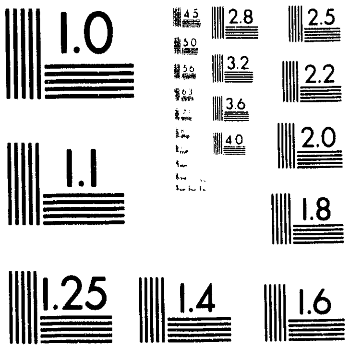
1.0
4.5
5.0
5.6
6.3
7.1
8.0
2.8
3.2
3.6
4.0
2.5
2.2
2.0
1.1
1.8
1.25
1.4
1.6

1 of 1

2.

Conf-9305151--11

Report No.YSS-428

Y-12

OAK RIDGE Y-12 PLANT

MARTIN MARIETTA

MICROCOMPUTER RESOURCE INSPECTION/ SELF-INSPECTION PROGRAM

E. L. Hockett, Jr., CPP and K. A. Marlow

Y-12 Security Department
Safeguards, Security, and Emergency
Preparedness Division

March 22, 1993

Preprint for submission to:

DOE Computer Security Conference
Albuquerque, NM
May 3, 1993

Prepared by the
Oak Ridge Y-12 Plant
Oak Ridge, Tennessee 37831
managed by
Martin Marietta Energy Systems, Inc.
for the
U. S. DEPARTMENT OF ENERGY
under contract DE-AC05-84OR21400

MANAGED BY
MARTIN MARIETTA ENERGY SYSTEMS, INC.
FOR THE UNITED STATES
DEPARTMENT OF ENERGY

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, 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 any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

MICROCOMPUTER RESOURCE INSPECTION/ SELF-INSPECTION PROGRAM

E. L. Hockett, Jr., CPP, and K. A. Marlow
Martin Marietta Energy Systems, Inc.
Oak Ridge Y-12 Plant*
P. O. Box 2009
Oak Ridge, Tennessee 37831-8213

Introduction

A Computer Security Program is more than just a concept. It is real action by real people. Under direction of DOE Orders, Martin Marietta Energy Systems, Inc., personnel have developed a Microcomputer Security Program that is both effective and sensible. This program works because those involved have a sincere desire to protect DOE information and assets.

General Information

The Oak Ridge Y-12 Plant is located in Oak Ridge, Tennessee. This facility covers 2.25 miles in the Bear Creek area and consists of approximately 500 buildings, which are located in Protected, Exclusion, and Property Protection Areas. There are some 50 different Energy Systems organizations that comprise the Y-12 Plant.

There are approximately 700 classified microcomputers and approximately 5,300 unclassified microcomputers at the site. These resources are used for many different functions including: word processing, Computer Aided Design operations, database management, servers for local area networks, and terminal emulators. Most microcomputers are used in a stand-alone mode of operation.

Computer Security Organizational Structure

The Computer Security Program at the Y-12 Plant is structured to provide a clear chain of functional responsibility. Additionally, the program allows for effective communication channels to exist from the Computer Security Site Manager/Computer Protection Program Manager (CSSM/CPPM) to approximately 6,000 users. The organization structure consists of the following:

Computer Security Operations Manager (CSOM)
W. G. Watson, DOE Oak Ridge Field Office

* Managed by Martin Marietta Energy Systems, Inc. for the
U. S. Department of Energy under contract DE-AC05-84OR21400

Computer Security Site Manager/
Computer Protection Program Manager (CSSM/CPPM)
R. C. Marcum, Martin Marietta Energy Systems, Inc.

Y-12 Plant Computer Security Officer (PCSO)
E. L. Hockett, Jr., CPP

Y-12 Plant Computer Security Officer Alternate
K. A. Marlow

Division Computer Security Officer (DCSO)
Forty Y-12 employees.

Computer System Security Officer (CSSO)
Approximately 6,000 Y-12 employees assigned to classified and unclassified microcomputers.

The Computer Security Site Manager/ Computer Protection Program Manager

The CSSM/CPPM serves as the director of the Computing and Telecommunications Security Organization (CTSO). The CSSM/CPPM is responsible for overall supervision of the Computer Security Program for all Energy Systems operating locations.

The Plant Computer Security Officer

The Y-12 PCSO reports directly to the Y-12 Security Department manager, is matrixed to the CSSM, and interacts with the CTSO. Additional responsibilities include incident investigation and reporting, division level training, inspections, and day-to-day administrative operations of the program.

The Division Computer Security Officer

A DCSO is appointed by each division manager to represent him/her concerning Computer Security issues and to implement the Computer Security Program within his/her division. Once appointed, the DCSO must complete an orientation course provided by the PCSO. This course supplies the DCSOs with the tools and knowledge they need to perform their DCSO responsibilities.

In addition to the day-to-day Computer Security responsibilities, the DCSO is responsible for the self-inspection program within the division. The DCSO self-inspection responsibilities include physically performing inspections of the computing resources within his/her divisions, reporting the results of the inspections to the organization management, ensuring corrective actions are in place for all identified deficiencies, and performing Computer Security training as required.

The Inspection Program

Annually, the DCSO is required to assist the PCSO in performing a formal Microcomputer Security inspection within his/her division. The inspection process is made up of five components:

(1) The inspection schedule.
(2) Notification of the inspection to the division and security management.
(3) Performing the inspection.
(4) Reporting the results of the inspection to the proper personnel.
(5) Following up on corrective actions.

