the materials into a presentation on securing Internet connections.

We were unable to find an appropriate commercial partner in time to submit a proposal to ARPA for developing an advanced firewall system. However, we worked with Sandia to submit a proposal to OSS for FY97. We believe that the type of technology we are exploring would be very useful for the national laboratories, especially in areas such as SecureNet.

VI. Profiling and Vulnerability Analysis Project (VAP)

B&R No.	Funding	Obligated
GD060403	$259K	$97K

We completed the database design, and have a working schema in place.

We installed an initial load of 25 vulnerabilities to test the design, and get a feel for the user interface.

At this time, we are beginning to investigate what external (protected) access mechanisms will be required. We anticipate that we will use a web server using Netscape's Enterprise server (available in May); utilize encrypted sessions; use links to the SQL server (Oracle); and maintain user names and passwords for each site through their local DAA.

VII. DOE Information Security (DOE-IS) Server

B&R No.	Funding	Obligated
GD060403	$150K	$24K

We continued to populate the server as an on-going activity. Highlights include: added all CSTC projects to the tools page (e.g., SPI, NID, etc.); added the Oak Ridge National Laboratory workstation day lock project to the tools section; added the CIAC Virus Database as an on-line database accessible from the web; and added pointers to the CTA and HR pages.

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

I. Computer Incident Advisory Capability (CIAC)

B&R No. GD060603

11 Bulletins/Advisories
- G-07: SGI Object Server Vulnerability
- G-08: splitvt(1) Vulnerability
- G-09B: Unix sendmail Vulnerability
- G-10A: Winword Macro Viruses
- G-11: HP syslog Vulnerability
- G-12: SGI ATT Packaging Utility Security Vulnerabilities
- G-13: Kerberos 4 Key Server Vulnerability
- G-14: Domain Name Server Vulnerabilities
- G-15: Sunsoft Demo CD Vulnerability
- G-16: SGI rpc.statd Program Security Vulnerabilities
- G-17: Vulnerabilities in Sample HTTPD CGIs

Notes 96-01: (1) Java and JavaScript Vulnerabilities
(2) FIRST Conference Announcement
(3) Security and Web Search Engines
(4) Microsoft Word Macro Virus Update

Changes to the CIAC Project Management Plan were completed and the document was delivered.

The CIAC document, "Computer Virus Information Update, CIAC-2301," was updated and delivered, meeting a milestone for this quarter.

The annual CIAC incident statistics report was completed and delivered, meeting a milestone ahead of schedule for the next quarter.

CIAC also updated the "Guide to the CIAC-2300 Series Documents." A new document was completed and released in the 2300 series entitled, "The Disinfectant Package for Macintosh Computers," CIAC-2315. All CIAC-2300 series documents are now available on-line, as fully formatted Adobe Acrobat files.

II. Network Intrusion Detector (NID)

B&R No. GD060403

No milestones or deliverables to report for this quarter.

III. AIS Alarm Project

B&R No. GD060403

No milestones or deliverables to report for this quarter.

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

B&R No. GD060403

The Tech Transfer plan was delivered and met the milestone for this quarter.

SPI documentation enhancements were made to anticipate the eventual Tech Transfer of SPI, and met the milestone for this quarter.

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

B&R No. GD060103

We presented a paper on firewalls for the LLNL Computer Security Practitioners Conference in February. We prepared material to be presented at the upcoming DOE Computer Security Group Training Conference.

VI. Profiling and Vulnerability Analysis Project (VAP)

B&R No. GD060403

No milestones or deliverables to report for this quarter.

VII. DOE Information Security (DOE-IS) Server

B&R No. GD060403

No milestones or deliverables to report for this quarter.

APPENDIX B:
LIST OF ALL PUBLICATIONS PRODUCED DURING THIS QUARTER

None.

Complex-Wide Access Control 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 all hardware and vendor software procurement for three enrollment/verification stations (LLNL development, DOE-Oak, DOE-HQ. Completed hardware assembly and checkout of the CWAC development and DOE-Oakland enrollment/verification stations.
2. Updated the definition of the interface between CWAC elements and the Visit Authorization Data Base (VADB).
3. Completed initial development of enrollment/verification station.

TASK DESCRIPTIONS AND QUARTERLY PROGRESS

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

B&R No.	Funding	Obligated
GD 060501	477K	256K

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

Quarterly Progress: Hardware and vendor-supplied software, including Oracle Secure Network Services has been received for all three enrollment/ verification stations. Two enrollment/verification stations have been assembled (LLNL Development System and DOE-OAK) and are operational. Assembly of the major components has been completed for the third enrollment/verification station. They will be connected and fully tested as we approach the scheduled time to install the system at DOE-HQ.

