A MODEL EMPLOYEE IDENTIFICATION SYSTEM FOR NATIONAL DEFENSE INDUSTRIES

Thesis for the Degree of M. S.

MICHIGAN STATE UNIVERSITY

George M. Small Jr.

1964

A MODEL EMPLOYEE IDENTIFICATION SYSTEM FOR NATIONAL DEFENSE INDUSTRIES

By

George M. Small Jr.

AN ABSTRACT OF A THESIS

Submitted to
Michigan State University
in partial fulfillment of the requirements
for the degree of

MASTER OF SCIENCE

School of Police Administration
and Public Safety

1964

APPROVED Raymond T. Galvin
(Chairman)

Leon H. Weaver
(Member)

(Member)

The purpose of this study is to: (1) develop a model system to identify employees working at national defense industries, and (2) determine whether the model system could be utilized at three selected defense industries of varying size and function, and whether such utilization would result in more positive security compliance.

Information and relevant data were then obtained by: (1) reviewing the Department of Defense contractual requirements for national defense industries, (2) reviewing other applicable literature, (3) interviewing authorities in the field, and (4) examining several representative identification systems. A model system was then developed on the basis of the controlling governmental regulations and on the additional criteria for identification systems.

The systems and procedures for employee identification at three selected defense industries were then reviewed to provide a basis for comparative tests of the model and the three companies. The same frame of reference was utilized in describing the three companies as was used in the model presentation. These comparative tests determined that: (1) the model system has the capability of performing all of the primary functional and procedural requirements of the three companies, and (2) the model system is in more complete compliance with the

Department of Defense regulations and with the additional criteria for identification systems. It was also determined that a need exists for improving the quality of the Department of Defense regulations that govern identification systems.

As this thesis progressed, the importance of employee identification as a basis for the security program became more evident. The study's results supported the view that establishing and maintaining an effective security identification system is a vital necessity in preventing the compromise of our military, industrial, and technological secrets; that realization of effective personnel identification is an essential prerequisite toward accomplishing the objective of sound security programs in our national defense industries.

A MODEL EMPLOYEE IDENTIFICATION SYSTEM FOR NATIONAL DEFENSE INDUSTRIES

By

George M. Small Jr.

A THESIS

Submitted to
Michigan State University
in partial fulfillment of the requirements
for the degree of

MASTER OF SCIENCE

School of Police Administration
and Public Safety

1964

TABLE OF CONTENTS

CHAPTER		PAGE
I.	NEED FOR EFFECTIVE INDUSTRIAL SECURITY . . .	1
	History of Espionage Against the United States	1
	The Threat of Soviet Industrial Espionage .	2
	Importance of the Industrial Security Program	6
	Lead-Time Concept	8
	Identification as Basis for Effective Security	11
II.	PURPOSE OF THIS STUDY	12
	Development of a Model System	12
	Testing the Model System	12
	Limitations of This Study	12
III.	DEPARTMENT OF DEFENSE REGULATIONS	14
	Industrial Security Manual	14
	Air Materiel Command Manual	18
IV.	ADDITIONAL IDENTIFICATION STANDARDS AND EXEMPLARY SYSTEMS	22
	Review of Authoritative Information	22
	Exchange Identification System	29
	Electronic Devices	30
	Key-Card System	31
	Badge System with Changeable Codes . . .	34

CHAPTER PAGE

V. MODEL EMPLOYEE IDENTIFICATION SYSTEM 38

Perimeter Identification 38

Identification Device 39

Issuance 40

Accountability 44

Entry/Exit Procedures 46

Temporary Identification 47

Closed Area and Clearance Identification . 49

Identification Device 50

Issuance 54

Accountability 58

Entry/Exit Procedures 61

Temporary Identification 61

VI. EMPLOYEE IDENTIFICATION SYSTEMS AT THREE SELECTED COMPANIES 63

A Company Perimeter Identification 64

Identification Devices 64

Issuance 70

Accountability 73

Entry/Exit Procedures 75

Temporary Identification 77

A Company Closed Area and Clearance Identification 81

Identification Devices 81

Issuance 84

CHAPTER PAGE

Accountability 87

Entry/Exit Procedures 92

Temporary Identification 93

B Company Perimeter Identification 98

Identification Device 98

Issuance 100

Accountability 101

Entry/Exit Procedures 103

Temporary Identification 104

B Company Closed Area and Clearance

Identification 106

Identification Device 106

Issuance 107

Accountability 107

Entry/Exit Procedures 108

Temporary Identification 109

C Company Perimeter Identification 110

C Company Closed Area and Clearance

Identification 111

Identification Device 111

Issuance 111

Accountability 112

Entry/Exit Procedures 112

Temporary Identification 113

CHAPTER PAGE

VII. COMPARATIVE TESTS OF THE MODEL AND THREE COMPANIES 114

Model Adaptability 115

Compliance with Requirements and Standards 118

VIII. CONCLUSION 124

BIBLIOGRAPHY 132

LIST OF TABLES

TABLE		PAGE
I.	Comparison of Perimeter Identification Functions	116
II.	Comparison of Closed Area and Clearance Identification Functions	117
III.	System's Degree of Compliance with Department of Defense Requirements . . .	121
IV.	System's Degree of Compliance with Additional Identification Standards . . .	122
V.	Percentage Comparison of Compliance Findings of Tables III and IV	123

LIST OF FIGURES

FIGURE		PAGE
1.	Industrial Security Lead-Time	9
2.	Key-Card Identification	33
3.	Electronically Coded Badge	36
4.	Proposed Identification Badge	41
5.	Proposed Identification Badge File Forms	45
6.	Proposed Temporary Identification Badge	48
7.	Proposed Clearance and Admittance Authorization Card	52
8.	Proposed Request for Clearance and Admittance to Area(s) Form	55
9.	Proposed Request for Clearance and Admittance to Area(s) Form	56
10.	Proposed Clearance and Admittance Authorization Card File Forms	60
11.	Identification Card	66
12.	Salaried Badge	67
13.	Hourly Badge	68
14.	Early Admittance and Odd-Shift/Odd-Lunch Cards	69
15.	Pass and Badge Receipt Card	74
16.	Temporary Identification Pass	78
17.	Clearance and Admittance Authorization Card	83
18.	Register Form	88

FIGURE PAGE

19. Receipt for Key-Card 91

20. Temporary Admittance Authorization 95

21. Identification Badge 99

22. Security File Card 102

23. "I FORGOT" Badge 105

CHAPTER I

NEED FOR EFFECTIVE INDUSTRIAL SECURITY

This chapter will review the area of espionage and the resulting need for positive and effective industrial security-identification practices.

I. HISTORY OF ESPIONAGE AGAINST THE UNITED STATES

The threat of foreign espionage to the United States is as old as the country itself. Since the days of the American Revolution, our country has been the object of espionage efforts by practically every major world power. Great Britain, Mexico, Spain, Germany, Italy, Japan, China, and the Soviet Union, have all, at one time or another, engaged in extensive espionage programs with the intent of subverting our national security. Only a few short years ago, the major threat was coming from Germany and Japan.[1] Today, espionage efforts against the United States are primarily being originated by the Soviet Union.[2]

---

[1]Colonel Allison Ind, A Short History of Espionage (New York: David McKay Company, Inc., 1963), pp. 61-315.

[2]J. Edgar Hoover, "Do You Really Understand Communism?" Industrial Security, Vol. VI, No. II (April, 1962), pp. 4-5, 23-24.

II. THE THREAT OF SOVIET INDUSTRIAL ESPIONAGE

Throughout this country's history, our nation's industries have consistently played a vital role in maintaining national security. The importance of the job that industry performs in the areas of production, maintenance, construction, and research is also recognized by the Soviets.[3]

American industry has been one of the primary targets of Soviet espionage for many years, dating back to the early days of the Bolshevik Revolution when the Russians established a Soviet government trading agency in 1924, called the Amtorg Corporation. This agency was successful in stealing formulas for industrial products such as petroleum and chemicals.[4]

Since this early start, the communists have expanded their efforts to the point today where every industrial company in the country is a potential target.[5]

---

[3] John R. Davis, Industrial Plant Protection (Springfield: Charles C. Thomas Publisher, 1957), pp. 453-55.

[4] J. Edgar Hoover, Masters of Deceit (New York: Pocket Books, Inc., 1958), pp. 271-87; and United States Congress, House of Representatives, Committee on Un-American Activities, The Shameful Years - Thirty Years of Soviet Espionage in the United States, (Washington: Government Printing Office, 1952), pp. 5-21.

[5] J. Edgar Hoover, "Do You Really Understand Communism?" Industrial Security, Vol. VI, No. II (April, 1962), pp. 4-5, 23-24; and Office of Defense Mobilization, Standards for Physical Security of Industrial and Governmental Facilities, (Washington: Government Printing Office, 1958), p. 1.

Authorities on Soviet espionage have, on numerous occasions, cited that our national defense industries, particularly those involved in classified contracts, are prime targets of Soviet espionage. General Trudeau, United State Army Chief of Research and Development and former head of Army Intelligence, has stated that Soviet espionage poses a serious threat to our industrial base, and that any industry which is even remotely connected with our defense efforts can expect to be subjected to Soviet espionage efforts.[6] Companies engaged in classified work, i.e., work involving information which requires protection in the interest of national defense,[7] are of special interest to the communists. Industries such as aircraft, electronics, missiles, chemical, steel, communications, and shipping are particularly subject to their efforts.[8]

Much information suitable for subsequent development into vital intelligence is gathered by the Soviets through open means, such as subscribing to our technical

---

[6]General Arthur Trudeau, U.S. Army Chief of Research and Development and former head of Army Intelligence, Speech to the American Society for Industrial Security, Washington, D.C., September 18, 1958.

[7]United States Department of Defense, Industrial Security Manual for Safeguarding Classified Information, (Washington: Government Printing Office, November, 1961). p. 2.

[8]Hoover, loc. cit; and William C. Sullivan. "The Continued Threat of Espionage and Sabotage in the U.S.," Industrial Security, Vol. VI. No. IV (October, 1962), pp. 44-45.

journals, purchasing government patents, attending scientific lectures, and monitoring exhibits. However, the communists are also operating in the area of clandestine spy operations to obtain information relative to our national security.[9] Hoover states that this continuing espionage and intelligence attack is being conducted on a scale unequaled in history.[10] Their intelligence service has been developed to the point where it is now the largest and most effective espionage agency the world has ever known.[11] Their spy sytem is well organized and is composed of highly trained personnel.[12] Their industrial espionage apparatus, in particular, is rated as superior by our own intelligence professionals. General Trudeau has stated:

> The advanced state of Soviet technology today is due more to Soviet success in espionage and subversion than it is to their scientific apparatus, good as it is.[13]

Hoover says that Soviet block diplomats now form

---

[9] Ibid.

[10] U.S. News and World Report, Testimony by J. Edgar Hoover before the House Appropriations Committee, June 5, 1963, U.S. News and World Report, LIV (June 17, 1963), p. 10.

[11] Major Andrew J. Kukucka, United States Army Department of Counterintelligence, Speech to the American Society for Industrial Security, Washington, D.C., September 18, 1958, (Printed Copy).

[12] J. Edgar Hoover, "Do You Really Understand Communism?" Industrial Security, Vol. VI, No. II (April, 1962), pp. 4-5, 23-24.

[13] Trudeau, loc. cit.

the backbone of espionage operations in the United States, and that their embassies are being used as bases of operation for conducting intelligence activities.[14] He also states that 75 per cent of Soviet officials in this country have some type of intelligence assignment,[15] and that there are 761 Soviet block diplomats assigned in this country who have been given extensive training in espionage. In addition, there are 1,066 dependents of Soviet block personnel, some of whom are also trained intelligence agents. He states that in the year ending June 30, 1962, Russian officials made fourteen trips through this country for the purpose of intelligence and reconnaissance. These officials visited numerous areas of strategic importance to our defense effort and closely studied many military installations and industrial facilities. During the same year, sixty-five scientific, industrial, and military exhibits, conferences, and symposia were attended by some ninety-five Soviet block personnel. Masses of information were collected, and numerous contacts were made with persons having potential value for future intelligence recruitment.[16]

---

[14]U.S. News and World Report, loc. cit.

[15]J. Edgar Hoover, Masters of Deceit (New York: Pocket Books, Inc., 1958), pp. 271-87.

[16]U.S. News and World Report, Testimony by J. Edgar Hoover before the House Appropriations Committee, June 5, 1963, U.S. News and World Report, LIV (June 17, 1963), p. 10.

Hoover states that there are many first-hand examples of instances where the Soviets have succeeded or tried to steal vital industrial secrets in the United States. He specifically cites the Harry Gold, Klaus Fuchs, Julius Rosenberg espionage apparatus which was primarily concerned with obtaining industrial information and eventually stole secret atomic energy data. He also refers to the case of Ivan A. Bubchikov, Assistant Soviet Military Attache assigned to the Soviet Embassy in Washington, who used the services of a naturalized American citizen in 1955 and 1956, for the purpose of securing data concerning jet fuel, atomic submarines, and aeronautical developments.[17]

III. IMPORTANCE OF THE INDUSTRIAL SECURITY PROGRAM

Industries where classified work is being performed often represent the most vulnerable phase in developing and evolving secret weapons and techniques.[18]

---

[17]J. Edgar Hoover, "Do You Really Understand Communism?" Industrial Security, Vol VI, No. II (April, 1962), pp. 4-5, 23-24.

[18]United States Air Force, Guide for Security Indoctrination; AFM 205-5 (Washington: Government Printing Office, 1955), pp. 133-36.

Industries allowing weaknesses in their industrial plant protection systems, such as: (1) leaving classified documents unprotected, (2) performing perfunctory plant security checks, and (3) permitting conditions that are conducive to clandestinely removing materials from the plant, become vulnerable targets for espionage efforts.[19] The first line of defense against conditions that make industries vulnerable to espionage is the industrial security program as implemented through the various plant protection and security systems.[20]

Although the Department of Defense Industrial Security Program is designed to safeguard classified information in the possession of Industrial firms, this program, in itself, is not sufficient to prevent valuable intelligence information from falling into the hands of a potential enemy.[21] The directives and regulations which have been established for use at industrial defense installations establish only the minimum

---

[19]Hoover, loc. cit.

[20]Ibid; and Trudeau, loc. cit.

[21]United States Air Force, Industrial Security Newsletter (Headquarters, Central Contracts Management Region, Wright Patterson AFB, Ohio, December, 1961), pp. 1-18.

standards of security.[22] It is necessary that management be constantly alert to vulnerable points within their facilities, particularly in the area of plant security protection.[23] Only through imagination and a full knowledge of the meaning and intent of applicable regulations by those responsible for implementing the security program can real security effectiveness be achieved.[24]

IV. LEAD-TIME CONCEPT

The primary objectives of the industrial security program are: (1) to safeguard classified information by entrusting it only to trustworthy persons, and (2) to establish procedures to prevent its compromise. Accomplishing these objectives becomes meaningless unless the security program is sufficiently effective to protect the scientific and technical advantages that we achieve.[25] Maintaining an advantage or lead-time is one of the

---

[22]United States Air Force, Guide for Security Indoctrination.

[23]United States Air Force, Industrial Security Newsletter.

[24]United States Air Force, Guide for Security Indoctrination.

[25]A. Tyler Port, Director, Office of Security Policy, Office of the Secretary of Defense, Speech to the American Society for Industrial Security, Washington, D.C., September 18, 1958, (Printed Copy).

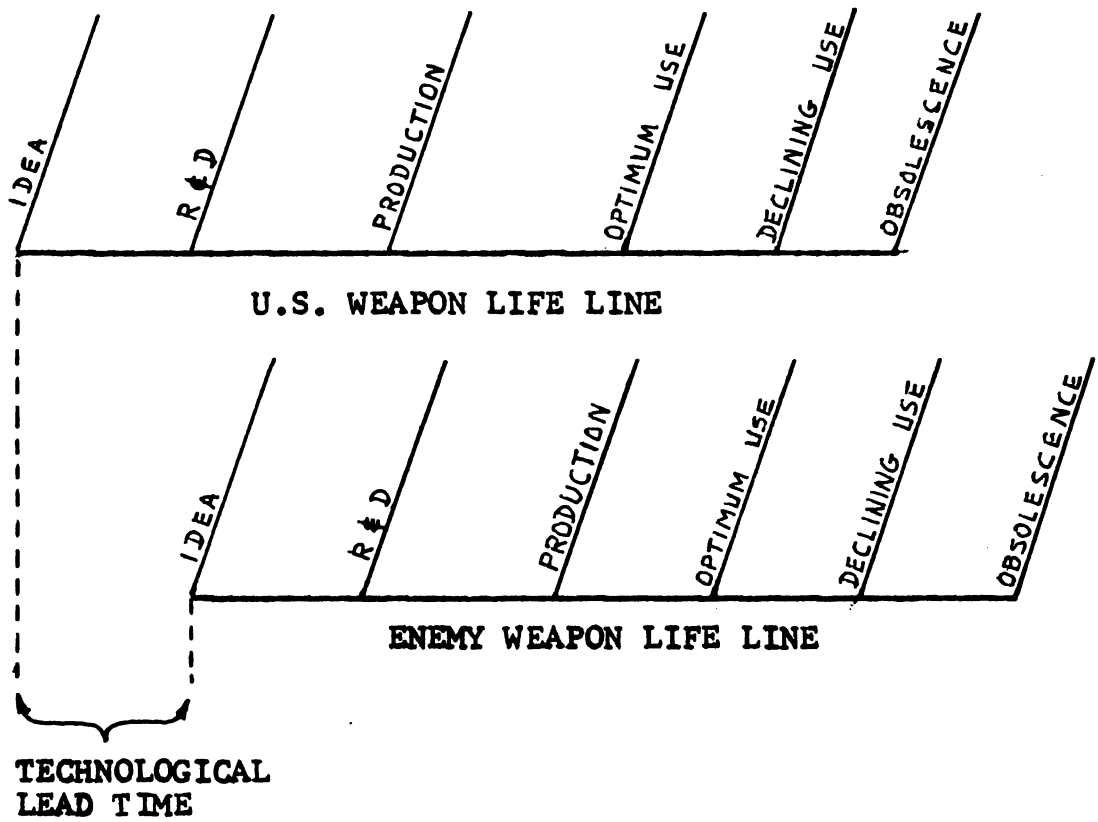


FIGURE 1

INDUSTRIAL SECURITY LEAD-TIME
(FROM UNITED STATES ARMY
INTELLIGENCE SCHOOL MANUAL)

basic concepts of the security program. As illustrated in Figure 1, the aim of an effective security program is to provide enough security protection so that by the time a foreign adversary is able to obtain one of our ideas, we have already proceeded well into the research and development phase. Continuing security protection is provided throughout the life of the weapon system to maintain this lead-time advantage.[26]

The Department of Defense Industrial Security Program is designed to insure that lead-times vital to our national security are protected. Various security systems and procedures have been established by the Department of Defense to provide this protection. These systems and procedures basically: (1) provide for appropriate classification of information, and (2) provide that classified information is disclosed only to authorized persons, i.e., persons with appropriate security clearance who have a need for the information.[27]

---

[26]United States Army, Industrial Security Management Manual, (United States Army Intelligence School, Fort Holabird, Maryland, May, 1959), No Page Numbers.

