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

Quarter Ending June 30, 1996

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

RECEIVED
AUG 16 1996
OSTI

July 1996

This is an informal report intended primarily for internal or limited external distribution. The opinions and conclusions stated are those of the author and may or may not be those of the Laboratory.

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

DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED

als
MASTER

DISCLAIMER

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

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

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

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

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

Quarter Ending June 30, 1996

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

July 1996

DISCLAIMER

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

Table of Contents

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

Task Descriptions and Quarterly Progress.....	SMA-2
I. DISS - Electronic Transfer of Personnel Security and Personnel Security Database Modernization Technology Development.....	SMA-2
II. Risk Based Evaluation of Computerized Nuclear Materials Accountability Systems.....	SMA-9
III. Z-Lock Electro-Mechanical Lock for Administrative Control LLNL-438.....	SMA-9
SMA Appendix A: Summary of all Milestones and Deliverables for This Quarter.....	SMA-11
SMA Appendix B: List of all Publications Produced During This Quarter.....	SMA-13
 Computer Security - Distributed Systems	CSDS-1
Introduction.....	CSDS-1
Summary of Major Accomplishments.....	CSDS-1
Task Description and Quarterly Progress.....	CSDS-3
I. Computer Incident Advisory Capability (CIAC).....	CSDS-3
II. Network Intrusion Detector (NID).....	CSDS-4
III. AIS Alarm Project.....	CSDS-4
IV. Security Profile Inspector for Unix and VMS Operating Systems (SPI/UV).....	CSDS-5
V. Profiling and Vulnerability Analysis Project (VAP).....	CSDS-5
VI. DOE Information Security (DOE-IS) Server	CSDS-6
CSDS Appendix A: Summary of all Milestones and Deliverables for This Quarter.....	CSDS-7

CSDS Appendix B: List of all Publications Produced
During This Quarter..... CSDS-8

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

CWAC Appendix B: 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
Appendix A: Summary of all Milestones and Deliverables for This Quarter.....	SSS-4
Appendix B: List of all Publications Produced During This Quarter.....	SSS-4
 Information Technology & Security Center.....	 ITS-1
Introduction.....	ITS-1
Summary of Major Accomplishments.....	ITS-1
Task Description and Quarterly Progress.....	ITS-2
ITS Appendix A: Summary of all Milestones and Deliverables for This Quarter.....	ITS-3
ITS Appendix B: 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 Third Quarter of Fiscal Year 1996 (April through June, 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.

The Safeguards Technology Program team presented a review to Dr. G. Dan Smith and other members of the Planning and Technology Planning Branch on April 10, 1996 at the Lawrence Livermore National Laboratory.

SUMMARY OF MAJOR ACCOMPLISHMENTS

I. Development of Advanced Isotopic Analysis Software

- An MGA++ software program with a pre-screen module than can determine the appropriate assay methodology and call the MGA, MGA-hi (PU600), and U235 modules as necessary has been demonstrated.

II. Emission/Transmission Computed Tomography

- Scanner system data acquisition capabilities have been exercised using a PIDIE plutonium source.

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

- Preparation of the Monte Carlo simulation software for application of general users has begun, including preparation of templates for input files.

TASK DESCRIPTIONS AND QUARTERLY PROGRESS

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

I. Development of Advanced Isotopic Analysis Software

<u>B&R No.</u>	<u>Funding</u>	<u>Obligated</u>
GD060402	\$350K	\$236K

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) has been successfully demonstrated, and was presented at the review in April. In this demonstration, the pre-screen model was able to select the appropriate analysis module by doing a variety of tests on the data file itself, with no intervention by the operator.

The present software consists of five separate modules in a Win32 environment: executive capable of selecting between the three analysis methodologies, the MGA, the MGA-hi (PU600), 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 to decide which analysis application to use, based on the data itself in the spectral file. The intelligent pre-screen, graphics, and the analysis methodologies can all be enhanced independently under this scheme.

Software for assay of Uranium

DeLynn Clark

A computer program has been written that can non-destructively evaluate the percentage of ^{235}U in a uranium sample from the analysis of the emitted gamma rays. The program, U235, is operating and work is underway to improve the accuracy of the assay, particularly at the high (>90%) and low (<0.7%) enrichments. At this point accuracies to within + 2% have been demonstrated for uranium samples with enrichments ranging from 0.017% to about 99%. This software has

been tested with some uranium samples contaminated with plutonium, samples that cannot be assayed with MGAU or other standard codes. Early results show accuracies to within less than 10% for these contaminated samples. The only other method to assay these samples, hands-on analysis using GRPANL, gives assays that vary from the known assay by 23% or more. Work continues to test this software module on as many uranium spectra as possible. The test version of the program has been made operable as one of the analysis methodologies of MGA++, and has been successfully demonstrated.

Gamma-Ray Line Shapes from CdZnTe Detectors

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

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.

The gamma-ray line shape parameter study is essentially complete, and a report of the results is being prepared. A preliminary report of the results was presented ACS symposium on Nuclear and Isotopic Methods of Analysis for Safeguards and Security in March.

The results of this work is being incorporated into uranium analysis software being developed under a CRADA with EG&G Ortec. This software, CZTU, will analyze data taken with cadmium-zinc-telluride detector also under development at LLNL with the support of EG&G Ortec. CZTU is being designed to operate within the MGA++ framework, and it can be included in a comprehensive software suite. This software will include capabilities for Pu detection, and the detection of medical and industrial isotopes. In addition to EG&G Ortec, Euratom, and soon ISPO/IAEA are providing some support for this software development.