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 development has been completed to the point that we are able to communicate with a developmental version of the VADB to enroll badges and biometrics, and retrieve information for identity verification. (A demonstration of this capability was made at the April OSS Program Review at LLNL). The functions implemented in the CWAC Enrollment/Verification Station and which are operational with the developmental VADB include:

1) Encoding badges - This function uses the badge S/N and SSN from a pre-enrollment file, and a DES key generated by the E/VS.
2) Enrolling badges - This function acquires PIN and weight information, and encrypts it using the DES key read from the worker's badge. It also acquires hand geometry information. Badge information (badge S/N, badge status, PIN/weight encryption block, expiration date, and comments) and biometrics data (biometrics type, biometric preference, and biometric template(s)) are enrolled in VADB and associated with an existing "person" record.
3) Badge verification - This function reads the badge S/N and DES key from the worker's badge, and acquires a PIN from the worker while his/her weight is measured. It then uses the badge S/N as an index to obtain encrypted PIN/weight information from VADB. Using the DES key read from the badge, the E/VS decrypts the VADB PIN/weight data and compares it to the information acquired from the worker.
4) Biometrics verification - This function reads the badge S/N from the worker's badge, and uses it as the index to obtain the biometrics data contained in VADB. It then acquires a biometric measurement from the worker, and compares it to the VADB biometric data to ensure there is a match.

5) Display user/badge/access/enrollment information - This function requests VADB person, badge, clearance, and biometrics information for display to the E/VS operator. Information is requested using either the worker's SSN or Badge S/N as the search index.

6) Validate user by biometrics template - This function uses the worker's SSN as the index to obtain biometrics data contained in the VADB. It then acquires a biometric measurement from the worker, and compares it to the VADB biometric data to ensure there is a match. This function is especially useful to verify identity of an individual who may have lost his/her badge.

Several enhancements will be provided to supplement this basic functionality:

1) Providing a configurable selection to allow users to enter their weight through a keypad. This will provide an option which will avoid the cost of installing a weighing system.
2) Creating a "person" record in VADB for uncleared workers. For enrollment of cleared workers, person records associated with clearance records already exist. Since VADB will not provide the capability to create person records for workers not being processed for clearances, the E/VS must provide this capability. This function is required to provide complete standard badge accountability throughout the complex.
3) Enrolling badge and biometrics information for a worker with a standard badge that was encoded by another system. This is required for situations such as at DOE-HQ, where badges have been encoded but not enrolled in VADB.
4) Implementing a transaction queue for enrollment data. This will be useful for cases where workers are being enrolled at a high volume, but either the VADB servers are not functional, or the communication lines are down. This function will allow all enrollment information to be acquired as scheduled, and to be transmitted to VADB when communication is restored.
5) Update and maintain badge status information. 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 will be provided in the 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: An initial software design has been developed for the Argus ACS/VADB interface. A substantial part of the ACS/VADB software

interface will utilize software developed for the enrollment/VADB interface. Software development will commence after the enrollment/verification software enhancements discussed previously have been implemented.

A firewall design has been developed to ensure appropriate security is provided for connection of the LLNL Argus production system to DOEBINET. This firewall will restrict communication between Argus processors and VADB. The design has been reviewed, and will be implemented following successful completion of an associated Vulnerability Analysis.

For planning purposes only, the definition of the developmental interface between CWAC elements (enrollment/verification station, access control system) and the VADB has been distributed to attendees at two Quality Panels, and to interested individuals. Recipients of this information have been cautioned to not use it for interface design until the feasibility and performance of the interface have been demonstrated.

IV. **Provide installation requirements, support installation, test and activate an enrollment/verification station at DOE-OAK. 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: Two visits were made to the Federal Building in Oakland to survey potential locations for the DOE-OAK E/VS. Installation requirements and data were transmitted to DOE-OAK personnel. We provided a sketch of a proposed equipment arrangement, including badge production equipment, in the location initially preferred by DOE-OAK. We have requested that DOE contacts be identified regarding connection to and utilization of DOEBINET (DOE Business Information Network), the frame relay system which we intend to use for communication with VADB.

Communication between the enrollment/verification station and VADB using Oracle SQL*Net was demonstrated at the DOE OSS Program review in early April.

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

Quarterly Progress: No activity this quarter, since the DOE-OAK enrollment verification station is not yet operational.

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: No activity this quarter.