[27]United States Department of Defense, Industrial Security Manual for Safeguarding Classified Information, (Washington: Government Printing Office, November, 1961), pp. 1-8.

V. IDENTIFICATION AS BASIS FOR EFFECTIVE SECURITY

Assuring that only authorized persons have access to classified information becomes a complex problem. Systems for document control, material control, physical security, subcontractors and consultants, visitor control, and personnel clearances are required for every contractor who engages in classified defense work with the government. Some requirements are relatively simple to implement while others are very complex. Requirements also vary greatly, depending on the size of the defense contractor's facility, the number of employees, the volume and size of classified documents and hardware, the type of work being done, and the sensitivity of the projects.

However, all of these variables have a common factor, for they all depend on personnel identification systems as one of the foundations for their effective operation. Without establishing and enforcing rigid identification procedures, none of the above systems could function effectively.[28]

---

[28] Ibid., pp. 1-37.

CHAPTER II

PURPOSE OF THIS STUDY

I. DEVELOPMENT OF A MODEL SYSTEM

The first purpose of this study is to develop a model system of employee identification based on applicable governmental regulations and on accepted security standards.

II. TESTING THE MODEL SYSTEM

The second purpose of this study is to determine whether the model system could be utilized at three selected defense industries of varying size and functions by analyzing the three systems in reference to the model, and, if so, whether such utilization would result in more positive security compliance.

III. LIMITATIONS OF THIS STUDY

This study will be limited to the area of employee identification. No consideration will be given to the areas of identification of visitors, subcontractors, resident contractors, military personnel, civil service personnel, suppliers or vendors. The area of pre-employment screening and identification will not be considered, and the processing of the contractor's

government security clearances is also not considered. Other closely related security subjects such as fencing, lighting, alarm systems, guard patrols, employee theft, vehicle parking, vehicle searches, material control, and document control are not included in this thesis. Only those specific practices and procedures directly pertaining to employee identification systems will be studied.

The field of industrial espionage between companies is also not covered in this study.

CHAPTER III

DEPARTMENT OF DEFENSE REGULATIONS

When civilian industries perform work for the United States Government, they enter into a contract covering various phases of the work to be accomplished. The contractual requirements pertaining to the national security program and the United States Air Force Air Materiel Command's Security Guide will be reviewed.

I. INDUSTRIAL SECURITY MANUAL

Civilian industrial work involving classified information necessitates a contract between the industry and the government for the safeguarding of the classified information. The contractor industry agrees to abide by certain rules and regulations, as specified in the contract known as the Department of Defense Security Agreement (DD Form 441) and the Industrial Security Manual for Safeguarding Classified Information (Attachment to DD Form 441). The rules and regulations set forth in this agreement are for the specific purpose of establishing uniform security practices within industrial facilities which have classified information of the military departments (Army, Navy, or Air Force) in

their custody.[1]

Prior to the release of classified information to the contractor's facility, it is necessary that a Facility Security Clearance be granted to the contractor by the Department of Defense. Whether or not a Facility Security Clearance is granted is based on the results of a security survey conducted by Department of Defense inspectors. If it is determined that the contractor has the ability to adequately safeguard and protect the classified information needed in the performance of his contract, the Facility Security Clearance is granted.[2]

The "General Requirements" section of the Industrial Security Manual for Safeguarding Classified Information makes the contractor directly responsible for safeguarding all classified information under his control and prohibits the contractor from allowing unauthorized persons to have access to such information. The contractor company is further required to provide adequate protective measures within his facility to safeguard all classified information under his control.

---

[1]United States Department of Defense, Industrial Security Manual for Safeguarding Classified Information, (Washington: Government Printing Office, November, 1961), p. iii.

[2]United States Department of Defense, Armed Forces Industrial Security Regulation, (Washington: Government Printing Office, November, 1961), pp. 13-20.

The contractor must also establish a system to control access of employees and visitors to closed and restricted areas within his facility, i.e., areas where classified information is accessible during working and/or non-working hours.[3] Examples of such areas would include assembly rooms where large classified pieces of equipment or classified charts are in the open and subject to visual access.

The section of the Industrial Security Manual which states the requirements governing employee badges and identification cards is quoted below:

> a. Employee Badges. Provided the contractor deems it necessary, he may use identification cards or badges to assist in identifying the degree of security clearance of the holder and/or to indicate that the holder is authorized to enter closed or restricted areas. If identification cards or badges are used for such purposes, the following shall apply:
>
> (1) The minimum identifying information to be shown on employees' identification badges or cards shall be the name and photograph of the holder. Other descriptive information to identify the authorized holder may be included on badges and/or cards at the option of the contractor.
>
> (2) The identification badge or card may include color or symbol coding to indicate the degree of security clearance of the holder and/or that he is authorized to enter a closed or restricted area, or a separate coded badge or card may be used for such purposes. When the combination of badges and/or cards are used, both must bear correlating data such as the same registration number or the name of the holder.

---

[3] Industrial Security Manual, pp. 5-7.

(3) The words "TOP SECRET," "SECRET" or "CONFIDENTIAL," or abbreviations thereof shall not appear on the badges or identification cards.

(4) The makeup and construction of badges and identification cards shall be designed to minimize the possibility of tampering or unauthorized use.

(5) Badges and identification cards indicating the degree of security clearance or access to closed or restricted areas shall be rigidly controlled and accounted for by the contractor by use of a numbering system. Such badges and identification cards shall be surrendered by the holder upon termination of employment, termination of security clearances, or for other appropriate reasons.

(6) Coded badges and cards shall be considered only as an aid in determining the current degree of personnel security clearance of the holder or the areas to which the holder may have access. The clearance status of a person who holds such a badge or identification card shall be verified when there is doubt as to the validity of the badge or card.

c. Reporting. The procedures for the use of badges or identification cards as authorized in 'a' . . . above shall be incorporated in the Standard Practice Procedure.[4]

Failure on the part of the contractor to maintain the standards for physical security as specified in the Industrial Security Manual may result in: (1) cancellation of all government contracts involving classified information, and (2) permanent revocation of the contractor's Facility Security Clearance.[5]

---

[4]Industrial Security Manual, p. 8.

[5]Armed Forces Industrial Security Regulation, p. 23.

Close adherance by the contractor to the provisions and requirements of the Industrial Security Manual is vital. As a means of monitoring the degree of compliance by the contractor with these provisions, security inspections are periodically conducted by the Department of Defense. If the results of one of these inspections reveal that the contractor's facility is no longer adequately safeguarding classified information, the Department of Defense may prohibit additional classified information from being furnished to the contractor and may withdraw all classified information previously furnished to the contractor until such time as the facility meets the standards of the Industrial Security Manual.[6]

II. AIR MATERIEL COMMAND MANUAL

When the three Companies viewed in this study became involved in classified defense contracts, the Department of Defense assigned security cognizance to the United States Air Force. The major air command within the Air Force having responsibility for overseeing the security of all industries under their jurisdiction is the Air

---

[6] Ibid.

Materiel Command.[7] Although the Air Force reorganization of July 1, 1961, officially changed the name of the Air Materiel Command to the Air Force Logistics Command, its responsibilities and functions relating to security cognizance over industrial security remained unchanged.[8]

As an aid to the various companies under their cognizance, Air Materiel Command Manual 205-9 is furnished to the companies as a guide for maintaining a satisfactory degree of security compliance.[9] Although the information in the manual is provided only as a guide, and is not an official part of the contractor's contractual obligations, the Air Force security inspectors also use it as a guide when conducting their periodic security inspections. Thus, the willingness and ability of the contractor to heed the suggestions of the manual is often directly reflected in the inspection results.[10]

---

[7]United States Army, Industrial Security Management Manual, (United States Army Intelligence School, Fort Holabird, Maryland, May, 1959), No Page Numbers.

[8]United States Air Force, Industrial Security Bulletin, (Headquarters, Western Contracts Management Region, Mira-Loma, California, July, 1961), p. 1.

[9]United States Air Force, Air Materiel Command Manual 205-9, Industry Guide for Preparation of Standard Practice Procedures for the Handling and Protection of Classified Matter, (Washington: Government Printing Office, August, 1957), p. A-1.

[10]David Grand, United States Air Force Industrial Security Inspector, Western Contracts Management Region, Mira-Loma, Calif., Personal Interview, November 14, 1961.

The section of the manual which pertains to personnel identification suggests that whenever employees can not be admitted to the plant on personnel recognition, employee identification badges or cards should be used. The manual further states that badges should be tamper-proof and should contain sufficient descriptive information, including photograph, to identify the bearer. Badges should be worn in a visible, uniform place at all times. Persons without badges should be challenged, and anyone without proper credentials claiming to be an employee should not be admitted to the plant. Periodic checks of badges should be conducted to assure possession by persons to whom the badges are issued. The manual suggests that badges should be serialized and rigidly controlled. Whenever more than five per cent of the total badges issued are lost, new badges should be issued. Positive means should also be taken to assure the return of badges and identification cards upon separation of employment. The manual further states that the contractor should establish a program to control admittance of employees to the plant outside of their normal working hours to assure that entry is authorized and necessary. Contractors should also make provisions for positive identification and determination of "need-to-know" before employees are admitted to

restricted and closed areas within the plant.[11]

---

[11]Air Materiel Command Manual, pp. A-1, A-4.

CHAPTER IV

ADDITIONAL IDENTIFICATION STANDARDS AND EXEMPLARY SYSTEMS

I. REVIEW OF AUTHORITATIVE INFORMATION

The type of identification and pass system suitable for use at a given company will depend greatly on the size of the company and the scope of security work in which it is engaged. Quite often in small plants, employees are identified by personal recognition, and badges or passes are not used. Larger companies find it necessary to utilize an identification system of badges and passes as an essential means of maintaining good security and control of personnel.[1] It is generally felt that organizations with more than thirty persons should use some type of pass or badge system.[2]

A review of applicable literature, in addition to those Air Force and Department of Defense publications previously cited, indicates certain basic require-

---

[1]National Industrial Conference Board, Industrial Security, Combating Subversion and Sabotage (Studies in Business Policy No. 60. New York: National Industrial Conference Board, 1957), p. 76.

[2]B. W. Gocke, Practical Plant Protection and Policing (Springfield: Charles C. Thomas Publisher, 1957), pp. 9-17; and United States Atomic Energy Commission, Physical Security Standards, (Washington: Government Printing Office, 1950), p. 12.

ments in establishing a pass and badge system of personnel identification. These criteria are as follows:

1. Badges should be of a tamper-resistant design. A plastic laminated pass or badge is generally considered the most tamper-resistant type available. Such badges usually consist of ordinary paper or card material laminated between two pieces of slow-burning acetate or vinyl plastic. Using a plastic insert laminated between two transparent pieces of plastic makes a much more secure badge, as the three pieces of plastic, when laminated together, are fused into one tamper-resistant piece. Metal rimmed or plastic envelope devices are not considered as tamper-proof.

2. Badges should be of sturdy construction, waterproof, and resistant to abuse and hard wear.

3. Badge design should be such that rapid employee entrance and egress during peak traffic periods at the gates is facilitated.

4. A clear photograph of the bearer should be laminated into the front of the badge. The picture should be at least one inch in its smallest dimension, and the bearer should be re-photographed at least every five years or when necessary to reflect any significant physical change in facial appearance.

5. The name of the company and plant is entered in order that a badge used at one plant is invalid at

any other plant.

6. Identifying information such as the name and signature of the person to whom the badge is issued, together with his social security number, date of birth, color of eyes and hair, height, and weight is normally included.

7. Passes and badges should be numbered serially in a prominent manner, and the same number of a lost badge should never be used again.

8. Cross file records by name and badge number should be kept to aid in checking on lost or cancelled passes or badges.

9. Color or number codes are recommended to identify work shifts and/or work areas authorized.

10. The date of issuance and the expiration date should be entered on the pass or badge.

11. The badges should be signed by a representative of management or stamped with his facsimile signature.

12. Badge make-up and issuance should be carefully controlled.

13. A close check of terminated employees is recommended to ensure return of badges.

14. Returned badges should be destroyed periodically along with mutilated and defective badges.

15. Badges should have an intricate design which is difficult to reproduce by normal photocopying.

16. An ink or dye which is noticeably affected by erasure, or by heat required to alter or laminate the badge or pass, is recommended.

17. Strict enforcement of badge rules should be maintained. Employees must be aware of identification procedures applicable to them and must know what to do if they lose or damage their badges. Badges and passes should be prominently displayed on the employees' outer garments in a uniform position at all times within the plant. Violators should be reported immediately, irrespective of official rank, to a member of the plant guard force. Support from supervision in enforcing regulations is required, and penalties are often inflicted on violators who lose badges or otherwise disregard identification rules. Procedures for the plant guard force and the identification unit must be thoroughly understood and complied with.[3]

---

[3]National Industrial Conference Board, pp. 74-82; Gocke, loc. cit; Atomic Energy Commission, pp. 12-17; National Industrial Conference Board, Industrial Security, Plant Guard Handbook (Studies in Business Policy No. 64 New York: National Industrial Conference Board, 1953), p. 24; United States Department of the Army, Physical Security of Military and Industrial Installations, FM 19-30, (Washington: Government Printing Office, 1952), pp. 41-50; United States Atomic Energy Commission, Security, (Washington: Government Printing Office, 1960), Chapter 2401, No Page Numbers; Office of Defense Mobilization, Standards For Physical Security of Industrial and Governmental Facilities, (Washington: Government Printing Office, 1958), p. 22; and Committee on Identification, "Report of the Committee on Identification," Industrial Security, Vol. 1, No. 4, (December, 1956), 17-18.

Authorities in the security field acknowledge that no system is absolutely foolproof, and that practically all badges or passes can be reproduced or altered by persons sufficiently skilled in the arts of photography, engraving, and printing.[4] Passes and badges produced in accordance with the previously listed specifications are, however, sufficiently difficult to reproduce or alter to be acceptable for use at the vast majority of plants, provided they are used in conjunction with systems of rigid control and accountability. The previously listed requirements are particularly adequate when utilized in the exchange badge systems.[5]

At a plant or area where it is necessary to use credentials which are extremely difficult to alter or duplicate, the following specifications are suggested as methods to be considered:

---

[4]Edward Brosnan, Chief of Physical Security for the Atomic Energy Commission, Washington, D.C., Personal Interview, March 22, 1962; David Grand, United States Air Force Industrial Security Inspector, Western Contracts Management Region, Mira-Loma, California, Personal Interview, November 14, 1961; Robert Meader, Director of Security, Varian Associates, Palo Alto, California, Personal Interview, October, 1961; Harry L. Shaw, Plant Protection Manager, Lockheed Missiles and Space Company, Sunnyvale, California, Personal Interview, November, 1961.

[5]Edward Brosnan, Personal Interview; and David Grand, Personal Interview.

1. Insert paper with a distinctive watermark.

2. Insert paper that will lose its fibrous strength during the laminating process so that attempts to separate the paper or to peel off the outer plastic will result in a physical breakdown of the insert paper.

3. Cross threads or wires that are readily visible and laminated within the plastic cover sheets of the badge or pass. Alterations such as superimposing a photograph, changing a signature or badge number, or any attempts to re-laminate the badge are usually obvious with such badge systems.

4. Printing the photograph on sensitized plastic material made according to the same chemical formula of the plastic covers so that the front and back transparent plastic sheets and the plastic photograph are laminated to form a solid piece of plastic.

5. Ink which may or may not be normally visible but which is visible under ultraviolet light.

6. Ink which will bleed and/or change color when it is exposed to solvents which dissolve plastic covers.[6]

---

[6]Department of the Army, Physical Security of Military and Industrial Installations, pp. 41-50; Atomic Energy Commission, Physical Security Standards, pp. 12-17; Atomic Energy Commission, Security, Chapter 2401, No Page Numbers; and Office of Defense Mobilization, Standards For Physical Security of Industrial and Governmental Facilities, p. 22.