Licensing of MGA++ based Software

William M. Buckley, Wayne Ruhter, and Robert Lanier

Discussions with vendors on the licensing of MGA++ based software are continuing. Necessary documents are being prepared by LLNL personnel, in consultation with the LLNL legal office. A meeting with EG&G Ortec is planned for July for the specific purpose of licensing MGA++ technology with the current LLNL production version of MGA and the CZTU code, followed by the U235 code. After this first round of discussions is complete, we intend to start licensing discussions with Aquila Technologies, BNFL Instruments, and Canberra Industries.

II. Emission/Transmission Computed Tomography

<u>B&R No.</u>	<u>Funding</u>	<u>Obligated</u>
GD060402	\$150K	\$116K

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

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

Emission and Transmission Computed Tomography Application

Tzu-Fang Wang

A criticality analysis for 300 g of ^{239}Pu has been completed for our Operational Safety Procedure for use of the tomographic scanner (now approaching 9 months in the approval process). If it is approved in July, we will have two months in which to complete the proposed scan of the molten-salt-extraction button. Two months is enough time to complete this scan.

In lieu of the use of a MSE button, we have completed a passive computed tomography scan of the PIDIE #7 source with the 5 mm x 2 mm collimator to test overall operation of the scanner system. An intermittent problem has been discovered that shuts off the detector high voltage bias. This problem has been attributed to an interference between the Ortec 92X spectroscopy electronics and the staging control system. We are currently debugging this problem.

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

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

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

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

Evaluation of Uranium Spectra

DeLynn Clark, and Kenneth E. Raschke

A subset of high enriched uranium samples held by the Materials Management at LLNL are contaminated with plutonium. Standard uranium assay software such as MGAU can not assay spectra from these samples. An analyst-controlled analysis of these spectra using a custom setup of GRPANL has been used to determine the uranium isotopics of two of these samples, with poor results. A test version of the U235 code has been applied to two of these spectra, and the assay of ^{235}U agrees with the declared value of within 10% for one sample, and 5% for the second sample. These results represent a substantial improvement over previous results.

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

<u>B&R No.</u>	<u>Funding</u>	<u>Obligated</u>
GD060402	\$175K	\$110K

The simulation of gamma-ray spectra for a known radioactive source, sample matrix, and geometry can be an important tool in designing and understanding non-destructive analysis (NDA) instruments such as Pu and U gamma-ray isotopic analysis systems. There are also a number of significant and major MC&A problems associated with heterogeneous materials, lump corrections, holdup, waste, and shipper-receiver measurements that can be addressed with this calculational tool. The gamma-ray spectra from each of these problems can be simulated with a Monte Carlo method by mocking up various geometries and transporting the gamma-rays of a known source through the material to a detector. Monte Carlo calculations may be used to calculate plutonium "standard" gamma-ray spectra that may be used to determine such characteristics as systematic biases in spectral data-analysis codes. With so many possible variations of the problems described above, the simulation

of gamma-ray spectra from them is more efficient and cost effective than the development and measurement of various reference materials.

Simplification of the Monte Carlo Calculation of Gamma-Ray Spectra

Tzu-Fang Wang

We have started to simplify the software codes and input files to make them easier to use on personal computers. One aspect is to simplify the MCNP code by limiting its capabilities to photon transport and interactions, eliminating subroutines dealing with neutrons, and modifying many others to make the program much smaller. Of 345 subroutines, 21 dealing with neutrons will be eliminated, and about 175 others will be essentially eliminated by rewriting parts of some crucial subroutines. The result will be a substantially stream-lined computational code. A second aspect is to set up input files so that the general user can set up his own specific simulation, with no detailed knowledge about MCNP being required on the part of the user. Templates for common or typical problem input files are being developed for this purpose.

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

<u>B&R No.</u>	<u>Funding</u>	<u>Obligated</u>
GD060402	\$75K	\$26K

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

It is well known that the leading edge of signals from solid state detectors displays details that arise from the particulars of the interaction of the incident gamma-ray (amount of energy deposited and locations of deposition) and the properties of the detector (electric field, charge carrier traps, etc.). If the detector response is understood, which is the case for high purity germanium detectors (HPGe), these signal details can be used to correct individual signals, thus improving the measured spectrum. We have already established the proof-of-principle that signals from conventional coaxial HPGe detectors can be unfolded with sufficient accuracy to determine the radial locations where energy is deposited with good resolution (about 2 mm). Our algorithms utilize this location information to perform Compton suppression without anticoincidence detectors. Monte Carlo predictions show that it should be possible to choose algorithm parameters that would actually allow nuclear assays to be performed in less time. To test this hypothesis we propose to apply our algorithm to measurements of gamma-rays from nuclear material samples of interest to materials control and nonproliferation. We will test the effectiveness of the algorithm and optimize the algorithm parameters. We will implement our algorithm with a digital signal processor in order to perform the

Compton suppression in real time. If successful, this work could lead to improved techniques for materials assay. When used with cryo-cooled HPGe detectors, our signal processing system and algorithm would enhance capabilities for remote assays.

Signal Processing

Dean Beckedahl and Judith Kammeraad

We are moving our experimental equipment, including HPGe detector, associated electronics, and special gamma-ray shielding, from the ATLAS test facility at North Los Vegas to the Isotope Sciences Division at LLNL where it is being reassembled. Other equipment necessary for the demonstration that will be integrated with the above experimental equipment, the signal digitizer and digital signal processor, has been ordered or is in the process of being ordered.