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: An FY98 Field Work Proposal was prepared for the CWAC project. This FWP proposed an expanded scope for FY97 to address additional CWAC implementation requirements, including active VADB notification of badge "hot-stops", and use of PSAP certification data for selected access control decisions.

A presentation concerning the purpose of complex wide access control, CWAC project objectives, design criteria, and status was given at a February Access Control Systems Quality Panel meeting in Las Vegas.

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: SUMMARY OF ALL MILESTONES AND DELIVERABLES FOR THIS QUARTER

MILESTONES STATUS TABLE

Original Milestone	Description of Milestone	Status
1/30/96	Demonstrate ACS/VADB communication between the Argus development system (with CAIN booth) and a development VADB (unencrypted communication)	CWAC Change Proposal 3a* submitted to change date to 5/31/96
2/28/96	At LLNL, demonstrate encrypted communication between a CWAC enrollment station and the pre-operational VADB	CWAC Change Proposal 3b* submitted to change date to 4/30/96
2/28/96	Begin operation of LLNL Argus production ACS connected to pre-operational VADB for production shake down	CWAC Change Proposal 3c* submitted to change scope and date of milestone
3/30/96	CWAC enrollment station installed at DOE-Oakland (but not tested)	CWAC Change Proposal 3d* submitted to change date to 6/30/96

* LLNL FESSP Letter 96-0448, dated 4/12/96

APPENDIX B: LIST OF ALL PUBLICATIONS PRODUCED DURING THIS QUARTER

Complex Wide Access Control Functions and Requirements Document, Version 1.1, dated January 18, 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

For the period 1/1/96 through 3/31/96

I. Preparation and presentation of Argus Lifecycle Cost analysis at the 2nd Access Systems Quality Panel meeting in Las Vegas.

II. As a part of the Federal standardization effort, work was done identifying the commonalties of the DOE, DoD, and NSA badge systems.

III. The Argus Homepage has been operating throughout the quarter with secure sockets and secure registration enabled. Individuals from two sites have been allowed to log in and to evaluate the homepage.

TASK DESCRIPTIONS AND QUARTERLY PROGRESS

B&R No.	Funding	Obligated	
GD 06 0201	$96K	$79.4K	as of 3/30/96

I. **Support for the DOE Access Systems Quality Panel meeting**
The first comprehensive document on Argus system lifecycle costs was prepared by Erv Behrin Security Consultants (EBSC). It provided a detailed breakdown of job functions and staffing requirements for a large facility using Argus. It drew on the experience at LLNL and at the National Test Facility. The Sandia SAMACS document was also reviewed and extensive comments made.

II. **Standardization of Federal Systems**
The badge plans for the DoD were reviewed and contrasted with the DOE badge and infrastructure plans. NSA plans were also discussed. From the information provided by DOE HQ, it is clear that although the DoD and NSA intend to produce a common system across their agencies, there has been little design effort put into defining the infrastructure necessary to support a common system. Most notable, the information that must be transferred and the need to protect it does not seem to be addressed. This is an area where the DOE has put considerable effort and can contribute significantly to the discussion of a common federal badge system. It also can have a significant impact on the viability of various magnetic encoding schemes being considered.

III. **Argus Homepage**
This quarter saw a major security enhancement of the Argus Homepage with the fielding of Star-Nine's Webstar secure communications. The Secure Sockets Layer (SSL) capability was activated in February for the Unclassified Argus Internet Homepage. The security capabilities that this added are described below. Another security feature was that all generic passwords were removed and a user registration form was placed on line.

The activation of the Secure Socket Layer was not without problems. There was a conflict with the server software and Apple Computer Company's "Open Transport" system communication software which neither Apple nor Star-Nine were able to immediately resolve. It turned out that the problems were platform dependent, so the homepage was temporarily moved to a different platform.

This quarter has continued the steady improvement to the webpage. All released documentation have been linked to the webpage, as well as all current console software release notes.

The webpage is ready to open a page for the DOE Access Systems Quality Panel minutes and schedule of meetings. We await HQ approval to make the webpage available to the community of DOE and other Argus users.

IV. Argus Web Server Protection

he Argus Web Server is designed to provide unclassified information about the Argus Security System to its users throughout the Department of Energy community using the Internet and World Wide Web technology. The use of WWW technology will allow the timely dissemination of important Argus system information that will help educate current Argus users and serve to improve the usability of the system at their site. It will also assist DOE sites in planning for the DOE standard system. While unclassified, it is felt that the distribution of Argus information must still be conducted in a secure manner. This protection is necessary to prevent unauthorized individuals from gaining technical insight that might be used against an Argus installation in ways unforeseen at present. The Argus Web Server system was specifically designed to make use of the latest Internet communication technology in such a manner that the security and integrity of the Argus system would not be compromised or put at risk.