John R. Davis states that in checking the identification of incoming personnel during peak periods of shift change, the gate guard has time to only distinguish the color and design of the employee's badge. He says that performing a proper comparison of the individual with his badge picture would soon result in chaos, and that both the delayed employees and their supervisors would create a storm of protest because of the resulting delay in starting production. He also states that identification cards and badges will not keep subversives out of a plant, and that such devices have never been and should never be construed to accomplish such a measure. He feels that subversives will gain admittance to a plant by obtaining a position within the plant instead of resorting to such amateurish measures.

However, according to Davis, badges are of significant value in detecting attempts of unauthorized persons to enter the plant premises. He states that badges and cards are also a help in such things as payroll distribution, tool check-out, and restricted area control. He re-emphasizes that identification systems are not foolproof and are only an aid in accomplishing the over-all security program.[7]

---

[7] John R. Davis, Industrial Plant Protection (Springfield: Charles C. Thomas Publisher, 1957), pp. 260-69.

II. EXCHANGE IDENTIFICATION SYSTEM

One of the most secure identification systems is undoubtedly one which incorporates the above listed features into an exchange system. An exchange system requires that two identical badges are constructed, each one usually of a different color. One badge is issued to the bearer, and the other is kept on file at the security control point. The bearer presents his badge to the control point guard who then carefully makes a three-way comparison of the bearer's badge, the file badge, and the individual. The bearer may or may not then be given the file badge to wear while he is within the controlled area, the badges again being exchanged when he departs through the control point. This system prevents duplication or alteration, since it would be necessary in some way to have a duplicate badge in the guard's file.

The final control point in an exchange system rests with how carefully the guard performs his three-way comparison. This aspect is, of course, one of the major controlling factors in any identification operation, since no system can be any better than its enforcement. Close supervision and follow-up of personnel responsible for checking identification media are necessary to insure the successful operation of any identification system and to keep it from becoming

ineffective and perfunctory.

One disadvantage of the exchange system is that the bearer must enter and exit through the same control point unless additional file badges are made for use at other points. Making additional file badges increases the cost factor and requires elaborate standardization of the control point files to ensure exact duplicity of the records at each point. Another disadvantage is that ingress and egress at the control point is impeded due to the time required for the guard to obtain the file badge from the file and to make the three-way comparison.[8]

III. ELECTRONIC DEVICES

In the past several years the industrial security field has witnessed the introduction of a variety of electronic security devices. Ultra-sonic alarms which detect movement within an area, closed circuit television for monitoring sensitive areas, and electronically coded identification cards for gaining access to secure areas are but a few of these unique systems.[9] A major

---

[8]Edward Brosnan, Personal Interview; David Grand, Personal Interview; Robert Meader, Personal Interview; and Harry Shaw, Personal Interview.

[9]Business Week, "Tightening Up Industrial Security," Business Week, (October 15, 1960), 181-85.

disadvantage of electronic methods is the added cost which, in many security budgets, is found to be prohibitive. However, if the budget will provide, they are very worthy of consideration.[10]

Key-Card System. One of the most widely used devices for personnel identification is the Key-Card system. This system consists of an electronically coded identification card used either by itself or in conjunction with a push button combination. The method which uses only the card requires the bearer of the card to insert the card into a small slot next to the entrance door or turnstile. Electronic wiring laminated inside the card triggers circuitry within the locking mechanism and releases the latch. The bearer then removes his card and enters through the door or turnstile. This system allows any person possessing the card to enter and thereby does not allow suitable protection against unauthorized use of lost or stolen cards. The more secure method incorporates a series of push buttons similar to the keys on an adding machine. The bearer must, in addition to inserting the card, know which keys to press and in what order to press them. Inserting a

---

[10]John R. Davis, Industrial Plant Protection (Springfield: Charles C. Thomas Publisher, 1957), pp. 265-67.

forged card or pressing the keys out of sequence will cause an alarm to sound.[11] Another variation of this system is to require the individual to enter a small cubicle which is built into the perimeter structure of the area being entered. Once inside the cubicle, the bearer inserts the key-card and presses the keys, causing an inner door to open. The doors are inter-locking so that only one can be opened at a time, thereby preventing more than one person from entering at a time. The cubicle also provides complete privacy and prevents unauthorized observation of the key pressing operation. Whenever an employee who knows the key punch combination terminates or is transferred, or in the event of a compromise of the combination, the keys to press and the sequence can be readily changed.[12]

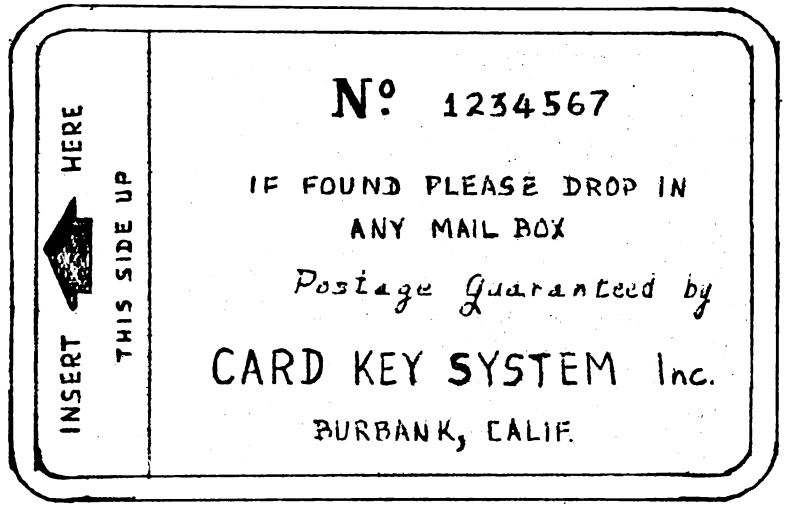
Use of the Key-Card cubicle system has generally been restricted to controlling access to Confidential security areas,[13] because Department of Defense regulations require that admittance to Secret areas must be controlled by guards or by an employee inside the area who unlocks and locks the entrance. Entrance to a Top

---

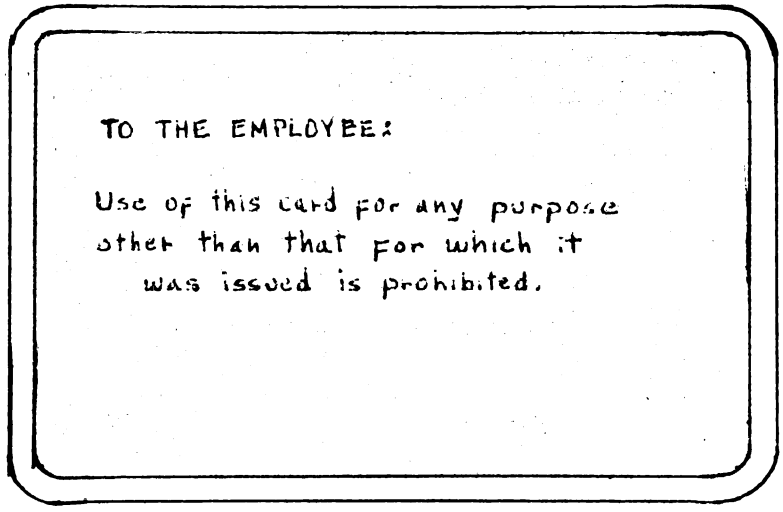
[11] Ibid.; and Identification Brochure from Card Key Systems, Inc., Burbank, California.

[12] Identification Brochure from Card Key Systems.

[13] David Grand, Personal Interview.



FRONT



BACK

FIGURE 2

KEY-CARD IDENTIFICATION
(SAMPLE CARD FROM CARD
KEY SYSTEMS, INC.)

Secret area must always be controlled by a guard. However, the Contracting Officer may, at his discretion, approve the use of electronic identification systems and waive the guard requirement on Secret areas.[14]

Badge System with Changeable Codes. Another excellent identification system which incorporates practically all of the previously listed criteria for badges and passes is the one-piece badge made by Whitehead and Company. This badge also has the added feature of an electronic coding system.

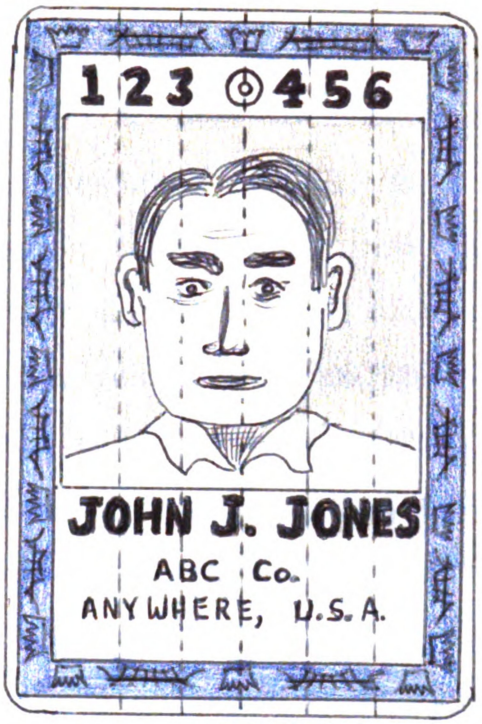
The Whitehead badge consists of a stainless steel plate laminated between sheets of vinyl base plastic. A 1½' by 2" full-face photograph of the bearer is laminated into the front of the badge. Vertical black and gold threads are woven in and out of slits cut into the plastic overlay sheet prior to lamination. This feature prevents superimposing a fraudulent picture over the top of an original photograph or altering the badge serial number. Inks and photographic materials of the same chemical base as the vinyl plastic are used, so that immersing the badge in solutions such as 100 per cent

---

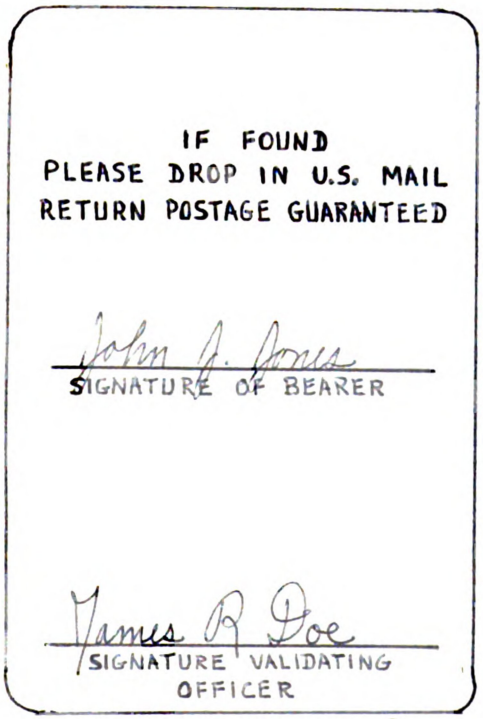
[14]United States Department of Defense, Industrial Security Manual for Safeguarding Classified Information, (Washington: Government Printing Office, November, 1961), pp. 31-32.

acetone will result in dissolving everything but the metal badge core. Lamination with a steel insert makes the badge exceptionally strong and durable. Attempts to alter the badge by relamination causes the detailed engraving of the badge to distort and the electronic coding in the steel core to be erased. Additional information on the front or back of the badge such as color codes and a description of the bearer can be added, if desired.

The stainless steel badge core is designed to allow each badge to be coded by magnetic fluxes to form up to 1,000,000 six digit codes, any one of which can be erased and recoded at will simply by changing the magnetic polarity. Coding is accomplished when the badge is issued and may be changed any time the badge is used. Multiple codes may be entered in each badge for use at different places. Using this magnetic coding feature consists of having the bearer insert his badge in the slot of an electronic "switch-recorder." If the badge is properly coded for that particular entrance, the "switch-recorder" will open the gate or door and allow entry. If the card's coding is not valid, the device locks the card in the slot and sounds an alarm. The additional protective measure of punching a key code combination such as previously described with the Key-



FRONT



BACK

FIGURE 3

ELECTRONICALLY CODED BADGE
(SAMPLE FROM WHITEHEAD AND CO.)

Card system may also be utilized.

Periodically, or whenever the security officer deems it necessary due to lost or stolen badges, all badges can be double-checked by the guards and recoded at the time the bearer inserts his card into the slot. The "switch-recorder" can be set to read or change one or more of any of the possible 1,000,000 codes.[15]

Incorporating this system encounters a major obstacle, since its use in controlling entry to Secret or Confidential areas is limited, as was the Key-Card system, by the Department of Defense regulations. Specific approval of the electronic system and a waiver of the guard requirement would have to be given by the Contracting Officer before this method could be used to control access to Secret or Confidential areas.[16] Such waivers are often difficult, if not impossible, to obtain.[17]

---

[15]Ned Whitehead, President of Whitehead and Company, Inc., Personal Interview, August, 1960; and Identification Brochure from Whitehead and Company, Inc., Washington, D.C., January, 1960.

[16]Industrial Security Manual for Safeguarding Classified Information, pp. 31-32.

[17]David Grand, Personal Interview.

CHAPTER V

MODEL EMPLOYEE IDENTIFICATION SYSTEM

The model system for employee identification presented in this chapter will be in two separate categories. One badge system will apply to perimeter identification and control and will be primarily used for identifying employees who are authorized ingress and egress through a perimeter control point. The other badge system will be for the identification of employees who are authorized admittance to classified closed areas and to provide a means of identifying the bearer's degree of security clearance. Regulations and criteria presented in the preceding two chapters have been used where applicable.

I. PERIMETER IDENTIFICATION

The device recommended for identifying employees who are authorized ingress and egress through a perimeter control point is not designed to identify the degree of security clearance of the holder or to indicate that the holder is authorized to enter closed areas. The device, therefore, would not normally come under the regulations provided in the Department of Defense Industrial Security Manual previously outlined in Chapter III.[1]

---

[1]David Grand, United States Air Force Industrial Security Inspector, Western Contracts Management Region, Mira-Loma, California, Personal Interview, November 14, 1961.

However, since the device presented here will be used in conjunction with another identification card to be presented later in this chapter and designed to identify clearance and closed area access, the Department of Defense regulations will apply.[2] The device will also be based on the seventeen criteria for identification systems listed on pages 23-25.

Identification Device

The recommended device for perimeter control would be a laminated, photo-type badge. Semi-rigid, vinyl-base plastic pre-printed with identifying information would be hot-laminated, along with a poloroid photograph of the bearer, between two pieces of clear, semi-rigid, vinyl-base plastic. The front of the badge would include the employee's name in 3/8" type, employee number, badge number, company name, and employee full-face poloroid photograph measuring 1"x 1½". An additional line would be available to enter information such as odd-shift times or early admittance authorizations. The top and bottom borders of the badge would have an intricate design and all pre-printing would be of vinyl-base inks.

---

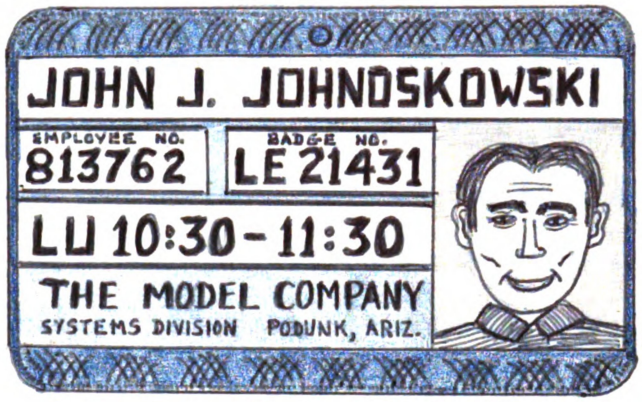
[2]United States Department of Defense, Industrial Security Manual for Safeguarding Classified Information, (Washington: Government Printing Office, November, 1961), p. 8.

The back of the badge would include the employee's social security number, height, weight, birthdate, color of hair, color of eyes, and signature. In addition, the back of the badge would have the date the badge was issued and the facsimile signature of the security manager. Postal instructions for returning the badge would also be included at the bottom.

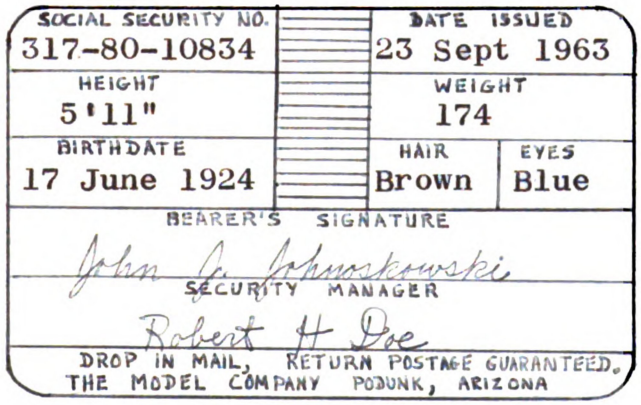
If the company wished to differentiate between salaried and hourly employees, salaried employees would all wear badges of the same color and hourly employees would wear varying colored badges, depending on the shift they work. As an example, salaried employees could wear brown badges, hourly day shift employees could wear blue badges, swing shift could use yellow, and graveyard shift could use red. Letter prefixes would be used with the badge number to designate a variety of information such as "L" for a medical lifting limitation, "T" for tool crib checkout, "E" for inter-departmental parts expiditer, "M" for mail carrier, etc.