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

<u>B&R No.</u>	<u>Funding</u>	<u>Obligated</u>
GD060404	\$25K	\$6K

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

Report Planning

Eugene A. Henry

Preliminary planning has begun for the status report task. An experienced technical editor has been identified as well as design and production resources. A tentative schedule has been laid out leading to publication of the report in January 1997. A preliminary contact by telephone has been made with the points-of -contact for the projects identified by the Planning and Technology Development Branch.

VII. Other Related Activities

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.

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

I. Development of Advanced Isotopic Analysis Software

B&R No. GD060402

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

Conclude development phase of MGA-like code for analyzing uranium spectra--prototype test program available 5/96, report available 8/96.

Peak shape fitting methodology for CdZnTe spectra--concluded 5/96, report 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. GD060402

Continue studies and analyses of layered and shielded SNM materials to optimize measurement parameters--Studies of the MSE button are delayed because of OSP approval. Report on a 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--prototype software in place 2/96.

III. 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 for Calibration

B&R No. GD060402

Evaluation and testing of MGA analyses of plutonium samples in DOE-approved thick steel containers -- testing complete 3/96, report to be available 9/96.

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

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

B&R No. GD60402

Assemble demonstration hardware; purchase digital signal processor--begun 5/96.

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

B&R No. GD60404

Start process leading to publication of OSS Technology Development report--begun 5/96.

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

None this quarter.

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 AL
- DISS Rel. 2.1 released to beta testing

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	\$4,200K	\$2,398K
GH-03 carryover	\$ 895K	\$ 895K

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

DISS Release 2.0 is completed and has been installed and acceptance tested at DOE OAK, SR, RL, SNR, and AL 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 beta testing.

Production

The current production release of DISS is the baseline DISS Release 2.0.2; The request for release approval was been submitted to DOE HQ on June 11, 1996. Version components of this baseline are listed below. Release notes for 2.0.2 have been prepared and will be made available on the DISS homepage (<http://diss.llnl.gov>) on the Released Project Documents page in June.

DISS Release 2.0.2 Baseline	
module	version
CDUI	2.0.2
Admin Client	1.0.1
Notary	2.05
RPS/OPM Unix software	Build_2_0_2
RPS Database	RPS_2_0_1d.tar plus patches to bring definition to 2.0.2 Patches that bring 2.0.2 definition to 2.0.3 are currently being applied in the field and documented by Specification Exception Release (SXR).

Deployment/Operations Support

Operations support for deployed sites is continuing to exceed the planned level of support designated for these activities. Impact of this increased level of deployment/operations support is currently being felt across the design team. Multiple, parallel deployment, operations, and design activities are frequently placed in competition for limited design team resources, sometimes necessitating weekly or even daily reprioritization of directed support. This has resulted in complaints from field activities that suffer as a result of design team support of other higher priority activities.

Savannah River

Savannah river is in production operation. Monitoring of the OPM gateway indicates that SRS is sending approximately 10-13 cases to OPM daily since cutover to production.

During the week of May 20th, members of the LLNL DISS team traveled to Savannah River to finish data conversion begun by DynCorp and finalize deployment to permit production usage of the DISS system. The trip proved very successful. The following was accomplished:

- (1) Successfully imported 10,865 out of 10,874 historical datafiles into the RPS system. The 9 that didn't import will be examined for data problems, and may be hand-entered if necessary. The sizing of the SRS RPS database proved to be fully capable of handling the number of imported cases with plenty of space to spare.

- (2) Successfully completed the SRS link to OPM, sent test cases to demonstrate correct end-to-end functioning and observed while Savannah River sent 2 live cases on Friday, May 24. System response time was around 20 minutes to receive acknowledgment of successful transmission back from OPM.
- (3) Deployed the latest production releases of the CDUI and Admin Client to DOE SRS and Westinghouse.
- (4) LLNL team met with DOE SRS, Westinghouse, and Wackenhut clearance offices to observe operations methods and discuss options and enhancements for DISS. They were able to discuss issues common to operations staff and share direct experience that should prove invaluable to the DISS design team for future system enhancements.
- (5) Provided post-deployment support for an additional 2 days to help insure that the system was production ready, observe the successful transmission of live cases to OPM, install upgraded production software, and be available to answer questions.

Savannah River is now a production RPS site, actively sending live cases successfully to OPM. We see no difficulty with SRS moving to a full production capacity of 20 cases per day (or more).

Richland

The Richland RPS database has been upgraded to the latest DISS production release (2.0.2 plus patches to 2.0.3). This upgrade was completed during the week of July 8. The LLNL DISS design team is currently assisting RL technical staff with data conversion efforts.

Schenectady

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

DOE Oakland has been upgraded to DISS 2.0.3 and is ready for production operations.

DOE HQ and Chicago

The PSDB server version 2.1b1 and CPCI Client version 1.0b1 were installed for beta testing at DOE HQ during the week of May 6th. NN-512 beta test activities are currently underway. Beta versions of the WDAC client has been installed

with DP 45. The HQ and Chicago RPS has been installed. RPS acceptance testing is scheduled for late July.

An initial plan for deployment of the Release 2.1 project deliverables was presented at the July 9th meeting of the DISS Change Control Board. An abbreviated outline of the plan is as follows:

1. Establish Mainframe data feed for PSDB server.

This task will involve completing the "PSDB Import" utility that will convert mainframe data to PSDB format and load it into PSDB server, release the PSDB server to production from it's current beta-test status, and then begin running the PSDB import utility as a nightly process to feed live clearance data into the PSDB server. The PSDB server will then be a mirror of live production data, thus permitting DAVAC and VADB produce same results (query same data), and so VADB cutover can begin.