The Inspection Schedule

The PCSO inspects 50 divisions at the Y-12 Plant on an annual basis. In developing the inspection schedule, the PCSO considers several factors. These factors include:

(1) The size of the division.
(2) Whether the DCSO is responsible for more than one division and, if so, if the divisions can be combined into one inspection.
(3) The number and classification of the microcomputer resources in the division.
(4) Previously identified Computer Security findings and incidents.
(5) The performance of the DCSO.

Once these factors are considered, the PCSO will develop an inspection schedule that prioritizes the divisions in the following order:

(1) History of Computer Security findings and/or incidents.
(2) The performance of the DCSO.
(3) Number and classification of the microcomputing resources.
(4) Length of time since the last inspection.

Inspection Notification

Once the PCSO has determined when each division inspection should be scheduled, the PCSO notifies the DCSO and security management two weeks prior to the inspection start date. The

DCSO is informed of the inspection date and the topical areas to be inspected. The PCSO also requests the following information:

(1) The number, classification, and locations of the microcomputing resources within the division.
(2) A division mission statement.

The PCSO will use the information concerning the number, classification, and location of microcomputing resources to select resources to inspect. This information will be included in the inspection report. The mission statement provides background information used in the report.

The Inspection

The PCSO determines most of the resources to inspect prior to the inspection date. On the date of the inspection, the PCSO meets with the DCSO to discuss the parameters of the inspection. The DCSO is asked to identify any areas of concern within his/her division and to provide verification of training for CSSOs of classified computing resources. After these items are addressed, the DCSO accompanies the PCSO to each resource location.

An Inspection Checklist is used to evaluate each selected resource. This checklist addresses six topical areas:

(1) Waste, fraud, and abuse.
(2) Equipment labeling.
(3) Media labeling and accountability.
(4) Classified/unclassified separation.
(5) Accuracy of Automated Data Processing (ADP) Protection Plans for computing resources processing classified and Unclassified Security-Related Information.
(6) Software license compliance.

Any findings identified during the inspection of a resource are recorded on the checklist. At the conclusion of the inspection of a resource, the System User or CSSO is briefed on the finding(s). The PCSO gives immediate feedback of corrective actions that must take place. The System User or CSSO is asked to acknowledge the finding(s) by recording his/her initials on the checklist; the PCSO initials the checklist also. The System User or CSSO is advised that the division manager will receive a report of all findings. The DCSO is made aware of personnel who requires additional training and of trouble area(s) within his/her division.

Reporting the Results of an Inspection

After the completion of a microcomputer inspection, an inspection report will be submitted to the DCSO, division manager, CSSM, and Security Department management. The inspection report summarizes all findings, both positive and negative.

All Microcomputer Security Inspection Reports conform to a standard format. The following topics are discussed in each inspection report:

(1) Executive summary.

- a. Purpose.
- b. Inspection date.
- c. Inspection team members.
- d. Names of DCSO and alternate.
- e. Division mission statement.
- f. Division microcomputer resources.
- g. Microcomputer resources inspected.
- h. Major findings.
- i. Overall rating.
- j. Statement of corrective actions required.

(2) Inspection methodology.

- a. Compliance requirements.
- b. Inspection criteria.

(3) Inspection results.

- a. Finding analysis.
- b. DCSO evaluation.

(4) Corrective action requirements.

(5) Issues for management attention.

Each division is rated on its compliance with Energy Systems procedures and DOE Orders relevant to Computer Security. The rating for each division is determined by the following:

(1) Adherence to Computer Security guidelines.
(2) Computer Security awareness level of division personnel.
(3) Range of finding severity.

The overall goal of the inspection and the inspection report is to help the DCSO and the division manager to assess the present Computer Security awareness level in the division, to identify areas within the division that need attention, and to report positive findings. The position of the PCSO is one of being an **advocate** rather than adversary.

Corrective Actions and Follow-up

If findings are identified during an inspection, the division manager is required to submit corrective actions to the PCSO. These corrective actions must resolve the current problem and aid in preventing future occurrences of the same finding. If a division is rated Unsatisfactory or does not provide acceptable corrective actions, the division is scheduled for reinspection.

A Common Sense Approach

Security is largely common sense. Computer Security is no exception. The first requirement for a successful program is to have management support at the highest level. Senior management at the Y-12 Plant has demonstrated support for the program by issuing policy statements and working with the local DOE field office to appoint a CSSM/CPPM. Management also made appropriate resources available to staff the CTSO.

Experience tells us most employees want to do the right thing. We place trust in the users and make them accountable for their actions and their use of the systems. Very few occasions occur where employees refuse to follow procedures. Based on this philosophy and the DOE Orders, plant procedures are clearly written and communicated to the plant population. Employees are trained before they are approved to process classified and/or Unclassified Security-Related Information on the microcomputer. Additionally, each user receives a brochure that states the basic rules for classified and unclassified users.

If security does not make sense to the employee, it will be difficult for the employee to comply. Understanding why we do things provides creditability to the program. Unnecessary requirements reduces the creditability of the program instead of strengthening the program. The key to having a successful program is knowledgeable people. If the people are properly trained, are accountable for their actions, and alert, they are less likely to compromise classified or sensitive information by making careless mistakes. We highly recommend spending time in the field getting to know the users and their functions.

Inspections are a way of life in today's governmental environment. You must continually be prepared for the announced and unannounced inspections. We have discovered that the best way to meet this challenge is to provide a sound self-inspection and training program.

DATE
FILMED

1 / 6 / 94

END