Issuance

Newly hired employees would be instructed to report to the Identification Unit by the Employment Department. Each new employee would be instructed to present his employment paper work, such as an Employment Certifi-



FRONT



BACK

FIGURE 4

PROPOSED IDENTIFICATION BADGE

cate or Payroll Addition form to the Identification Clerk.

The Identification Clerk would then check the information on the employee's paper work to determine that the person is a bona-fide employee, check his effective date of employment, whether he is a salaried or an hourly employee, and if he is hourly, what shift he will be working. Whether the new employee has any medical limitations would also be checked on the form, as well as any status as an expediter, mail carrier, odd-lunch time, etc.

The Identification Clerk would then type the appropriate information on an appropriate colored plastic badge core, using a typewriter with special 3/8" type for the information on the front of the badge and a standard typewriter for the back of the badge. The Identification Clerk would then have the employee sign the back of the badge, stamp the badge with the facsimile signature of the Security Manager, take a double poloroid photograph of the employee, and hot laminate the badge core and one photograph between two sheets of clear vinyl plastic. During the few minutes required to hot laminate the badge, the new employee would be given copies of any pertinent security instructions such as badge regulations and procedures, clearance

processing procedures, etc. After completion of the lamination process, an alligator or flat clip would be affixed to the top-center of the badge. The Identification Clerk would then tell the employee when and where to wear the badge and hand the completed badge to the employee.

Whenever an employee would require a duplicate badge because of loss, he would first be instructed to pay a fine at the payroll or cashier's office. The employee would then present the receipt of payment to the Identification Clerk who would make a new badge in accordance with the information obtained from the Identification Unit's records. No fine would be charged for replacing damaged or broken badges. The Identification Clerk would compare the appearance of the employee against the duplicate photograph maintained in the Unit's records before issuing new badges. The Identification Unit would report all instances of badge loss to the Security Office's Investigation Section for their follow-through.

Hourly employees assigned to another shift, promoted to salaried status, or given some other status change would have their badges changed on the effective date of the status change. The employee would present the Change of Status paperwork to the Identification

Clerk who would then construct a new badge for the employee and keep the old badge for subsequent destruction.

Accountability

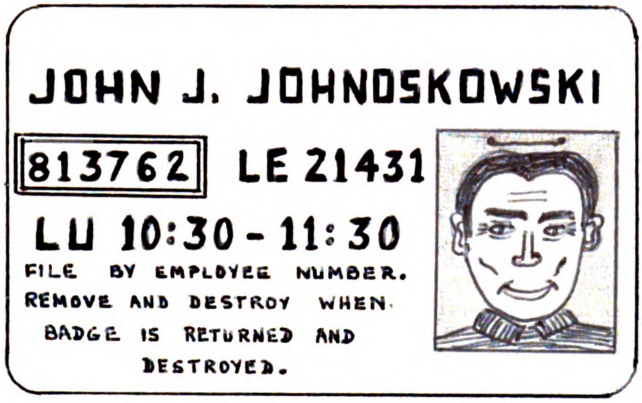
The plastic badge core described in the first part of this chapter would be the first part of a triplicate form. The duplicate and triplicate carbon copies of this form would be used for record purposes at the Identification Unit.

The duplicate copy would be filed by employee number in the Unit's employee number file. The extra poloroid photo of the employee would be stapled to this copy. This file would provide a check on all terminating employees who would be required to process through the Identification Unit prior to receiving their final pay checks. When the badge is returned and destroyed by the Unit, this copy would also be removed and destroyed.

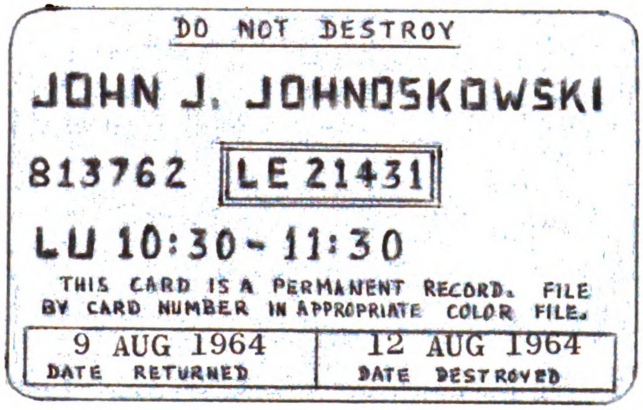
The triplicate copy would be a hard backed permanent record and would be filed by badge number in the appropriate colored file, i.e., brown for salaried, blue for hourly day shift, etc. The dates of badge return and destruction would be entered on this record card.

The forms would all be serially numbered when printed to ensure that no number was ever used twice.

Employees would be instructed to immediately advise their Security Office regarding instances of lost



DUPLICATE



TRIPLICATE

FIGURE 5

PROPOSED IDENTIFICATION BADGE
FILE FORMS

or stolen badges. If subsequent follow-up by the Investigation Section did not satisfactorily determine the disposition of the missing badge, a complete description of the badge would be provided to applicable guard posts. Lists of unresolved badges would be maintained at the posts.

Entry/Exit Procedures

Employees desiring to enter the plant would be required to have their badges in their possession. While inside the plant, each employee would display his badge at or above the waist on his left side. To gain admittance, the employee would hand his badge to the gate guard who would then:

1. Check the badge for authenticity.

2. Cross-check the employee's facial appearance with the photograph on the badge.

3. Verify that the badge color corresponds to the appropriate work shift.

4. Check the back of the badge for the Security Manager's facsimile signature.

5. Return the card to the employee and allow him to enter the plant.

An employee exiting the plant during shift change would be visually checked to verify that he is wearing the badge. Exiting the plant at any other time would

require the guard to verify that the employee is either salaried or, if hourly, has been authorized to depart the plant early as indicated by the odd-lunch time entered on his badge. Hourly employees exiting at any other time would be personally escorted to the gate by their supervisor.

All employees would wear either their permanent badges or temporary badges on their outer garments at or above the waist on their left sides at all times while inside the plant. All guards, employees, and supervisors would be instructed to challenge anyone not displaying his badge and to escort anyone who does not have a badge to the Security Office.

Temporary Identification

Employees who forget their badges would be issued temporary identification badges at the Identification Unit. These badges would be made of heavy paper stock in varying colors corresponding to the different employee status color codes, i.e., brown for salaried, blue for hourly day shift, etc. The badges would be used only within the confines of the plant and would be good for one entry and exit only. When the bearer would leave the plant, the badge would be turned in to the perimeter post guard who would then destroy it. No record of

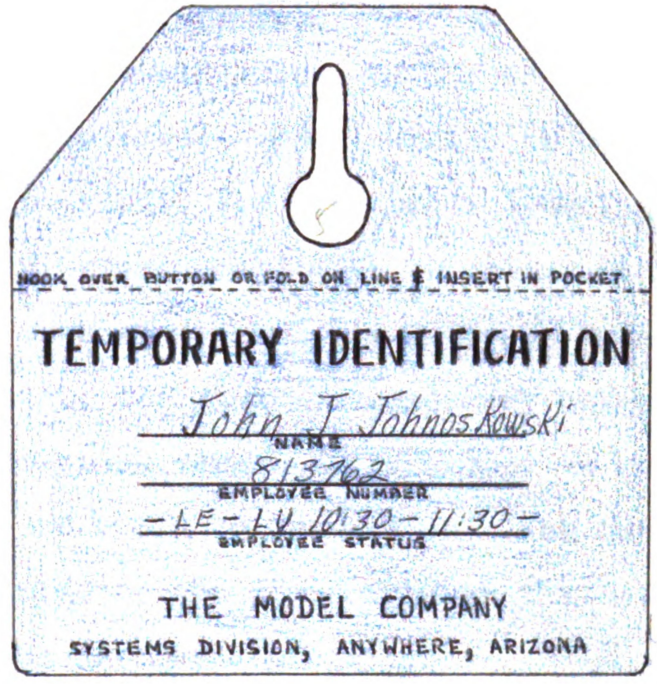


FIGURE 6

PROPOSED TEMPORARY IDENTIFICATION BADGE

issuance or destruction would be maintained.

An employee requiring a temporary badge would report to the outside perimeter entrance of the Identification Unit. The Identification Clerk would have the employee print his name and number on an appropriate colored temporary identification badge form. The Identification Clerk would check the information and photograph on the employee's badge receipt in the Employee Number File to verify the employee's identity. The Identification Clerk would then enter any other status information such as medical limitations, mail clerk, expediter, etc., and give the temporary badge to the employee along with verbal instructions on how to wear it and when and where to turn it in. The employee would then be admitted to the plant through the Identification Unit's outside perimeter entrance.

II. CLOSED AREA AND CLEARANCE IDENTIFICATION

The badge system described in this section is designed to identify employees who are authorized admittance to closed areas and/or to provide a means of identifying their degree of security clearance. As previously stated on page 16, badges used for such purposes are governed by the Department of Defense regulations quoted on pages 16 and 17. The badge system presented in this

section is, therefore, based on these regulations and on the additional criteria for identification systems previously presented in Chapter IV.

The proposed system would identify closed areas by letter designators, i.e., "A", "B", "C", "D", etc. Access to all areas would utilize guards to verify authorized admittance.

Identification Device

The identification device presented here is based on a snap out carbon triplicate form somewhat similar to the badge forms used for perimeter identification. However, there are several basic differences, since this badge is constructed of a soft paper core, is cold-laminated between two pieces of sticky-backed, pressure sensitive plastic, and does not have a photograph of the bearer.

The original copy of this three part form would become the core for the Clearance and Admittance Authorization Card and would be made of the same type of bleeding safety paper used in bank checks. The writer tested several of these safety papers from two paper companies[3]

---

[3]Samples from the Zellerbach Paper Company, South San Francisco, California; and from Blake, Moffitt & Towne, San Jose, California.

and found them all to be similar in that the colored inks used in the distinctive background patterns were extremely sensitive to solvents such as acetone and ink eradicator. Immersing the paper in either of these solutions for a fraction of a second resulted in washing away the colored inks. One of the paper samples also has the added feature that results in the hidden words "STOP" appearing whenever the ink is washed off. Attempts to erase information on the paper also resulted in removing the colored background inks.

All pre-printed information on the form would also be in vinyl base inks as an added deterent against tampering.

Information on the form would be entered by the Identification Unit as authorized by the Security Office, including the employee's name, employee number, card expiration date, areas to which admittance is authorized, and the facsimile signature of the Security Manager. Those areas to which the employee is authorized admittance would be typed on the clearance card as in the following examples:

- - - A C D F J K N O S T - - -

ALL AREAS

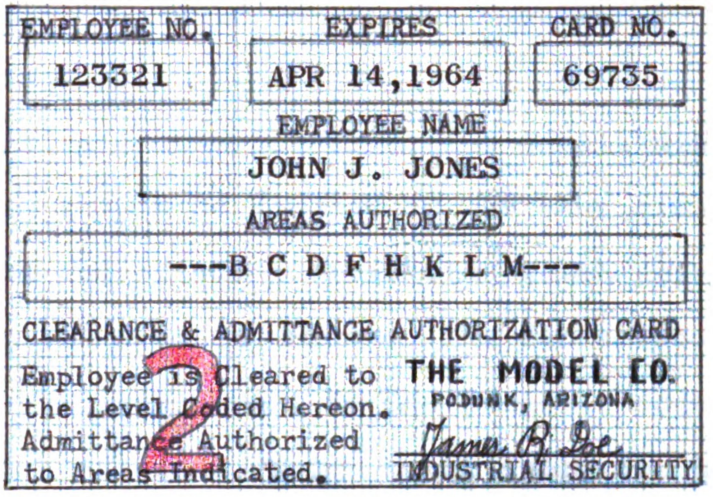


FIGURE 7

PROPOSED CLEARANCE AND ADMITTANCE AUTHORIZATION CARD

The core would be cold laminated between two pieces of sticky-backed, pressure sensitive, clear vinyl base plastic. Peeling this sticky-backed plastic from the core is virtually impossible due to the soft-grade, light-weight paper of which the core is made. However, if the plastic should ever be removed, any typing strike-overs or erasures would be readily apparent to the guard checking the card.

Printing of the Clearance and Admittance Authorization forms should be handled by the same cleared graphic arts and printing facilities which print the company's classified documents. The forms should be treated in the same manner as Confidential documents from the time of final design to delivery to the Identification Unit. By following this rigid control procedure, chance of an unauthorized person obtaining a supply of the forms would be reduced to a minimum.

Determining an employee's degree of security clearance would be accomplished by viewing the red number designator printed on the lower left corner of his Clearance and Admittance Authorization Card. The following code would be used for this purpose:

1 = Confidential

2 = Secret

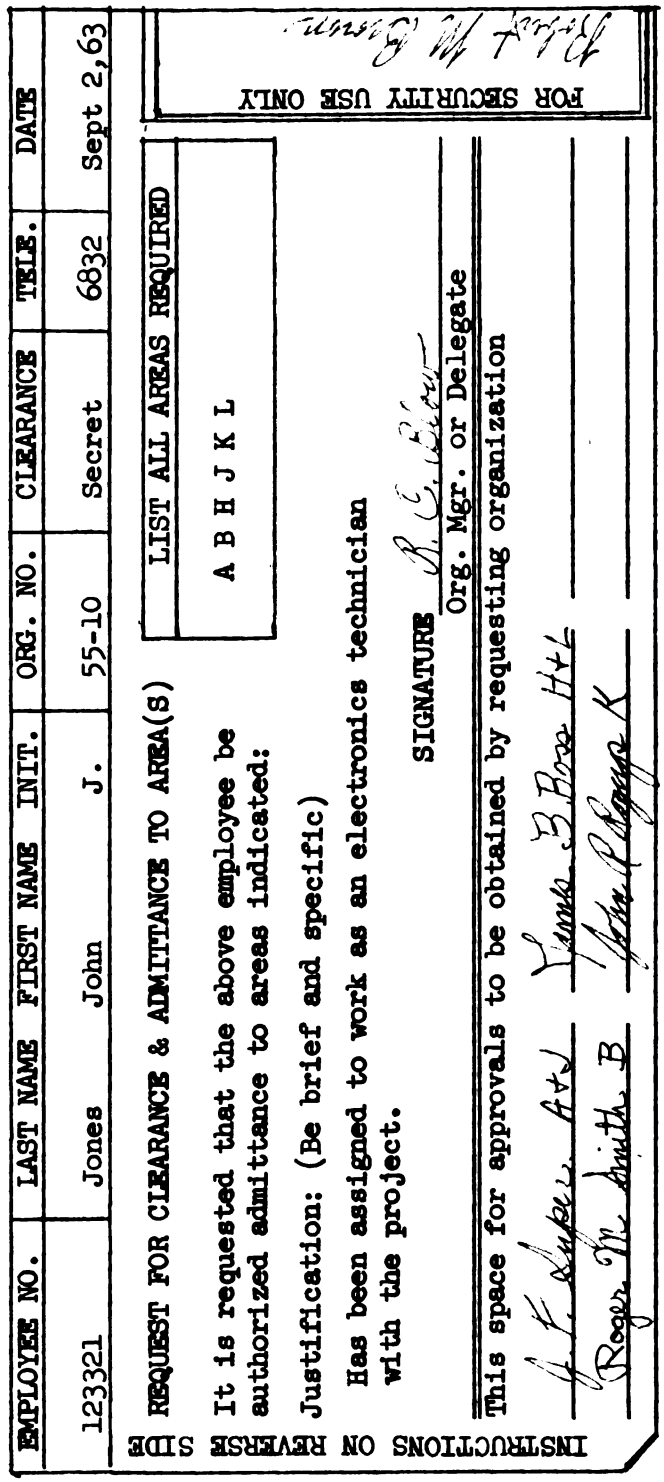
3 = Top Secret

Issuance

Although the governmental regulations listed on pages 16 and 17 refer only to "rigid control and accountability," some method of requesting and authorizing the issuance of Clearance and Admittance Authorization Cards is necessary as indicated in the criteria in item 12, page 24.

As a means of establishing a controlled and standardized request procedure, a "Request for Clearance and Admittance to Area(s)" form would be utilized. These request forms would be initiated by Department Managers or their delegates in accordance with instructions given on the back of the request form.

Upon receiving a completed request form, the Security Office would check the employee's security clearance in the office clearance records, and verify the signature of the requesting Manager or delegate. If the request form was not hand-carried to the Security Office by the Manager or delegate signing the card, a telephone call would be made by the Security Office to the requesting manager's office to verify that the request was properly initiated. A signature list of those Managers and delegates who are authorized to sign the request forms would also be maintained at the Security Office. The request form would then be countersigned



FRONT

FIGURE 8

PROPOSED REQUEST FOR CLEARANCE AND ADMITTANCE TO AREA(S) FORM

PREPARATION INSTRUCTIONS FOR REQUESTING ORGANIZATIONS

1. Use typewriter only.
2. List one employee per card.
3. Complete all items required. Justification should consist of a brief statement of reasons why the employee must be authorized admittance on a continuing weekly basis to the areas requested.
4. Requesting Manager or delegate must sign in ink.
5. Obtain authorized signatures from appropriate closed area supervision for each area requested.
6. Forward completed request to the Area Security Office.

When notified, all previously issued Clearance & Admittance Authorization Cards must be returned to the Area Security Office by the bearer and exchanged for the new card.

RECEIPT ACKNOWLEDGED

John A. Jones
Name

Sept 13, 1963
Date

54321
Card No.

BACK

FIGURE 9

PROPOSED REQUEST FOR CLEARANCE AND ADMITTANCE TO AREA(S) FORM

by an authorized security official in the block "FOR SECURITY USE ONLY" and routed to the Identification Unit via some type of secure plant mail service such as a guard mail service or classified mail service.