2. Deploy VADB to field.

This task will involve identifying existing DAVAC users, establishing new PSDB accounts for them, installing Netscape web browser software on PC's accessible to DAVAC users, and establishing net access where required for those DAVAC users without direct connection to the local site's network. VADB training can proceed once browser software is installed and operational. Cutover to VADB from DAVAC can proceed on a site-by-site basis.

3. Deploy CPCI to field

This task can be performed concurrent with 2.0 deployment, and/or VADB deployment, or as a separate tasking. CPCI can be installed on the same workstations as the CDUI application. CPCI will initially be pointed as a training server located at LLNL, not the headquarters PSDB production server.

4. Once VADB fully deployed, begin CPCI cutover

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

We expect to release PSDB server and begin one-way feed as soon as the PSDB import function is completed; currently this is forecast for late August. Netscape installations, user enrollment, DAVAC user identification, and determination of net access can begin immediately (LLNL design team resources permitting); CPCI deployment can begin as soon as it is released from beta. An estimate of the time needed to complete VADB deployment is in preparation. The time will be dependent on the results of a DAVAC user data and site location survey.

Albuquerque

Albuquerque DISS system successfully completed Acceptance testing. Equipment for DOE Albuquerque was received at LLNL in April. Configuration of the RPS database and firewall were undertaken during the weeks of April 22 and 29. A bug in the Oracle installation of the RPS database required several days to troubleshoot and necessitated reporting to Oracle's in-house technical support staff for resolution. This delayed end-to-end checkout of the RPS and Firewall, however, the end-to-end was successfully completed and the hardware shipped to Albuquerque on May 15, and was reported received and unpacked by the DynCorp team on-site for deployment on May 16. The planned upgrade to RPS 2.0.3 has not yet been scheduled.

Nevada

Configuration of Nevada hardware at LLNL is currently underway.

Oak Ridge

Configuration of the Oak Ridge RPS and Firewall hardware is scheduled to take place at LLNL during the weeks of July 22 and July 29.

OPM

A problem identified with the OPM firewall has been found to be related to insufficient system resources (disk space and memory) on the AIX computer. Symptoms include occasional garbling of PEM email at an unacceptable rate for full production usage when all sites are completely deployed and operational. 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 has analyzed OPM firewall load requirements in light of actual empirical data (unavailable at design time), and will forward recommendations for the purchase of increased disk storage and memory to DOE HQ as soon as we receive cost information from the vendor. The DISS team will be performing daily direct monitoring of the OPM gateway to insure correct production operations while the equipment is on order.

Calls were received by the DISS Helpdesk during the week of June 3rd that indicated that OPM operators were having difficulty uploading cases from the DISS OPM Gateway computer to the PIPS mainframe. The DISS Helpdesk proceeded with troubleshooting, and a DISS team member stationed in the FESSP Germantown offices was dispatched for direct on-site troubleshooting at OPM on June 11, 1996.

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. This is consistent with HQ's latest guidance to the

field on electronic transmission of fingerprints until Identicator software problems are overcome.

Release 2.0 Maintenance (WBS#2.1.5)

Analysis of the RPS database has uncovered undersize conditions. These problems affect RPS databases deployed in the field that are version 2.0.2 and lower. The effect of these conditions is to limit the number of cases that can be stored and processed on the system before archival is necessary to an unacceptably low number (potentially less than 300, depending on case size and number of scanned documents). A software fix to correct these sizing constraints with existing RPS hardware has been identified and a patch to correct the problem for production systems is being applied to all fielded systems that brings the RPS database up to RPS version 2.0.3. This patch has been applied to Savannah River, Richland, and Oakland; Sites under deployment (Albuquerque, HQ, and Chicago) will have the patch applied prior to completion of acceptance testing. Other deployed sites will be scheduled. New builds (Oak Ridge, etc.) will be built to the 2.0.3 definition.

Release 2.1 Development

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

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

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

The PSDB server v2.1b1 was released to DOE HQ for beta testing during the week of May 6. Beta 2 incorporating bug fixes and enhancements is expected to be available for release on or before August 15, 1996.

The CPCI Data Sync utility is intended to provide two-way synchronization of active clearances between PSDB and the existing mainframe for the limited period of time that R2.1 deployment requires. This synchronization will support old DAVAC and new VADB during the interim while some sites are still using the old mainframe and other sites are using the newly deployed R2.1.

Because of difficulties encountered in development, the Data Sync utility is being re-scoped to provide one-way data transmission of all mainframe CPCI clearance data (not just active clearances as previous) to the PSDB server. This will permit the R2.1 deployment planning to proceed on schedule. The re-

scoped CPCI data sync will be referred to as "PSDB Import utility" and will be available with the next version of the PSDB by August 15.

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

The CPCI user interface v1.0b1 was released to DOE HQ for beta testing on March 29, 1996. We are making changes to the interface based on NN512.2 requests and CPCI 62 will be available for release concurrent with PSDB server 2.1b2 by August 15, 1996.

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

The WDAC DP-45 interface and WDAC Web Client are currently in beta testing.

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

The VADB Web interface is in beta test and integration testing is continuing.

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

CWAC support functions are in test.

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

Both Applicant User Interface (AUI) and Applicant Diskette Interface (ADI) have completed development and was released to test May 20, 1996. Release to production forecast for July 30, 1996. Posting of the AUI to McIntosh has begun.

Release 3.0 Development

- **OPM Oracle Database**

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

- **Scanned Document Viewer - Notary replacement**

The scanned document viewer/binary image loader is under development. This is intended to provide a replacement for the current Notary as part of Release 3.0. A subset of the document viewer/printer functionality is being incorporated into CDUI 2.1 and is expected to be release to test the week of June 10.