The Argus Web Server system currently serves two different types of informational documents or "pages" to the World-Wide Web: unrestricted and secure. The unrestricted page(s) have specifically been designed so that they can be accessed by anyone from the Internet. Due to this unrestricted access, no substantive information regarding the Argus Security System is actually contained within these pages. In practice, only one information page actually falls in the unrestricted category. This page, know as the Argus Home Page, is provided mainly as a common entry point (HTTP://argus.llnl.gov) for all users who have a legitimate need to access Argus Web information. The remainder of the Argus pages fall into the secure category.

Secure information pages are protected in several ways. Secure pages are served using the Webstar Secure Sockets Layer (SSL) server software. All such pages are transmitted over the Internet in encrypted form using RC4-128, RC4-40, or DES encryption. All secure Argus pages are grouped into a security "realm" which requires a username/password to access. Additional security realms can be added by the Argus Webmaster at any time to add greater security granularity. Users may request a password through an enrollment page which is also protected by encryption. Usernames and passwords are transmitted only in encrypted form across the Internet both during

enrollment and during regular page access. User accounts are only granted with the express permission of the FESSP Associate Program Leader for Security and Automation Technology at LLNL. To prevent the theft of passwords via masquerading, the identity of the Argus server is automatically authenticated and can be examined by the user at any time. The Argus Web Server holds a certificate of authenticity which was issued by the Secure Server Certification Authority, RSA Data Security, Inc.

In order for any information to appear on an Argus web page, it must first be reviewed and approved by a knowledgeable Authorized Derivative Classifier (ADC). Furthermore, all Argus library documents available on the Argus Web Server have successfully completed the Laboratory's Technical Information Department review and release process.

The Argus Web Server is physically protected in a locked room located within a Q-access limited area at LLNL. At present, only a very small number of individuals (the Webmaster and authorized LLNL Argus system managers) have login access to the server. In addition, all Web accesses are logged and routinely audited by the Argus Webmaster. The sever computer itself is dedicated entirely to Web Server operations and provides no other Internet services or user functions.

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	
5/1/96	Report on DOE contribution to the Federal Standardization of electronic security systems	D	
6/15/96	Update of Argus Functional Description	D	
6/30/95	Demonstration of DOE's electronic security systems concepts	D	
9/1/96	Argus Advisory Group meeting support	M	
9/13/95	Host DOE community at an Argus Technical Interchange Meeting	D	
9/30/95	Argus Homepage report	D	

M=Milestone
D=Deliverable

APPENDIX B: LIST OF ALL PUBLICATIONS PRODUCED DURING THIS QUARTER

Argus Homepage HTML files

Information Technology & Security Center

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

INTRODUCTION

The Fission Energy and Systems Safety Program (FESSP), Information Technology and Security Center 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

- Continued development of the Geographical, Environmental & Siting Information System (GEn&SIS) for the Nuclear Regulatory Commission (NRC) Office of Nuclear Reactor Regulations (NRR).
- Continued development of the U.S. Business Advisor for the Small Business Administration (SBA) and the National Performance Review (NPR).
- Continued 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).
- Continued development of RuleNet for the U.S. Nuclear Regulatory Commission (NRC) Office of General Council (OGC).
- Continued development of SARNet for the Department of Energy (DOE) Office of Defense Programs (DP).
- Implementation of Collaborative Work Environment using NetForum and NetDoc for DOE Department Standards Committee (DSC).
- Implementation of a Collaborative Work Environment using NetForum and NetDoc for DOE Performance Measurement Coordination Team (PMCT).

TASK DESCRIPTIONS AND QUARTERLY PROGRESS

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

B&R No.	Funding	Obligated
	$200K	$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-on work by NRC and DOE. DOD has formally requested the source code developed in the pilot for use in DOD Acquisition Reform efforts. GSA, NRC, DOE, and Treasury are discussing with us the possibility of follow-on work using the NetForum and NetDoc software (EOM System).

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

Date	Milestone or Deliverable	Status
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 - draft generated 3/27/96
9/30/95	Provide DOE with requirements detailing the functionality of the web-based methodology	Milestone not met - draft generated 3/27/96
9/30/95	Provide DOE with plan for convening a second EOM	Milestone not met - draft generated 3/27/96
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 - draft generated 3/27/96

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 - draft generated 3/27/96

APPENDIX B: LIST OF ALL PUBLICATIONS PRODUCED DURING THIS QUARTER

None this quarter.