The Identification Unit would, upon receiving the request form, verify the authenticity of the security official's signature against a signature list of all authorized signers. After determining the validity of the signature, the Identification Unit would prepare a Clearance and Admittance Authorization Card in accordance with the information on the request form. The Unit would also note the card numbers of all outstanding Clearance and Admittance Authorization Cards previously issued to the employee on the back of the request form. Both the completed card and the request form would be returned to the Security Office via the next day's mail pick-up.

The Security Office would compare the completed Clearance and Admittance Authorization Card against the request form to double check the card's accuracy and then notify the requesting organization by telephone that the card was ready to be picked-up by the employee. Before the employee could obtain the card, he would first have to turn in all previously issued cards which were noted on the back of the request form. The em-

ployee would then sign the back of the request form to acknowledge his receipt of the new card. The Security Office would file the request form for one year as a record of issuance.

Request forms would be handled as a controlled security form. Department Managers and their delegates using the forms would be given explicit instructions about the use of the request form and the necessity for restricting its distribution.

The most inexpensive material at most companies for printing such a form consists of blank computor cards. Blank cards which are normally thrown out by the Data Processing Departments after repeated use could be readily used for printing the request forms. Printing of the forms could be accomplished at most companies by their in-plant printing department at negligible cost.[4]

Accountability

The duplicate copy of the three part form would be filed at the Identification Unit by employee number. The file would thereby identify any employee to whom one or more Clearance and Admittance Authorization Cards had

---

[4]Charles Daubert, Forms Control Department Supervisor, Lockheed Missiles and Space Company, Sunnyvale, California, Personal Interview, November, 1961.

been issued. Upon the return of clearance cards to the Identification Unit for destruction, the corresponding file card would also be removed and destroyed, insuring that this file would indicate issued, non-returned Clearance and Admittance Authorization Cards only. The file would also be used as a control over clearance cards assigned to terminating employees. The form would be made of medium-weight card material. Since the form would remain at the Identification Unit, there would be no need to use the sensitized material recommended for the Clearance and Admittance Authorization Card.

The triplicate copy of the form would be a "hard-back" of heavier grade material, and would be a permanent record of all issuances. Filing would be by Clearance and Admittance Authorization Card number in the appropriate clearance level file, i.e., Confidential, Secret, or Top Secret. Upon return of the clearance card to the Identification Unit, the return date and disposition would be entered on the file form. As with the duplicate copy, there would be no requirement to use sensitized material for this form.

Procedures for reporting instances of lost or stolen cards to the Investigation Section of the Security Office would be identical to that described for the Identification Badge on pages 44 and 46.

EMPLOYEE NO.	EXPIRES	CARD NO.
123321	APR 14, 1964	69735

EMPLOYEE NAME

JOHN J. JONES

2

AREAS AUTHORIZED

---B C D F H K L M---

FILE BY EMPLOYEE NUMBER IN THE EMPLOYEE CLEARANCE CARD FILE. REMOVE AND DESTROY WHEN CARD IS RETURNED TO THE I.D. UNIT.

DUPLICATE

EMPLOYEE NO.	EXPIRES	CARD NO.
123321	APR 14, 1964	69735

EMPLOYEE NAME

JOHN J. JONES

2

AREAS AUTHORIZED

---B C D F H K L M---

DO NOT DESTROY

THIS CARD IS A PERMANENT RECORD. FILE BY CARD NUMBER IN APPROPRIATE CLEARANCE FILE.

DATE RETURNED	DATE DESTROYED

TRIPLICATE

FIGURE 10

PROPOSED CLEARANCE AND ADMITTANCE AUTHORIZATION CARD FILE FORMS

Entry/Exit Procedures

To gain admittance to a closed area, the employee would be required to present his Clearance and Admittance Authorization Card to a guard stationed at the closed area entrance. The guard would then:

1. Check the card for authenticity and validity.

2. Verify that the card has the appropriate lettered area designator.

3. Cross-check the name on the card with the name on the employee's Identification Badge.

4. Cross-check the photograph on the employee's Identification Badge with the employee's appearance.

5. Return the card to the employee and let him enter the area.

No special procedure would be required for an employee to leave a closed area other then to verify that he is wearing an Identification Badge.

Temporary Identification

The Department of Defense regulations outlined on pages 16 and 17 make no provisions for utilizing temporary identification devices to authorize admittance to closed areas. An employee who presents a valid Clearance and Admittance Authorization Card to a closed area guard, but is wearing a Temporary Identification Badge,

would have to be personally identified by supervisory personnel from within the closed area before admittance would be authorized.

Closed Area supervisors would also be allowed to authorize the admittance of employees to the area who require access on a short-time, limited basis. Such employees would be personally identified by the supervisor at the entrance to the area prior to being allowed to enter.

CHAPTER VI

EMPLOYEE IDENTIFICATION SYSTEMS AT THREE SELECTED COMPANIES

This chapter will describe the employee identification systems being used by three selected companies, hereafter referred to as Companies A, B, and C.[1] All three companies are primarily engaged in defense contracts. However, their sizes vary greatly with A Company employing approximately 16,000 people; B Company, 2,000; and C Company, 75.

In order to establish a frame of reference which will lend itself to later comparison of the model with the three systems described in this chapter, the same format used to present the model system will be used in describing the systems of A, B, and C Companies. Accordingly, the systems and procedures for each company will be presented under the two basic categories of: (1) Perimeter Identification and (2) Closed Area and Clearance Identification. Each of these categories will be discussed according to: (1) Identification Device(s), (2) Issuance, (3) Accountability, (4) Entry/Exit Procedures, and (5) Temporary Identification.

---

[1]Since some of the material presented in this study may be critical of the companies studied, the writer feels that, as a matter of propriety, the actual names of the companies should not be used. Instead, the three companies will be fictitiously referred to as Company A, Company B, and Company C.

I. A COMPANY PERIMETER IDENTIFICATION

Approximately 16,000 employees at A Company are classified as either salaried or hourly workers.[2] Salaried employees consist of managerial, supervisory, staff, and engineering personnel and comprise approximately one-third of the company's work force. The other two-thirds of the employees are paid by the hour and work as technicians, shop foremen, production line personnel, secretaries, clerks, and general laborers. All employees are issued an identification card and a badge when they are hired. The same type of identification card is issued to everyone. However, different badges are issued to distinguish the salaried employees from the hourly employees and to identify work shifts.[3]

Identification Devices

One of the employee identification devices used by A Company is a laminated, photo-type Identification Card which is issued to all employees. Paper stock which is pre-printed with a variety of information is

---

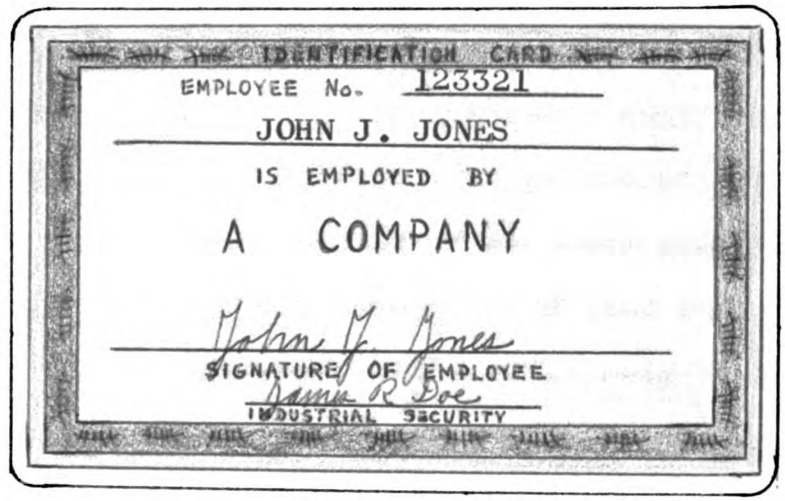
[2]Since A Company has no identification manual for use by its Identification Unit, it was necessary to obtain most of the following data by personally observing and studying the company's practices and procedures.

[3]Personal observation and study conducted by the writer at Company A, July, 1959, to December, 1961.

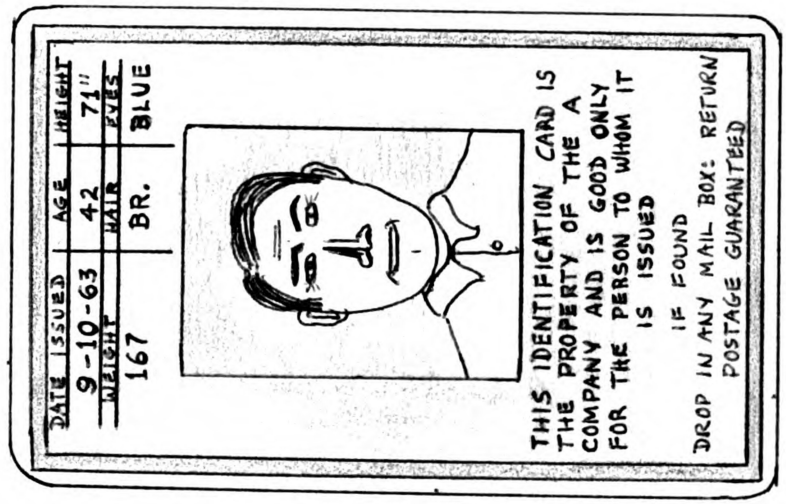
hot laminated, along with a poloroid photograph of the bearer, between two pieces of semi-rigid, vinyl base clear plastic. Information on the front of the card includes the employee's typed identification number, typed name, and signature. The front of the card also contains the name of the company and the authenticating facsimile signature of the company's Industrial Security Manager. The front of the card has an intricate engraved border design to make duplication difficult. The back of the card contains a 1¼" by 1½" full-face photograph of the bearer along with typed information including the employee's age, height, weight, color of hair, color of eyes, and the date the card was issued. The back of the card also has a statement that the card is the property of the company and that it is valid only for the person to whom it is issued. The back of the card also contains a statement of postal instructions for returning the badge to the company. Identification Cards are normally carried in the employee's billfold or purse except when required for plant entry or for some special in-plant requirement such as cashing checks at the cashier's office.[4]

---

[4] Ibid.



FRONT



BACK

FIGURE 11

IDENTIFICATION CARD
(SAMPLE FROM THE "A" COMPANY)

The salaried employee badge is a metal clip-on badge with a paper and plastic insert. The badge is constructed by typing the employee's name on to a colored, pre-printed paper insert, and then placing the paper insert along with a vinyl plastic overlay into the oval shaped metal casing. The assembled badge is placed in a manually operated badge press where the edges of the metal casing are crimped over to hold the paper and plastic inserts in place. A clip is built into the back of the metal casing and can be used as a pin-on badge or can be affixed with a clamp or alligator clip to avoid tearing the employee's clothing.[5]

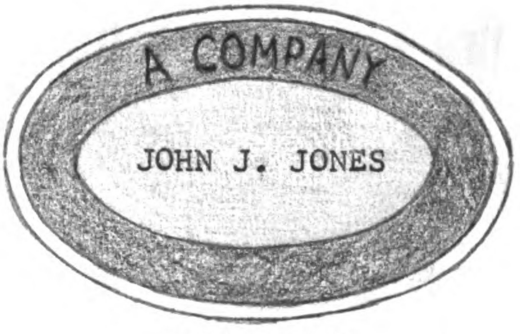


FIGURE 12

SALARIED BADGE
(SAMPLE FROM A COMPANY)

---

[5]Personal Observation and study conducted by the writer at Company A, July, 1959, to December, 1961.

The badge which is issued to hourly employees is similar to the salaried badges in materials and construction, the distinction being that it is round and of different colors. The border of the hourly badge is color-coded to distinguish which shift the employee works and whether he is a shop foreman. Medical limitations, if applicable, are entered as "M" below the employee's name.[6]

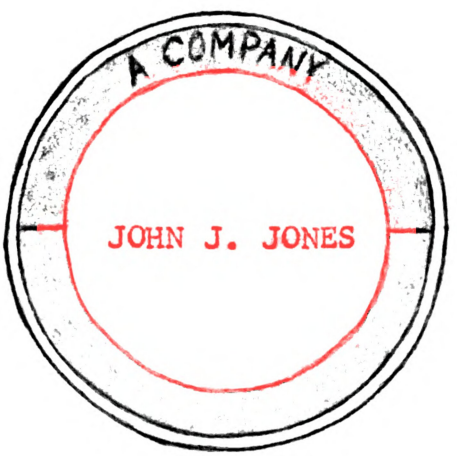


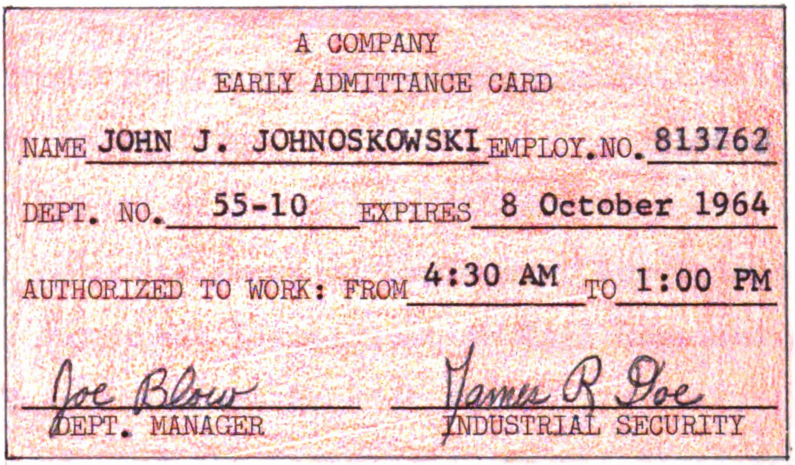
FIGURE 13

HOURLY BADGE
(SAMPLE FROM A COMPANY)

---

[6] Ibid.

Early Admittance and Odd-Shift/Odd-Lunch Cards are also issued to authorized hourly employees to allow entering the plant prior to their normal shift entry time and to allow entry and exit due to working a non-standard shift. Both cards are composed of heavy paper stock which is cold laminated between two pieces of pressure sensitive, sticky-backed vinyl plastic.[7]



A COMPANY
EARLY ADMITTANCE CARD

NAME JOHN J. JOHNOSKOWSKI EMPLOY. NO. 813762

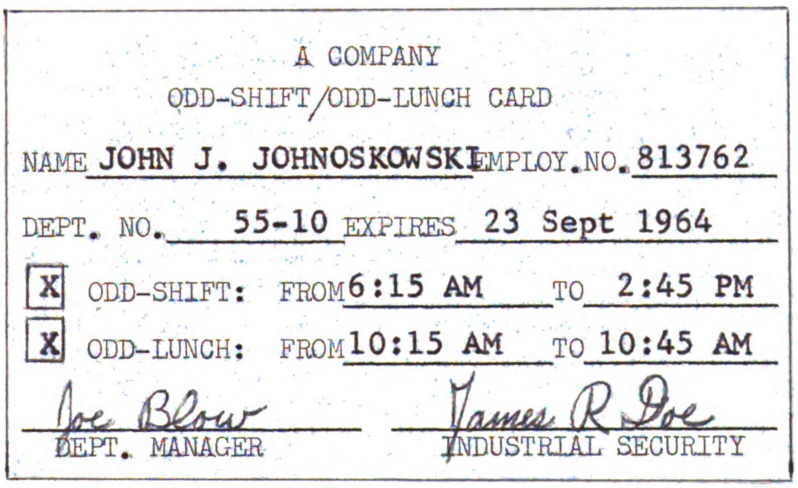
DEPT. NO. 55-10 EXPIRES 8 October 1964

AUTHORIZED TO WORK: FROM 4:30 AM TO 1:00 PM

Joe Blow
DEPT. MANAGER

James R Doe
INDUSTRIAL SECURITY

EARLY ADMITTANCE CARD



A COMPANY
ODD-SHIFT/ODD-LUNCH CARD

NAME JOHN J. JOHNOSKOWSKI EMPLOY. NO. 813762

DEPT. NO. 55-10 EXPIRES 23 Sept 1964

[X] ODD-SHIFT: FROM 6:15 AM TO 2:45 PM

[X] ODD-LUNCH: FROM 10:15 AM TO 10:45 AM

Joe Blow
DEPT. MANAGER

James R Doe
INDUSTRIAL SECURITY

ODD-SHIFT/ODD-LUNCH CARD

FIGURE 14

EARLY ADMITTANCE AND ODD-SHIFT/ODD-LUNCH CARDS
(SAMPLE FROM THE A COMPANY)

---

[7] Ibid.

Issuance

The Employment Department of the A Company instructs newly hired employees when to report to the Identification Unit for badging. Since the Employment Department is located outside the main plant, and the Identification Unit has a special admittance door directly from outside the plant perimeter, no type of temporary badge is necessary for new hires. Each new employee reporting to the Identification Unit will have in his possession:

1. Notice of Payroll Addition Form.
2. Acknowledgment of Employment Conditions Form.
3. Permanent Identification Card Core and an attached Pass and Badge Receipt Form.[8]

By checking the information on the first two forms, the Identification Clerk determines that the person is a bona-fide employee, verifies his effective date of employment, whether he is a salaried or hourly employee, and, if he is hourly, what shift he will be working and whether he is a shop foreman. The Identification Clerk then takes a double poloroid photograph of the employee, stamps the Identification Card core with the facsimile signature of the Industrial Security Manager, and laminates one picture and the card core be-

---

[8]Personal observation and study conducted by the writer at A Company, July, 1959, to December, 1961.

tween two pieces of clear vinyl plastic. No typing is done on the card core by the Identification Unit, as all typed information is entered on the card by the Employment Department. While the card is being laminated, the Identification Clerk constructs an appropriate hourly or salaried badge, based on the information given on the employment forms. The laminated Identification Card and the badge are then handed to the employee. The Identification Clerk tells the employee when and where to wear the badge, when to use the Identification Card, and hands him a booklet on security rules and regulations.[9]

Whenever an employee requires a duplicate card or badge due to loss or mutilation, he must first pay one dollar per card or badge to the Payroll Department. Upon presenting the receipt of payment to the Identification Unit, a new card or badge is made up for the employee based on the information contained in the Unit's records.[10]

Hourly employees who have been promoted to shop foreman or to salaried status, or who have been assigned to another shift, must have their badges changed on the

---

[9]Personal observation and study conducted by the writer at A Company, July, 1959, to December, 1961.