A subset of the document viewer/printer functionality is being incorporated into CDUI 2.1 and is currently in integration testing.

- **Low Cost Enrollment Station**

We completed an internal draft of a Requirements and Functional Specification document. We completed site visits to LLNL and ORNL. The results of these visits are reflected in the specification.

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	\$121K
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).

In the latest quarter this project has focused on four thrusts : 1) extension of the methodology; 2) evaluation of installed Local Area Network Materials Accounting Systems (LANMAS); 3) training and transfer of the technology; and 4) collateral activities. In order to extend the methodology to other information based systems, two developments have been accomplished. One is an approach for generalizing the application of evaluation criteria, and the other was the completion of an aggregation approach for 'scoring' the effectiveness of different system designs against insider threats. These developments are being included in a draft report. There are currently five LANMAS-type systems we are looking at in the complex: SRS, Hanford, Paducah, INEL, and Pantex. We developed structured questions for performing assessments and tradeoffs of the LANMAS security features, and visited SRS to evaluate their planned LANMAS implementation using the developed methodology. We have continued the development of methodology training and technology transfer materials and tools, including tutorial briefing materials, guidelines, and templates and elicitation forms. Collateral activities include the re-writing, after receiving review comments, of our methodology report; preparation of a paper for publication at the 12th Annual ADPA Symposium on Security Technology; and preparation of another paper for presentation at the 1996 INMM Annual Meeting.

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	\$73K	\$20K

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

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

I. DISS Personnel Security Network and Databases Modernization

B&R No. GH-03

<u>Date</u>	<u>Implementation Milestones</u>	<u>Status</u>
11/13/95	Begin NV Acceptance Test	System build in process
1/15/96	Begin RL Acceptance Test	Complete
2/12/96	Begin SR Acceptance Test	Complete
2/26/96	Begin SNR Acceptance Test	Complete
4/22/96	Begin CPCI/WDAC/VADB Acceptance Test	Beta testing
5/20/96	Begin AL Acceptance Test	Complete
6/17/96	Begin OR Acceptance Test	System build July 22, 1996
7/8/96	Begin HQ Acceptance Test	July 22, 1996
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 2.1 Operational Readiness Review	10/30/95
11/30/95	Standalone HQ server and network operational	5/9/96
12/31/95	CPCI Oracle-mainframe synchronization demonstrated	One-way complete
2/1/96	WDAC beta test begins	5/27/96
3/15/96	Integration testing of all standalone centralized system components (CPCI/WDAC/VADB/MFRS)	3/22/96
4/30/96	AUI ready for deployment	Beta

4/30/96	Standalone centralized system ready for deployment	Beta
6/30/96	Mac ports ready for deployment	AUI port in process

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

B&R No. GD 05-08-03

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

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

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

Various DISS User Guides and Training Materials

Computer Security - Distributed Systems

Doug L. Mansur, Program Manager
Computer Security Technology Center

INTRODUCTION

The Computer Security Technology Center (CSTC) serves the Department of Energy and its community by providing expertise and solutions to the many information security problems present in today's computer systems and networks. Incidents of intrusions, computer viruses, the purposeful replacement of legitimate software for illegal purposes, and similar acts are being addressed by the creation of security software, the delivery of incident response expertise, and research and development into secure systems.

SUMMARY OF MAJOR ACCOMPLISHMENTS

I. Computer Incident Advisory Capability (CIAC)

Incident handling remained relatively constant throughout the quarter. The team dealt with 30 incidents and 15 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 51 actions which includes 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: Concept Good Times (the hoax continues to pop up as real), NATAS, D3, and PKZIP300V. Intrusion attempts via the Internet continue: CIAC handled incidents involving ftp, e-mail spamming including a forged hate mail message, SATAN scans, a compromised host 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. and involved agencies beyond the DOE.

CIAC actively supported the 1996 DOE Computer Security Group Training Conference: Marvin Christensen delivered a training session entitled *Securing Your Internet Connections*, Sandy Sparks delivered the CIAC Threat Update, and Bill Orvis delivered a presentation on *Computer Virus Operation and New Directions*.

CIAC also was invited to participate in the 1996 DOE Telecom Conference; Sandy Sparks gave a presentation on today's threats. While in Albuquerque, CIAC took advantage of this opportunity to present a training course on

Internet Security for Charlene Douglas at LANL. Marvin and Sandy also participated in a meeting with Tom Rowlett and others from DOE headquarters to discuss preparations of the HQ Advice and Assurance (A&A) Review. Tom took the action item to get points on contact for each of the HQ entities and to get a request in writing from Bill Sylvester. There has been a subsequent meeting between Bill Huntman of LANL and Sandy Sparks to review the A&A and the work to be done by the end of FY96. CIAC will do a limited white hat for LBNL as part of this effort and lead the work for the DOE HQ white hat.

II. Network Intrusion Detector (NID)

We added an alpha (experimental) release directory for quick turnaround of bug fixes, incremental improvements, and new platform ports.

III. AIS Alarm Project

The LANL/LLNL/SNL team completed the Alarms Conceptual Design Document. In addition to sensor definition, LLNL produced the Communications Services definition for LANL. We designed and implemented the code development, subsystem test and binary distribution framework based upon these definitions.

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

The SPI team launched the DOE Computer Security Tools Usage Survey, designed to assess the degree and effectiveness of information security tools and technologies in use by DOE computer system administrators. Progress continued in SPI/SPI-NET Tech Transfer efforts.

V. Profiling and Vulnerability Analysis Project (VAP)

We continue to load the database with known vulnerabilities and intrusion methods. There are currently 60 vulnerabilities and 59 intrusion methods detailed in the database.

We have designed the system for protected external access and await arrival of the software to implement that access.

We presented an overview of the project at the DOE Computer Security Conference.

We have created a list of potential collaborators for the database and are currently discussing that access with those groups.

VI. DOE Information Security (DOE-IS) Server

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

We have initiated an active search of DOE sites for similar information security projects to include on the server.

We presented an overview of the server at the DOE Computer Security conference.

We have created a special project area on the server to use for conducting a User Needs survey. We created web pages and a database link for conducting the survey on-line.

We created a special projects area for the AIS Alarms project so they can coordinate the activities of the three national labs involved in the project.

TASK DESCRIPTION AND QUARTERLY PROGRESS

I. Computer Incident Advisory Capability (CIAC)

<u>B&R No.</u>	<u>Funding</u>	<u>Obligated</u>
GD060603	\$464K	\$347K

The Computer Incident Advisory Capability (CIAC) team members continued to assist DOE sites with computer intrusions, vulnerability assessments, security tools, evaluations, education, training, and awareness.

Incident handling included intrusions which crossed country borders, new clandestine techniques, and spamming of inappropriate messages. Intruders were using DOE systems to cross country borders in hopes of covering their tracks. More details can be seen in the major accomplishments section.

CIAC will continue to assist DOE Headquarters with their own internal information security program. This is part of CIAC's participation in the Advice and Assurance Program; we are coordinating efforts with Bill Huntman of LANL. A work request has been sent to LANL for money to be transferred to CIAC for this effort.

CIAC continues to monitor the security of its firewall and other file servers. In addition, CIAC is updating its ability to track calls and incidents so as to better support DOE HQ's request for information. CIAC also continues in

support of FIRST and will be participating in Santa Clara at the 1996 Workshop and Conference. 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	\$184K

We continued distribution and customer support for the NID 1.4 release. To respond more quickly to user requests with bug fixes, incremental improvements, and new platform ports, we added an alpha (experimental) release directory. Versions 1.5.0 through 1.5.8 have addressed immediate needs for changes at the risk of less formal testing.

Work continued on the development of additional ramp-up; we focused on switching between packet capture modes. We continued to develop the integrated NID graphical user interface in Tcl/Tk. Created a first version of the top-level xNID GUI.

III. AIS Alarm Project

<u>B&R No.</u>	<u>Funding</u>	<u>Obligated</u>
GD060403	\$500K	\$189K

LLNL completed its single Alarms milestone for this quarter. Beyond our required sensor conceptual design, LLNL provided the initial draft of the Alarms Conceptual Design Document. This included the operational concept, technical approach, sensor categories, and requirements. These were merged with graphical user interface (GUI approach from LANL) and assessment/response (from SNL) design in the final document.

In working meetings, the labs developed the technical approach in more detail. LLNL developed the interface control documents (ICDs) for Sensors and the Communications Services API (application programming interface). To further refine these documents, we designed and implemented the code development framework based upon these definitions. Using a single command, developers can make the entire code or a subsystem, run subsystem tests, or produce a binary distribution. Included were simplified versions of communications and three sensors sufficient to test compilation.

We also set up methods for secure DES login and file copy to the AIS Alarm Project web site through work with the DOE IS Server project. All lasting

project documents and source code access along with temporary file exchange have been handled through this service.

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

<u>B&R No.</u>	<u>Funding</u>	<u>Obligated</u>
GD060503	\$223K	\$190K

The SPI team launched the DOE Computer Security Tools Usage Survey in June. The survey plan was announced at the DOE Security Group Conference held in Seattle. The survey intends to interview a representative sample of computer system administrators at the major DOE sites, to assess the degree to which various computer security tools and technologies are deployed and utilized throughout the DOE, and to gauge their perceived effectiveness.

Through the end of June, the SPI team had contacted over 50 individuals at Lawrence Livermore Laboratory, and completed approximately 25 interviews. Pending the distribution of a formal notification from DOE HQ to the field offices, the team expects to cover other DOE sites through July and August.

The survey will also serve to promote the DOE-IS Information Server, a resource for both publicizing DOE-developed tools and techniques, and for submitting to DOE specific needs in the area of information security.

In the SPI Tech Transfer effort, negotiations with several firms that have expressed interest in commercialization continue.

V. Profiling and Vulnerability Analysis Project (VAP)

<u>B&R No.</u>	<u>Funding</u>	<u>Obligated</u>
GD060503	\$259K	\$158K

We are continuing to load the database and currently have 60 vulnerabilities and 59 intrusion methods detailed.

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

VI. DOE Information Security (DOE-IS) Server

<u>B&R No.</u>	<u>Funding</u>	<u>Obligated</u>
GD060503	\$150K	\$80K

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

We are actively promoting the use of the server by presenting it at the DOE Computer Security Conference and by actively approaching the DOE sites for submissions.

We are creating special access areas for multi-site projects to use to coordinate the project. We are using a combination of web servers and secure connection protocols to give the sites a protected area to work that is convenient to access from any platform attached to the Internet.

CSDS 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-18: Digital OSF/1 dxconsole Security Vulnerability
- G-19: IBM AIX rmail Vulnerability
- G-20: Vulnerability in NCSA and Apache httpd Servers
- G-21: Vulnerabilities in PCNFSD Program
- G-22: rpc.statd Vulnerability
- G-23: Solaris NIS+ Configuration Vulnerability
- G-24: FreeBSD Security Vulnerabilities
- G-25: SUN statd Program Vulnerability
- G-26: IRIX Desktop Permissions Panel Vulnerability
- G-27: SCO Kernel Security Vulnerability
- G-28A: suidperl Vulnerability

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

Deliverables completed:

04/30/96 Conceptual design specification for network alarms sensor subsystem prototype.