[10]Ibid.

effective date of the status change. Changing badges is accomplished upon the employee presenting a valid Change of Status Form to the Identification Unit. Upon receipt of this form, the Identification Clerk issues a new badge and retains the old one for subsequent destruction.[11]

Early Admittance and Odd-Shift/Odd-Lunch Cards are issued by the Identification Unit upon receipt of an inter-office memo request from a Department Manager or Supervisor. The Identification Clerk then completes a card with the employee's name and number, the expiration date of the card, and the authorized entry and/or exit times. The card is stamped with the facsimile signature of the Industrial Security Manager and signed by the employee's supervisor. Requests may be received by the Identification Unit through the intra-plant mail system, and completed cards may be sent out the same way. There is no requirement for the employee to personally come to the Identification Unit for either card to be issued. Cards may be issued for a specific number of days or may be issued for an indefinite period at the discretion of the requesting Manager or Supervisor.[12]

---

[11]Personal observation and study conducted by the writer at A Company, July, 1959, to December, 1961.

[12]Ibid.

Accountability

The Identification Card core which was filled out by the Employment Department and hand-carried by the new employee to the Identification Unit is the first part of a two part form. The second part is a hard-backed Pass and Badge Receipt Card which becomes the employee's permanent identification record at the Identification Unit. Prior to lamination, the Pass and Badge Receipt Card is detached from the card core. The Identification Clerk staples the extra poloroid photograph to the Pass and Badge Receipt Card, enters the word salaried or hourly, shift number, and whether the employee is a shop foreman. An "M" is entered for those employees having medical limitations. The Pass and Badge Receipt Card is then filed in the employee file by employee number. Notation of any subsequent change in status such as a change of shift, promotion to salaried status, etc., is also noted on the Pass and Badge Receipt Card.[13]

Employees terminating their employment with the Company must process through the Identification Unit to turn in all outstanding badges. This procedure enables the Identification Unit to determine whether the employee has turned in all badges and cards which

---

[13] Ibid.

PASS & BADGE RECEIPT

123321
employee no.

JOHN J. JONES
name

2
shift

6/10/3
date

55-10
orgn.

5
fac.

	HOURLY	X
	FOREMAN	
	SALARIED	

I hereby acknowledge receipt of the above property. I will wear my badge in plain sight and carry my identification card on my person at all times when on the premises of the A Company. I authorize the company to deduct $1.00 for each item that I may lose.

Date Issued June 10 '63 Signature John J. Jones

FIGURE 15

PASS AND BADGE RECEIPT CARD
(SAMPLE FROM THE A COMPANY)

have been issued to him. However, the company is making no attempt to follow through on instances of badge loss, theft, non-accountability, etc., to determine disposition.[14]

Entry/Exit Procedures

Salaried employees are allowed to enter and exit the plant at any time and are not required to punch time clocks. Hourly employees must enter the plant and clock-in within the period thirty minutes prior to their shift start time. Hourly employees must clock-out within the thirty minutes after their work shift ends. Both salaried and hourly employees follow the same procedure to enter the plant with the exception that approximately thirty of the company's top management personnel are allowed "visual recognition" by the gate guards and do not have to follow the normal gate procedure. All employees must wear their badges when entering or leaving the plant and at all times inside the plant. To gain admittance, the employee presents his Identification Card to the gate guard who then:

1. Checks the card for authenticity.

2. Cross-checks the name on the employee's badge with the name on the Identification Card.

---

[14]Personal observation and study conducted by the writer at A Company, July 1959 to December, 1961.

3. Cross-checks the employee's facial appearance with the photograph on the back of the Identification Card.

4. Checks hourly badges to make sure they have the appropriate shift color code.

5. Returns the Identification Card to the employee and allows him to enter the plant.[15]

Hourly employees who are authorized early admittance or odd-shift/odd-lunch entry also must present the appropriate admittance card to the guard. Exit from the plant is allowed for any employee who is wearing either a salaried badge or an hourly badge with the correct shift color code. Hourly employees leaving the plant due to odd-shift/odd-lunch must also show their cards to the guard.[16]

Employees of A Company are required to wear their badges on their outer garments at or above the waist on their left sides at all times while inside the plant. All employees, supervisors, and the roving security guards are instructed to challenge anyone not displaying his badge. If the person does not have a badge, he is escorted to the Security Office for further checking.[17]

---

[15]Personal observation and study conducted by the writer at A Company, July, 1959, to December, 1961.

16 & 17 Ibid.

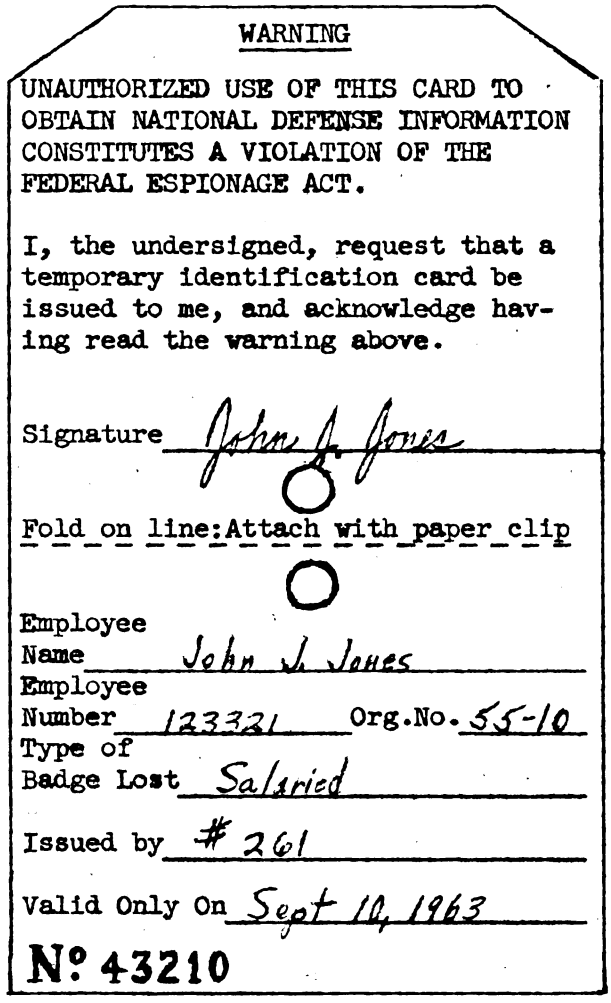
Temporary Identification

Whenever an employee forgets or loses his Identification Card and/or Badge, he is issued a Temporary Identification Pass to be used until such time as he retrieves the Identification Card and/or Badge or is issued duplicate identification by the Identification Unit.[18]

If the employee forgets his Badge but has his Identification Card, he must present his Identification Card to the gate guard. After the employee is compared against the card photograph, he is handed a Temporary Identification Pass and instructed to complete the information required. This includes his name, employee number, organization number, type of badge lost, and his signature. The guard then visually checks the information and enters the "Valid Only On" date and his guard badge number in the "Issued By" blank. The guard has no way of knowing whether the employee is salaried or hourly and can only take the employee's word for it. If the employee does not have his Identification Card with him, the employee must call his salaried supervisor on the gate phone and have him come to the gate and personally vouch for him, after which a temporary

---

[18]Personal observation and study conducted by the writer at A Company, July, 1959 to December, 1961.



WARNING

UNAUTHORIZED USE OF THIS CARD TO OBTAIN NATIONAL DEFENSE INFORMATION CONSTITUTES A VIOLATION OF THE FEDERAL ESPIONAGE ACT.

I, the undersigned, request that a temporary identification card be issued to me, and acknowledge having read the warning above.

Signature John J. Jones

Fold on line:Attach with paper clip

Employee Name John J. Jones

Employee Number 123321 Org.No. 55-10

Type of Badge Lost Salaried

Issued by # 261

Valid Only On Sept 10, 1963

No 43210

FIGURE 16

TEMPORARY IDENTIFICATION PASS
(SAMPLE FROM THE A COMPANY)

pass is completed. Temporary passes are attached to the employee's outer garment with a paper clip when being used in place of a badge. When taking the place of an Identification Card, they are kept in the Employee's pocket or purse.[19]

The temporary passes are valid for one day only and are turned in to the gate guard when the employee leaves the plant. The passes are also serially numbered. However, the only record kept of their issuance is the total number issued per month. The number on the pass is primarily used as a psychological deterrent to make the employee think that a record is kept and therefore motivate him to turn the pass in at the gate when he leaves.[20]

Use of a florescent colored pass was initiated as a measure to reduce the high number of passes being issued under a prior system which used a pass made of plain white paper. It was thought that by using an obnoxiously bright florescent colored badge, employees would dislike it so much that they would remember to bring their regular Identification Cards and Badges. During the six month period prior to changing to the florescent color, monthly statistics kept by the guard

---

[19]Personal observation and study conducted by the writer at the A Company, July, 1959, to December, 1961.

[20]Ibid.

force and Identification Unit showed an average of 2,536 Temporary Identification Passes issued per month. After using the florescent pass for three months and distributing a letter to all supervisory personnel about the problem, statistics showed an average issue rate of 2,385 per month, an average decline of 151 passes.[21]

---

[21] Ibid.

II. A COMPANY CLOSED AREA AND CLEARANCE IDENTIFICATION

The A Company has approximately seventeen closed areas, both Confidential and Secret. Areas are identified by a lettering system, i.e., A, B, C, D, etc. Access to all of the Secret areas and to the larger Confidential areas is controlled by guards. Access to the smaller Confidential areas is controlled by the Key-Card cubicle system previously described.[22]

The identification materials used by the A Company for controlling admittance to closed areas and in identifying employees' levels of clearance are all purchased from outside suppliers and vendors.[23] A check of the facility security clearance records revealed that none of these subcontractors has ever been processed for or granted a Facility Security Clearance.[24]

Identification Devices

In those areas controlled by guards located at the entrances, two methods are used to identify those employees authorized to enter. In Secret areas of an extremely sensitive nature, access lists of authorized

---

[22 & 23]Personal observation and study conducted by the writer at A Company, July, 1959, to December, 1961.

[24]Composite listing of contractor Facility Security Clearances maintained by A Company's Security Office.

employees are positioned at the guard posts. Confidential and Secret closed areas conducting operations of a less sensitive nature and requiring a large volume of employee ingress and egress, utilize a Clearance and Admittance Authorization Card as a means of identifying those employees who are authorized access.[25]

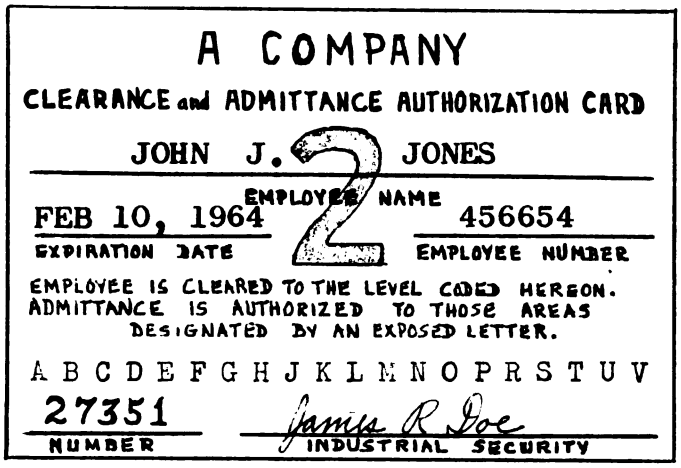
Clearance and Admittance Authorization Cards are constructed of a heavy paper stock which is cold laminated between two pieces of pressure sensitive, sticky-backed clear vinyl plastic. Information typed on the card includes the employee's name, employee number, expiration date of the card (no more than six months), Industrial Security Manager's facsimile signature, and serialized card number. Areas to which the employee may be authorized admittance are identified by letters which have been pre-printed on the card. Areas not authorized are punched out with a hand operated hole puncher, thereby leaving only authorized areas exposed on the card.[26]

Employees' clearance levels are identified on the Clearance and Admittance Authorization Cards by a large red number code in the center of card. The

---

[25]Personal observation and study conducted by the writer at A Company, July, 1959, to December, 1961.

[26]Ibid.



FRONT

FIGURE 17

CLEARANCE AND ADMITTANCE AUTHORIZATION CARD
(SAMPLE FROM "A" COMPANY)

number 1 = Confidential, 2 = Secret, and 3 = Top Secret. A Company is also allowing another method of identifying security clearance to exist that is not authorized by the Company's management or Security Office. All employees are granted a Confidential clearance and an employee salaried or hourly badge on their effective date of employment. It is therefore being assumed that any person inside the plant perimeter who is wearing an employee badge also has at least a Confidential clearance; i.e., the employee badge, which is not an authorized device to identify level of clearance, is being used for this purpose.[27]

Key-Card cubicles are installed in the perimeter walls of several Confidential closed areas that do not have a high volume of personnel traffic. Different cards are issued for each closed area so that the cards for one area will not work the cubicle entrances at another area. Key-cards were previously described and illustrated on pages 30 to 33.

Issuance

Access lists of authorized employees are compiled by the Department Manager(s) who controls the area's operations. Lists are then hand-carried to the Security

---

[27] Ibid.

Office for verification of the employees' security clearances. After the lists are signed by both the requesting Department Manager and an authorized representative of the Security Office, the lists are placed at the appropriate closed area guard posts by the Guard Captain. Additions or deletions to the lists are processed in the same manner.[28]

Requests for Clearance and Admittance Authorization Cards are initiated by the appropriate Department Manager and routed to the Security Office for verification of clearance. These requests, in the form of interoffice memos, vary in size from standard typing paper to 5" by 9" short forms. The wording is usually different on each request, required information is often omitted, and the authorization signatures are often written sideways in the margins, upside down, and across the face of the request. After being signed by both the requesting manager and the Security Office representative, the memo request is routed to the Identification Unit. Upon receipt of the memo, the Identification Clerk types in the required information and punches out those areas not authorized. The card is then cold

---

[28]Personal observation and study conducted by the writer at A Company, July, 1959, to December, 1961.

laminated and routed back to the Security Office for issuance to the employee.[29]

The typical Clearance and Admittance Authorization request is for admittance to four areas. Since the card has a possible total of eighteen letters exposed, the Identification Clerk making the card averages fourteen punches per card. At the average issue rate of 1300 cards per month, the Identification Unit is making approximately 18,200 holes with a hand operated paper punch every month.[30]

Key-Cards are issued by the Security Office upon receipt of an inter-office memo request from the Department Manager of the closed area. At the time the employee is issued his Key-Card, he is also told the current key combination being used for the cubicle. The key punch sequence is periodically changed by the Security Office or at any other time it may be deemed necessary. Whenever the sequence is changed, those employees having need of the new sequence are advised of it through the Department Manager of the area involved.[31]

---

[29]Personal observation and study conducted by the writer at A Company, July, 1959 to December, 1961.

[30]Ibid.

[31]Ibid.

Accountability

No records of access lists are maintained. Superceded or obsolete lists are destroyed by the Security Office.[32]

Records of Clearance and Admittance Authorization Card issuances are maintained at the Identification Unit. A register form is maintained which lists the number of each badge issued in numerical order. The employee's last name and initials, employee number, and expiration date are also entered, and the areas to which the employee is authorized admittance are circled. All entries are made in ink. When badges are returned to the Identification Unit for destruction, the date returned is entered on the register form.[33] Figure 18 shows the register form with several sample entries.

Accountability of Clearance and Admittance Authorization Cards is further maintained by entering the number of the issued card on the employee's Pass and Badge Receipt Card as a means of checking to see that the Clearance and Admittance Authorization Card is returned when the employee terminates. Whenever a card

---

[32]Personal observation and study conducted by the writer at A Company, July, 1959, to December, 1961.

[33]Ibid.