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

B&R No. GD060403

No milestones or deliverables to report for this quarter.

V. Profiling and Vulnerability Analysis Project (VAP)

B&R No. GD060403

A list of potential collaborators was created and submitted to DOE HQ.

The operating database was demonstrated to DOE personnel on 6/13/96.

VI. DOE Information Security (DOE-IS) Server

B&R No. GD060403

No milestones or deliverables to report for this quarter.

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

The DOE Information Security Server (DOE-IS), 1996 DOE Computer Security Conference, Seattle, WA, 4/22-26/96

The Vulnerability Analysis Project (VAP), 1996 DOE Computer Security Conference, Seattle, WA, 4/22-26/96

Complex Wide Access Control (CWAC) Project Safeguards Technology Program

Dan Johnson, Principal Investigator

INTRODUCTION

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

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

SUMMARY OF MAJOR ACCOMPLISHMENTS

1. Completed initial development of the ACS/VADB interface that will allow Argus systems to retrieve access control information from VADB.
2. Demonstrated encrypted communication between CWAC E/VS and a developmental version of the VADB.
3. Provided installation requirements packages to DOE-OAK and DOE Germantown to identify requirements relating to installation of a CWAC Enrollment/Verification Station at these locations. Completed several discussions with DOE-OAK regarding installation planning.

TASK DESCRIPTIONS AND QUARTERLY PROGRESS

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

<u>B&R No.</u>	<u>Funding</u>	<u>Obligated</u>
GD 060501	477K	372K

- 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.**

No change from last quarter. 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.**

In the previous quarter, we demonstrated that we are able to encode badges, communicate with a developmental version of the VADB to enroll badges and biometrics, and retrieve information for identity verification. We have since supplemented this basic capability with the following enhancements:

- 1) 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.
- 2) 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 allows all enrollment information to be acquired as scheduled, and to be transmitted to VADB when communication is restored.
- 3) 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 is being implemented 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.

The software required for the Argus to communicate with the VADB has been developed and successfully demonstrated between the LLNL Argus Test System and a developmental version of the VADB operating on the LLNL Open LabNet. After we enrolled workers in VADB using the CWAC Enrollment/Verification station, they were able to pass through an Argus CAIN booth that was disconnected from the Argus network and connected to VADB only through Open LabNet. This passage utilized the PIN, weight, and biometrics information enrolled in VADB.

A firewall has been designed and implemented to ensure appropriate security is provided for connection of the LLNL Argus production system to DOEBINET. This firewall will ensure that only VADB processors are allowed to communicate with the Argus processors, and that all other attempts to connect to Argus processors will be precluded. The design has been reviewed, and will be implemented following successful completion of an associated Vulnerability Analysis.

During the prior quarter the definition of the developmental interface between CWAC elements (enrollment/verification station, access control system) and the VADB had been distributed to attendees at two Quality Panels, and to interested individuals, for planning purposes only. 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.

DOE Oak withdrew their initial decision regarding which room in the Oakland Federal Building would be used for badge production and the CWAC Enrollment/Verification Station. Subsequently we supported analyses of installation alternatives, and after the new room selection was confirmed, we developed a new sketch showing equipment layout in the selected room.

Information was provided to DOE-OAK to allow them to complete the connection to DOEBINET (DOE Business Information Network), the frame relay system which we intend to use for communication with VADB.

Work is proceeding on a comprehensive test procedure to verify that the CWAC enrollment/identity verification and ACS/VADB interface requirements have been acceptably implemented.

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

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.

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.

Status reviews were presented to DOE OSS representatives on three occasions in April and May.

A presentation concerning the purpose of complex wide access control, CWAC project objectives, design criteria, and status was given at the Access Systems Quality Panel meeting in June at Argonne National Laboratory. We also supported discussions with the Security Policy Board group considering implementation of a standard badge across all Federal agencies.

A Field Work Proposal for FY98 containing an update of the Life Cycle Plan was developed and transmitted to DOE-HQ.

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

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

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

MILESTONES STATUS TABLE

Milestone Date	Description of Milestone	Status
4/30/96	At LLNL, demonstrate encrypted communication between a CWAC enrollment station and the pre-operational VADB	Complete
5/31/96	Demonstrate ACS/VADB communication between the Argus development system (with CAIN booth) and a development VADB (unencrypted communication)	Complete
6/30/96	CWAC enrollment station installed at DOE-OAK (but not tested)	CWAC Change Proposal 4a* submitted to change date to 8/15/96

* LLNL FESSP Letter 96-0725, dated 7/22/96

CWAC APPENDIX B: 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 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

I. The Security Policy Board (SPB) Director of Staff visited LLNL on June 13, 1996. Presentations were given on DOE's complex-wide personnel security and access control systems, and a meeting of the SPB access control group was held.

II. A Technical Interchange meeting was held at Livermore on June 4-6, 1996

III. The Argus Homepage received DOE approval for general operation. It operated without problems throughout the quarter with secure sockets and secure registration enabled. Approximately 200 accesses from 20 locations in the last six weeks.

IV. Preparation of "Evolving a Mature System with New Technologies" presentation for a CTA Interactive Television class to be held July 18, 1996

V. Preparation of paper "DOE's Nation-Wide system for Access Control Can Solve Problems for the Federal Government" for presentation at the 37th Annual INMM Conference.

VI. The "Standardization of Security Systems" task has been completed. The 4th quarter report will reflect the publication of the INMM paper and the participation in the CTA course, but all other work has been completed.

TASK DESCRIPTIONS AND QUARTERLY PROGRESS

<u>B&R No.</u>	<u>Funding</u>	<u>Obligated</u>
GD 06 0201	\$96K	\$97K as of 6/30/96

Hosting of the Security Policy Board

Peter Saderholm, Director of Staff of the Security Policy Board (SPB), and staff visited LLNL on June 13 and were briefed on DOE's Integrated Safeguards and Security system with an emphasis on the Complex-Wide Access Control system (CWAC). The SPB is actively pursuing a federal badge standard and is also interested in improving access control between agencies. Mr. Saderholm was invited by Ed McCallum to see DOE's system plans and to see demonstrations of the capabilities.

An access systems working group meeting was also held to discuss the possible formats for the magnetic stripe on a federal badge. There were representatives from the US Air Force, the US Navy, the Intelligence Community, and the DOE. The pros and cons of using the DoD SEIWG 012 specification were discussed, and problems with DOE's use were identified. Livermore provided analysis on both the DoD and CIA badges for use in the discussions. Analysis indicated that the DoD badge magnetic encoding format appeared to be designed to be independently enrolled in each compatible access control system, and not in support of a complex-wide access control system. Concerns were raised about the level of intersite security of an access control system based on this encoding format.

Technical Interchange Meeting at LLNL

151 Invitations were sent covering most DOE sites, the event was posted on the Argus Web page, and coordinated with DOE HQ. Participants came from DOE-ALU, DOE-Amarillo, DOE-HQ, DOE-Oak, INEL, LLNL, Pantex, Rocky Flats, Sandia, and Savannah River to attend the Technical Interchange meeting held at LLNL June 4-7. The meeting spanned 3 days and each day had a different focus. The first day's focus was working specific technical issues associated with each site (SPR discussions). The second day's focus was on technical and project briefings, with discussions about the Argus software and hardware, including introduction of new system features, the status of the hardware, and tours of facilities. The third day focused on new technologies with presentations on the DOE Integrated Safeguards and Security system, the Complex-Wide Access Control system, the Argus Web Page, future technologies for Argus, and ended with a general Argus Users meeting. Reports back from the participants indicated that this was a successful meeting.

Argus Homepage

Based on the security features incorporated into the Argus Web Page and the security plan established for its operation, DOE-HQ approved activation of the

Argus Webpage on May 1, 1996. The counters were reset on May 17, and since then approximately 200 page accesses have been recorded from approximately 20 locations. Requests for access to the webpage have been coming in at about one per week.

This quarter saw information added on the Training program, Baseline 19 software release, the Technical Interchange Meeting, and updates to released Argus documentation.

Preparation for class

Work was performed in preparation for the CTA Interactive Television class held on July 18, 1996 titled "Emerging Technologies". The presentation given was titled "Evolving a Mature System with New Technologies". Information was presented about the new technologies developed for the DOE Integrated Safeguards and Security system and the Complex-Wide Access Control system and how they are being integrated into DOE's Argus system. This work was completed in July.

Preparation of Paper

Work was performed in preparation for a paper to be presented at the 37th annual INMM conference in Naples, Florida on July 27, 1996. The paper is titled "DOE's Nation-Wide System for Access Control Can Solve Problems for the Federal Government". The paper outlines DOE's creation of the DOE Integrated Safeguards and Security system and the Complex-Wide Access Control system and suggests that access control challenges facing the federal government might be addressed by systems analysis and tools available from the Department of Energy. This work was completed in July.

This Task is Complete

The "Standardization of Security Systems" task is now complete. The status table shows that the task to update the Argus Functional Description and a report on the Argus Homepage remain to be completed. A Change request is being submitted to substitute the effort involved in preparing and presenting the CTA class for those two minor deliverables. The 4th quarter report will reflect those changes. The need to update and publish the Argus Functional Description has diminished, with information about functional changes now on-line on the Argus Homepage, along with the entire functional description. The need for a detailed Argus Homepage report has also diminished, with the Argus Homepage now on-line and available for browsing. The only thing required to understand the Homepage the URL ([HTTP://argus.llnl.gov](http://argus.llnl.gov)). In general, the progress of the Homepage has been documented in these quarterly reports and in the "Latest Argus Web News" section of the Homepage.

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

**MILESTONE & DELIVERABLE
STATUS TABLE**

Original Deliverable	Description of Deliverable	M/D	Status
12/1/95	Argus Internet Homepage with user registration required	D	Complete
2/14/96	Presentation to and report on Argus Advisory group meeting	D	Complete
3/9/96	Draft report on DOE contribution to the Federal Standardization of electronic security systems	M	Complete
5/1/96	Report on DOE contribution to the Federal Standardization of electronic security systems	D	Complete
6/15/96	Update of Argus Functional Description	D	to be deleted
6/30/95	Demonstration of DOE's electronic security systems concepts	D	Complete
7/18/96	Presentation at CTA ITV Course on "Emerging Technologies"	D	to be added
9/1/96	Argus Advisory Group meeting support	M	Complete
9/13/95	Host DOE community at an Argus Technical Interchange Meeting	D	Complete
9/30/95	Argus Homepage report	D	to be deleted

M=Milestone
D=Deliverable

SSS 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
\$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-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).

ITS APPENDIX 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 met
9/30/95	Provide DOE with requirements detailing the functionality of the web-based methodology	Milestone met
9/30/95	Provide DOE with plan for convening a second EOM	Milestone met
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 met
9/30/95	Present to DOE a program plan for conducting a second prototype meeting using the enhanced expert-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 met

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

EOM Methodology Report