CLEARANCE & ADMITTANCE AUTHORIZATION CARDS

SER. NO.	NAME	EMP. NO.	AREAS	EXP. DATE	RET. DATE
27349	Mary C. Employee	427601	A (B) C (D E F G) H J K L (M N) O P R S T	Feb 9 1964	
27350	John Q. Public	279335	A B C D E (F G) H J K L M N (O P) R S T	Feb 10 1964	
27351	John J. Jones	456654	(A B C D E F G H J) (K L M N O P R S T)	Feb 10, 1964	
27352	Robert R. Smith	196822	A (B C D E) F G H J K L M (N O P) R S T	Feb 10, 1964	
			A B C D E F G H J K L M N O P R S T		
			A B C D E F G H J K L M N O P R S T		
			A B C D E F G H J K L M N O P R S T		
			A B C D E F G H J K L M N O P R S T		
			A B C D E F G H J K L M N O P R S T		
			A B C D E F G H J K L M N O P R S T		
			A B C D E F G H J K L M N O P R S T		
			A B C D E F G H J K L M N O P R S T		
			A B C D E F G H J K L M N O P R S T		
			A B C D E F G H J K L M N O P R S T		
			A B C D E F G H J K L M N O P R S T		

REGISTER FORM
(SAMPLE FROM A COMPANY)

FIGURE 18

is turned back into the Identification Unit, the card number which was entered on the Pass and Badge Receipt Card is crossed-out.[34]

The control and accountability system for the Clearance and Admittance Authorization Cards has been firmly established at the A Company. Records maintained at the Identification Unit provide a positive means of accountability. A check of Identification Unit records indicated that less than one per cent of all cards issued have been lost or not turned back in upon termination of employment. The Identification Unit immediately notifies the Investigation Section of the Security Office whenever a Clearance and Admittance Authorization Card is reported lost or is not turned in at the appropriate time. However, no notification is provided to the guards so that they can check for unauthorized use of lost or terminated cards.[35]

Use of Key-Card cubicles for controlling admittance to Confidential Closed Areas was approved by A Company's Contracting Officer. The requirement for using names and photographs on the Key-Cards was waived, providing the requirements for rigid accountability

---

[34] Ibid.

[35] Ibid.

were strictly adhered to and the key punch sequence was changed periodically.[36]

Whenever a Key-Card is issued by the Security Office, a receipt form, illustrated in Figure 19, is signed at the Security Office by the receiving employee and is maintained in the Security Office's files. The memo requests are filed by requesting organization number. Both the receipt form and memo request are destroyed when the card is returned.[37]

No control is being maintained over the return of Key-Cards when an employee transfers or terminates. The Identification Unit is not advised of Key-Card issuance by the Security Office, and therefore has no way of knowing whether a transferring or terminating employee should turn in a Key-Card. This lack of control is also negating any positive enforcement in changing the Key-Card punch sequence whenever an employee terminates or transfers, since the clerk in the Security Office who handles the Key-Card records is not being informed of employee transfers and terminations.[38]

---

[36]Letter to the A Company from the Air Force Contracting Officer, October 13, 1959.

[37]Personal observation and study conducted by the writer at A Company, July, 1959, to December, 1961.

[38]Ibid.

RECEIPT FOR KEY CARD

This is to certify that I, the undersigned, have been issued Key Card number 123456-1 on 12 Sept 1943.
This card is for my personal use only and will not be loaned to anyone else, and I agree not to misuse this card in any way.
I understand that to do so will be a violation of security and may be cause for disciplinary action as prescribed by company policy.
Further, the loss of this card, and circumstances surrounding the loss, must be reported in writing immediately to the Area Security Office.

John B. Jones
Recipient

123321
Employee Number

55-10
Department

James R. Jones
Issuing Authority
Security Office

FIGURE 19

RECEIPT FOR KEY-CARD
(SAMPLE FROM THE A COMPANY)

Entry/Exit Procedures

An employee whose name appears on an Access List may be allowed to enter the area by presenting either his Identification Card or a Temporary Identification Pass to the guard. The guard cross-checks the name and the employee number on the card or pass with that on his access list. He then cross-checks the photograph on the Identification Card with the appearance of the employee. This photo check is not possible, however, with the Temporary Identification Pass, since it has no photograph. If the checks are satisfactory, the card or pass is returned to the employee, and he is allowed to enter the area. No special checks are performed to leave the area.[39]

Employee admittance to those areas controlled by Clearance and Admittance and Authorization Cards is accomplished by presenting both a valid Clearance and Admittance Authorization Card and an Identification Card (or Temporary Identification Pass) to the guard at the closed area entrance. The guard then:

1. Checks both cards for authenticity and validity.

2. Verifies that the Clearance and Admittance Authorization Card has the appropriate area listed.

---

[39] Ibid.

3. Cross-checks the names on both cards with the badge he is wearing.

4. Cross-checks the photograph on the Identification Card with the employee's appearance.

5. Returns the Cards to the employee and lets him enter the area.

No special procedure is accomplished for the employee to leave the area.[40]

No guards are used at Key-Card entrances. Admittance is gained by entering the outer door of the cubicle, inserting the Key-Card in the slot, pressing the correct button combination, and then entering through the inside door. Only one door opens at a time, and a weight sensitive floor is connected to the door-locking mechanism, so that excessive weight on the floor will lock both doors and sound an alarm. Removing power from the cubicle or any attempt to force entry also results in sounding the alarm and locking both doors.[41]

Temporary Identification

Temporary Admittance Authorization Passes are used at all Confidential and Secret closed areas to authorize entry up to one week. Employees who will

---

[40]Personal observation and study conducted by the writer at A Company, July, 1959, to December, 1961.

[41]Ibid.

only require short term access are issued this pass so that permanent cards need not be issued. Booklets of the paper passes are issued to those Department Managers and their delegates who have jurisdiction over the closed area for use in authorizing employees to enter the area.[42]

The pass is filled out in duplicate by the authorizing official, the original going to the employee and the duplicate staying in the book. Upon presenting the pass to the guard at the area entrance, the employee signs in on a guard register form and enters the area. A list of those managers and their delegates who are authorized to sign the temporary passes for that particular area is maintained at the guard post. The authorizing official is responsible for verifying and certifying to the employee's clearance and need to be in the area before he issues the pass.[43]

Initial issuance of the books of temporary passes must be approved by the Security Office. Renewal of used-up books is accomplished by exchanging the old book for a new one at the Security Office. A secretary in the Security Office maintains a list of

---

[42] Ibid.

[43] Ibid.

DATE: 10 Sept 63

A COMPANY TEMPORARY ADMITTANCE AUTHORIZATION TO CLOSED AREAS

NUMBER: 456654

NAME: John L. Brown

EMPLOYEE NUMBER: 123321

ORGANIZATION: 55-11

PHONE: X 3456

AUTHORIZED ENTRY TO CLOSED AREA(S): A + C

FROM: 10 Sept 63 THROUGH: 13 Sept 63

PURPOSE: Technical assistance to the project

AUTHORIZING DEPARTMENT MANAGER OR DELEGATE

Roger L. Brown Mgr. 67-32

FIGURE 20

TEMPORARY ADMITTANCE AUTHORIZATION (SAMPLE FROM THE A COMPANY)

each person who has been issued a book.[44]

Many of the several dozen managers and their delegates authorized to issue Temporary Admittance Authorization Passes are making it a common practice to leave the books of blank passes unprotected. The writer, on numerous occasions, found blank books of passes in unlocked desks, on top of desks, on top of bookcases, and in one instance, in a wastebasket.[45]

Each closed area guard post is provided with a list of those managers and delegates who are authorized to sign passes for that area. However, no corresponding list of sample signatures is provided to the guard so he can verify that the signature appears to be authentic.[46]

No control is being maintained over books assigned to employees who are transferred or terminated. Managers and delegates who transfer from or terminate their positions are not required to process through the Security Office. Although terminating employees process through the Identification Unit, the unit does not have a record of pass book issuances and is therefore unable to check on this problem. This deficiency makes it impossible; (1) to assure that books of unused passes are

---

[44]Personal observation and study conducted by the writer at A Company, July, 1959, to December, 1961.

[45]Ibid.

[46]Ibid.

are returned when they should be and (2) to keep the guard post authorization lists up to date.

Managers in charge of Confidential areas that are controlled by Key-Cards are allowed to authorize the admittance of employees who require entry on a limited basis. In these instances, the Manager opens a door to the area that is normally secured with a combination security lock to allow temporary admittance. Leaving the area is via the Key-Card cubicle.[47]

---

[47] Ibid.

III. B COMPANY PERIMETER IDENTIFICATION

B Company makes no distinction between hourly and salaried employees. Each of the approximately 2,000 employees are issued a clip-on badge when they are hired.[48]

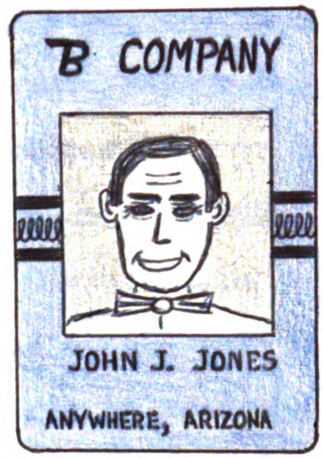
Identification Device

The badge used to identify employees is a laminated, photo-type badge. Paper stock which has been pre-printed with a variety of information on both sides is hot laminated, along with a photograph of the bearer, between two pieces of clear vinyl plastic. The front of the badge has the employee's name and a 1" by 1&1/8" full face poloroid photograph, along with the company name and address. The front of the badge also has an intricate design. The back of the badge has the employee's number, badge number, date issued, date of birth, color of hair, color of eyes, weight, height, employee signature, and Security Manager facsimile signature. An alligator clip is affixed to the top of the badge for attaching to the employee's outer garment. Postal instructions for returning the badge are also included.[49]

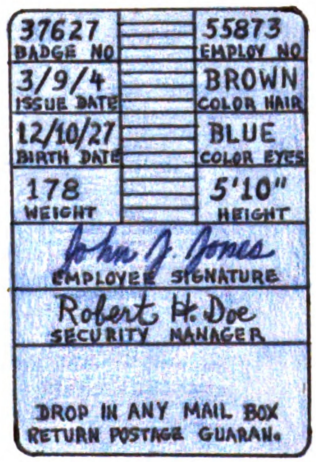
---

[48] B Company Division Procedure Manual; Personnel Identification Section. Procedure 3.101. section 3; and Personal observation and study conducted by the writer at B Company, December, 1961, to August, 1962.

[49] Ibid.



FRONT



BACK

FIGURE 21

IDENTIFICATION BADGE
(SAMPLE FROM THE "B" COMPANY)

Issuance

New employees report to the Security Office as part of their processing procedure. In addition to other security processing, the Security Clerk handles identification matters. Each new employee is instructed by the Personnel Department to present his employment papers to the Security Clerk.[50]

The Security Clerk checks the paper work to verify that the person is a bona-fide employee and to determine the effective date of employment. The clerk then types the appropriate information on a badge core, has the employee sign the back of the badge, stamps the badge with the Security Manager's facsimile signature, takes a poloroid photograph of the employee, hot laminates the photograph and badge core between two pieces of clear vinyl plastic, and attaches an alligator clip to the top of the badge. The clerk then gives the badge to the employee and tells him when and where to wear it.[51]

The Security Office charges a one dollar fee to replace a lost badge. Broken or damaged badges are replaced without fee.[52]

---

[50]Personal observation and study conducted by the writer at B Company, December, 1961, to August, 1962.

[51]Ibid.

[52]B Company Division Procedure Manual; Personnel Identification Section. Procedure 3.101, section 3.

Employees requiring changes in the information on the badge such as a marriage name change are able to accomplish this by presenting change of status paperwork from the Personnel Department to the Security Clerk. The Security Clerk then issues a new badge and retains the employee's old badge for destruction.[53]

Accountability

The badge core is a one-piece form. The only record of badge issuance is maintained by the Security Office Clerk on 5" by 7" file cards that are filed alphabetically by employee last name. Whenever a badge is issued, the Security Clerk types in the name of the employee, employee's number, badge number, and date of issuance on the file card. This card is also utilized for other security information such as level of clearance, date clearance was granted, etc. Whenever a badge is returned, this is also noted on the card. When an employee terminates, the card is removed and filed alphabetically in an inactive file.[54]

There is no file maintained by badge number. Badge numbers are assigned numerically by the Security

---

[53]Personal observation and study conducted by the writer at B Company, December 1961, to August, 1962.

[54]Ibid.

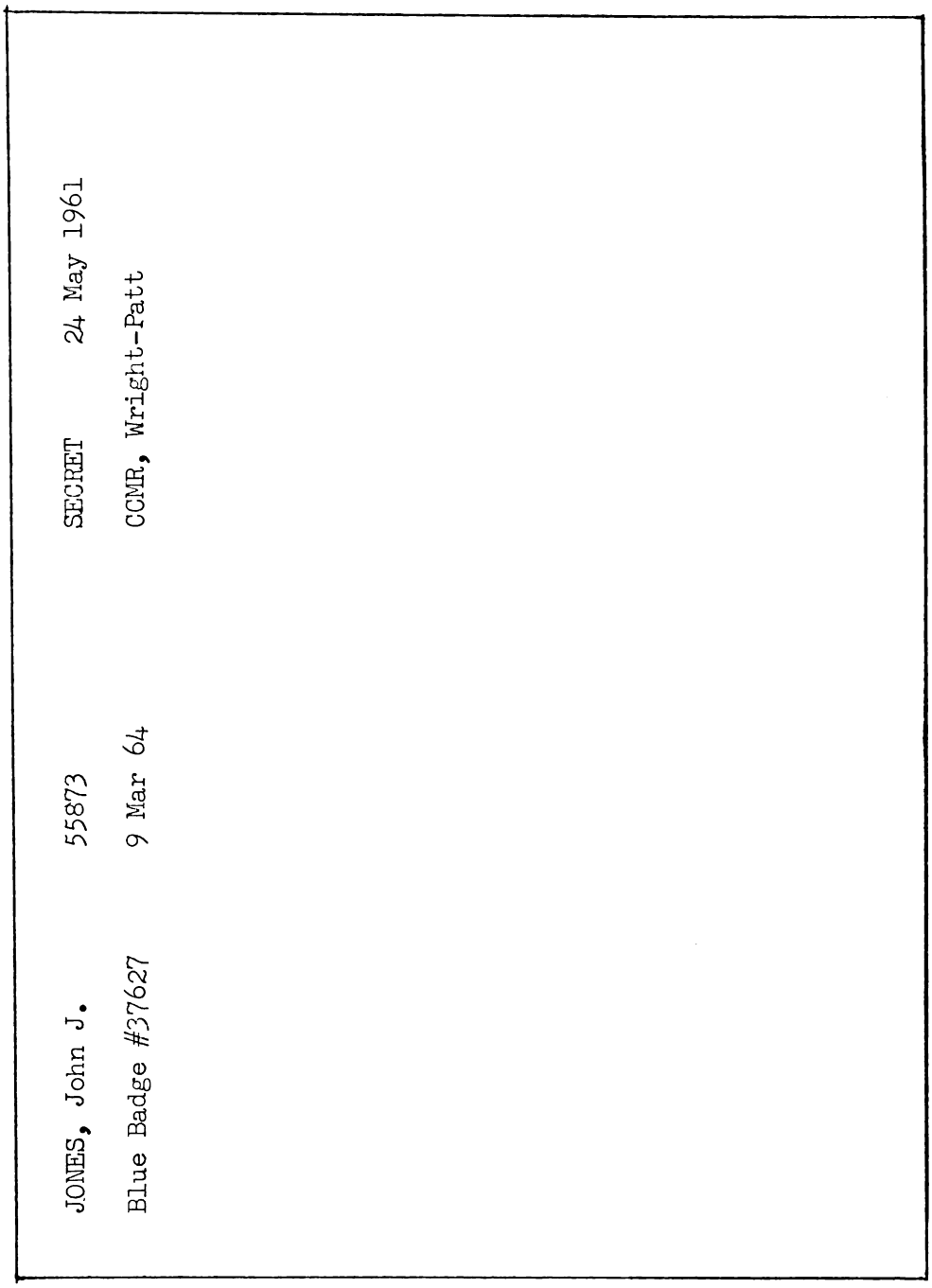


FIGURE 22

SECURITY FILE CARD
(SAMPLE FROM THE "B" COMPANY)

Clerk who makes a temporary notation of the badge number on a sheet of paper at the time she issues the badge. In this way, the Clerk knows which number to use for the next issuance.[55]

B Company is making no attempt to follow through on instances of badge loss, theft, or unaccountability. Guards are not being provided with descriptions of unresolved badges.[56]

Entry/Exit Procedures

Employees entering the plant are required to wear their badges above the waist on their outer garments. Guards permit employees to enter the plant after verifying that:

1. The badge being displayed appears to be a valid company badge.

2. The photograph on the badge corresponds with the appearance of the employee.

Employees are permitted to leave the plant at anytime, provided they are wearing badges.[57]

Employees are required to wear their badges above the waist on the outer garments at all times

---

[55]B Company Division Procedure Manual; Personnel Identification Section. Procedure 3.101, section 3; and Personal observation and study conducted by the writer at B Company, December, 1961, to August, 1962.

[56]Ibid.

[57]Ibid.

while inside the plant. Guards are instructed to challenge anyone inside the plant who is not wearing a badge.[58]

Temporary Identification

Employees who have forgotten their badges are issued "I FORGOT" badges by the perimeter guard posts. These badges are constructed of the same materials as the company's Identification Badge described on page 98, i.e., paper stock that is hot laminated between two pieces of clear vinyl plastic. The badges are turned back into the gate guards when the employees leave the plant. Since the badges are of a permanent nature and do not have any personal identifying information, such as employee name or number, they are re-issued until worn out.[59]

An employee needing an "I FORGOT" badge is required to sign his name on a register at the guard post. The guard then issues an "I FORGOT" badge if he personally knows the employee, along with instructions on wearing the badge and when and where to turn it in. If the employee is not known by the guard, the employee must identify himself by some type of identification

---

[58] Ibid.

[59] Ibid.

such as driver's license, social security card, etc. The guard then calls the Security Office Clerk to verify that the person is on record as being a company employee. An "I FORGOT" badge is then issued along with appropriate instructions for its use.[60]

FIGURE 23

"I FORGOT" BADGE
(SAMPLE FROM THE "B" COMPANY)

---

[60]Personal observation and study conducted by the writer at B Company, December, 1961, to August, 1962; and B Company Division Procedure Manual; Personnel Identification Section. Procedure 3.101, section 3.

IV. B COMPANY CLOSED AREA AND CLEARANCE IDENTIFICATION

B Company has several closed areas, both Confidential and Secret. Areas are identified by title such as "Classified Library," "Reproduction," "Document Control," etc. Access to these areas is controlled by guards or by employee personnel who work within the areas.[61]

Badge core materials are being purchased from outside suppliers who have not been granted Facility Security Clearances.[62]

An employee's degree of security clearance is identified by the color of the Identification Badge or "I FORGOT" Badge that he is wearing. A red badge denotes a Top Secret clearance, blue means Secret, and green means Confidential.[63]

Identification Device

Two methods are used to identify employees authorized to enter closed areas. In those areas where the volume of traffic is relatively high, guards use

---

[61] Personal observation and study conducted by the writer at B Company, December, 1961, to August, 1962.

[62] Ibid.

[63] B Company Division Procedure Manual; Personnel Identification Section. Procedure 3.101, section 3.

access lists as a means of controlling access. In smaller areas where the traffic is light, designated employees who work within the area identify those who are authorized to enter by visual recognition.[64]

Issuance

Access lists of authorized employees are compiled by the Manager or Supervisor who is in charge of the area. The lists are then given to the guard at the entrance to the area. Additions or deletions to the lists may also be made by the Manager or Supervisor who originated the list. It is the responsibility of the individual originating the list to determine that all employees on the list have the required level of security clearance and a legitimate need to be in the area. The Security Office is not involved in the processing or validating of access lists.[65]

Accountability

No records of access lists are maintained. Superceded or obsolete lists are picked up and destroyed by the Manager or Supervisor who originated the lists.[66]

---

[64]Personal observation and study conducted by the writer at B Company, December, 1961, to August, 1962.

[65]Ibid.

[66]Ibid.

Entry/Exit Procedures

An employee whose name appears on an access list is permitted to enter the area after being identified by the guard. The guard is responsible for verifying that the name on the employee's badge is listed on the access list prior to allowing admittance. No special checks are made for employees leaving the area.[67]

Those areas controlled by designated employees within the area rely entirely on visual recognition to identify employees authorized to enter. The largest closed area utilizing this method of identification has approximately forty employees working there, and identification is performed by a secretary positioned at the entrance. She is responsible for determining that employees entering the area are wearing either an employee Identification Badge or an "I FORGOT" Badge, and that the employee has a legitimate need to be in the area. In instances where she is not sure that the employee should be authorized admittance, she contacts her supervisor for his decision on allowing admittance to the area. In those smaller areas that utilize visual recognition to identify employees coming into the area, the same methods are used. However, the

---

[67]Personal observation and study conducted by the writer at B Company, December, 1961, to August, 1962.

identifying process is performed by whoever happens to be by the entrance at the time, and not specifically by one secretary.[68]

Temporary Identification

Since access to closed areas is accomplished by access lists and visual recognition, no temporary identification device is utilized. However, before an employee who is wearing an "I FORGOT" Badge can be admitted to an area that is controlled by an access list, he must be visually identified by some authorized employee from within the area. This is required since the "I FORGOT" Badges do not have the employees' names on them, and the guard would have no way of identifying the employee.[69]

---

[68]Personal observation and study conducted by the writer at B Company, December, 1961, to August, 1962.

[69]Ibid.

V. C COMPANY PERIMETER IDENTIFICATION

Since the total number of employees working at this company is approximately 75, the company's management has decided that no type of badging system needs to be utilized. All employees work in a one floor building and enter and leave through the front door.[70]

All of the C Company employees work on the same day shift. Entry to the plant during non-working hours is restricted to the managerial personnel of the company who have keys to the front door of the plant.[71]

Employees entering the building are visually identified by a Secretary-Receptionist who monitors and controls the entrance to the building. Each new employee is personally introduced to the Secretary-Receptionist by the new employee's supervisor, so that the Secretary-Receptionist will be able to identify the employee whenever he enters the building. In any instance where the Secretary-Receptionist is not able to identify a person as an employee of the company, she contacts the company's Personnel and Security Supervisor for his action.[72]

---

[70]Personal interview with C Company's Personnel and Security Supervisor, October 17, 1961.

[71]Ibid.

[72]Ibid.

VI. C COMPANY CLOSED AREA AND CLEARANCE IDENTIFICATION

The company has two closed areas, one for document reproduction, mailing, etc., and one for chart drafting. Both are controlled by personnel working within the areas.[73]

An employee's degree of security clearance is determined by personal knowledge of the individual's clearance. In those instances where an employee is not sure of a co-worker's degree of clearance, it is his responsibility to determine this from his supervisor before divulging any classified information.[74]

Identification Device

Both closed areas are controlled by access lists, that are provided to secretaries who monitor the entrances to the areas.[75]

Issuance

The Supervisor of each area is responsible for preparing an access list of those employees who are authorized to work in his area. It is his responsi-

---

[73]Personal interview with C Company's Personnel and Security Supervisor, October 17, 1961.

[74]Ibid.

[75]Ibid.

bility to determine that those employees on the list are properly cleared and have legitimate business in the area. The list is provided to the secretary whose responsibility it is to monitor the entrance to the area. Additions and deletions to the list are also made by the supervisor.[76]

Accountability

No records of access lists are maintained. Outdated lists are picked up and destroyed by the supervisor who originated the list.[77]

Entry/Exit Procedures

Before an employee may enter a closed area, the secretary at the entrance to the area verifies that the employee's name is on the access list. If there is any doubt as to the identity of the individual, admittance is not allowed until the employee is personally identified by the supervisor of the area. However, this is rarely a problem, since the largest list has only approximately fifteen employees' names. No check is made of employees leaving the area.[78]

---

[76]Personal interview with C Company's Personnel and Security Supervisor, October 17, 1961.

[77]Ibid.

[78]Ibid.

Temporary Identification

Those employees who are not on an access list, but who require admittance to a closed area on a short-time, temporary basis, must be personally identified and authorized to enter the area by the supervisor in charge of the area.[79]

---

[79] Ibid.

CHAPTER VII

COMPARATIVE TESTS OF THE MODEL AND THREE COMPANIES

The second purpose of this thesis, as stated in Chapter II, is to determine whether the proposed model system could be utilized at the three selected companies, and, if so, whether such utilization would result in more positive security compliance.

Determining whether the model system could be used at the three companies requires that the model system be compared against each of the three companies in relation to their various functions and purposes.

Determining whether using the model system would result in more positive security compliance requires that the model and three companies be analyzed and compared with respect to the applicable security regulations and standards.

Therefore, this chapter will:

1. Compare the model system against the systems used by the three companies to determine adaptability of the model.

2. Compare the model and the three companies against the Department of Defense security regulations where applicable and against the seventeen criteria for identification systems outlined on pages 23 to 25 to determine whether using the model would result in more positive security compliance.

I. MODEL ADAPTABILITY

Tables I and II on pages 116 and 117 provide a comparison of the functions of the model and the three companies. The various functions listed across the tops of these two charts represent a composite view of the primary functions of the systems presented in Chapters V and VI. The methods and devices for identification listed in the left columns of the tables were also obtained from Chapters V and VI. Page references to other sections of the thesis have been included for each item in the table.

In analyzing the data contained in these two tables, it is seen that the proposed model methods for employee identification provide the capability of accomplishing the various functions and purposes for which the several A, B, and C Company identification methods and devices are utilized. The tables also indicate that the proposed identification procedures, controls, and accountability methods more than fulfill the methods and standards being used by the three companies. Thus, the model system has the adaptability necessary for its being utilized at the three companies.

TABLE I

COMPARISON OF PERIMETER IDENTIFICATION FUNCTIONS

		DEVICE				ISSUANCE	ACCOUNTABILITY		ENTRY/EXIT	TEMPORARY IDENTIFICATION
	IDENTIFICATION DEVICE	Authorizes Admittance To Plant During Normal Shift Time	Authorizes Admittance To Plant At Non-Standard Times	Identifies Hourly Or Salaried Status Inside Plant	Identifies Other Status Such As Medical Limitations & Shop Foreman	Forms From Personnel Or Other Authorization Procedures Used As Basis For Issuance & Changes	Records Maintained By Name Or Employee Number	Records Maintained By Badge Number	Employees Identified By Guards Or Authorized Employees According To Established Procedures	Provides Means Of Authorizing Temporary Admittance To Plant & In-Plant Identification
MODEL	Identification Badge	X pp. 39-40	X pp. 39-40	X p. 40	X pp. 39-41	X pp.40, 42-44	X pp. 44-46	X pp. 44-46	X pp. 46-47	
MODEL	Temporary Badge			X pp. 47-49	X pp. 47-49	X pp. 47-49			X pp. 47-49	X pp. 47-49
A CO.	Identification Card	X pp. 64-65	X pp. 64-65			X pp. 70-72	X pp. 73-75		X pp. 75-76	
A CO.	Salaried Badge	X pp. 75-76	X pp. 75-76	X pp.67, 75-76		X pp. 70-72	X pp. 73-75		X pp. 75-76	
A CO.	Hourly Badge	X pp. 75-76	X pp. 75-76	X pp.68, 75-76	X p. 68	X pp. 70-72	X pp. 73-75		X pp. 75-76	
A CO.	Odd-Shift/ Odd-Lunch Card		X pp. 69, 76			X p. 72			X pp. 75-76	
A CO.	Early Admit-tance Card		X pp. 69, 76			X p. 72			X pp. 75-76	
A CO.	Temporary Pass			X pp. 77-79		X pp. 77-79			X pp. 77-79	X pp. 77-79
B CO.	Identification Badge	X pp.98, 103-4	X pp.98, 103-4			X pp. 100-101	X pp. 101-103		X pp. 103-104	
B CO.	"I FORGOT" Badge					X pp.104-105			X pp. 104-105	X pp. 104-105
C CO.	Visual Recognition	X p. 110							X p. 110	X p. 110

TABLE II

COMPARISON OF CLOSED AREAS AND CLEARANCE
IDENTIFICATION FUNCTIONS

	IDENTIFICATION METHODS & DEVICES	DEVICE		ISSUANCE	ACCOUNTABILITY		ENTRY/EXIT	TEMPORARY IDENTIFICATION
		Authorizes Admittance To Specified Closed Areas	Identifies Degree Of Employee Security Clearance	Issuance Authorized By Delegated Officials According To Established Control Procedures	Records Maintained By Name Or Employee Number	Records Maintained By Badge Number	Employees Identified By Guards Or Authorized Employees According To Established Procedures	Provides Temporary Means Of Authorizing Admittance To Areas And/Or Identifying Clearance
MODEL	Clear. & Admit. Author. Card	X pp. 50-53	X pp. 52-53	X pp. 54-58	X pp. 58-60	X pp. 58-60	X p. 61	
	Identified By Area Supervisor	X pp. 61-62					X pp. 61-62	X pp. 61-62
A CO.	Clear. & Admit. Author. Card	X pp. 81-83	X pp. 82-84	X pp. 84-86	X pp. 87-89	X pp. 87-89	X pp. 92-93	
	Access List	X pp. 81-82		X pp. 84-85			X p. 92	
	Key-Card	X pp. 81-84		X p. 86	X pp. 89-91		X p. 93	
	Temp. Admit. Author. Pass	X pp. 93-95		X pp. 94-97	X pp. 94-96		X p. 94	X pp. 93-94
	Identified By Area Supervisor	X p. 97					X p. 97	X p. 97
B CO.	Identification Badge		X p. 106	X pp. 100-101	X pp. 101-103			
	Access List	X pp. 106-107		X p. 107			X p. 108	
	"I FORGOT" Badge		X p. 106	X pp. 104-105	X p. 104			X p. 106
	Identified By Area Supervisor	X p. 108					X p. 108	X p. 108
C CO.	Access List	X p. 111		X pp. 111-112			X p. 112	
	Identified By Area Supervisor	X p. 113					X pp. 112-113	X pp. 112-113

sys
reg
tic
by
lat

per
sul
rev
the
of
bas
sol
ide
ute
pee
and
on
tee

on

Dec
C C

II. COMPLIANCE WITH REQUIREMENTS AND STANDARDS

Tables III and IV provide a comparison of the systems in question against the Department of Defense regulations and the additional seventeen identification standards. Each identification device utilized by the model and the three companies is viewed in relation to each security requirement and standard.

The data in Tables III and IV pertaining to tempering at the three companies was obtained as the result of tests conducted by the writer.[1] These tests revealed that every identification device being used by the three companies can be successfully altered. All of the plastic overlays or laminations are made of vinyl base plastic which readily dissolved when immersed in a solution of 100 per cent acetone. The hot laminated identification devices required approximately six minutes of immersion before the plastic was soft enough to peel off the device. Immersion time for other cards and badges varied from two to four minutes. Plastic on the hot laminations had completely dissolved in fifteen minutes.[2]

These tests also revealed that all information on the cards, badges, and lists could be erased. How-

---

[1] Tests conducted by the writer at A Company on December 15, 1960; at B Company in June, 1962; and at C Company on October 17, 1961.

[2] Ibid.

ever, some of the signatures required an application or two of ink eradicator to remove them. Depending on the type of device, fictitious information was typed and written in, different photographs applied, and new plastic laminated on badges and cards. These devices were then used on several authorized test cases to accomplish the various purposes for which they were designed, such as normal plant entry and departure, early admittance, clearance verification, and closed area admittance.[3]

All that was required for even the most difficult alterations was some 100 per cent acetone, ink erasure, ink eradicator, pen, typewriter, polaroid photograph, vinyl base plastic, and a lamination press.[4]

Whether the identification devices at the three companies meet the Department of Defense requirement of being "designed to minimize the possibility of tampering and unauthorized use"[5] becomes a rather abstract subject for discussion. The systems certainly are not tamper-proof as was revealed by the writer's tests. Whether the systems minimize tampering would depend on who is defining the term "minimize." Does it mean be-

---

[3] & [4] Ibid.

[5] United States Department of Defense, Industrial Security Manual for Safeguarding Classified Information, (Washington: Government Printing Office, November, 1961), pp 5-7.

ing able to significantly alter a badge in five minutes or five hours? Does it imply that all cards and badges should be completely tamperproof?

The writer discussed this area with an Air Force Industrial Security Inspector in an attempt to arrive at a more positive meaning of the requirement. The Inspector stated that the term "minimize" was very nebulous, and that this was one of the gray areas which was usually concluded by a mutual agreement between the company and the inspector involved. He also mentioned the restriction on their offices against imposing any requirement that would favor one commercial contractor or product over another.[6]

The standard used to determine whether a device minimized tampering was therefore based on the result of the writer's tests. If the device could be altered to allow unauthorized use, it was judged as not meeting the Department of Defense requirement.

Security compliance in Tables III and IV is indicated as "Yes," "No," or "N/A" (not applicable). Page references to other sections of the thesis have also been included for each item.

---

[6]David Grand, United States Air Force Industrial Security Inspector, Western Contracts Management Region, Mira-Loma, Calif., Personal Interview, November 14, 1961.

TABLE III

SYSTEMS' DEGREE OF COMPLIANCE WITH
DEPARTMENT OF DEFENSE REQUIREMENTS

	IDENTIFICATION DEVICE	DEPARTMENT OF DEFENSE REQUIREMENTS**							
		Name And Photograph	Coded Clearance And Closed Area Access Info.	Correlating Data When Used With Other Badge	Words Top Secret, Secret, Or Confidential Not Used	Designed To Minimize Tampering And Unauthorized Use	Rigid Control And Accountability	Badges Returned When Employee Terminates	Written Procedures Utilized
MODEL	Identification Badge	Yes p. 39	Yes*	Yes p. 39	Yes pp. 39-41	Yes pp. 39-41	Yes pp. 40-47	Yes pp.43,44-46	Yes p. 42
	Clear. & Admit. Auth. Card	Yes* pp. 51-52	Yes pp. 51-53	Yes pp. 51-52	Yes p. 53	Yes pp. 50-53	Yes pp. 54-61	Yes p. 59	Yes p. 42
	Temporary Badge	Regulations not applicable since this badge is not utilized for Clearance or Closed Area Identification, pp. 16, 47-49							
A CO.	Identification Card	Yes pp. 64-66	Yes*	Yes pp. 64-66	Yes pp. 64-66	No pp. 118-120	No p. 75	No p. 75	No p. 64
	Salaried & Hourly Badges	No pp. 67-68	No pp. 67-68	No pp. 67-68	Yes pp. 67-68	No pp. 118-120	No p. 75	No p. 75	No p. 64
	Odd-Shift & Early Admit. Cards	Regulations not applicable since these cards are not used for Clearance or Closed Area Identification, pp. 16, 68							
	Temporary Pass	No pp. 77-79	No pp. 77-79	Yes pp. 77-79	Yes pp. 77-79	No pp. 118-120	No pp. 77-79	N/A	No p. 64
	Clear. & Admit. Auth. Card	Yes* pp. 82-83	Yes pp. 82-84	Yes pp. 82-83	Yes pp. 82-84	No pp. 118-120	Yes pp.85-9,92-3	Yes p. 89	No p. 64
	Access List	No pp. 81-82	No pp. 81-82	Yes p. 92	Yes pp. 81-82	No pp. 118-120	Yes pp.84-5,87,92	N/A	No p. 64
	Key-Card	No pp.31-34,84	Yes pp.31-34,84	N/A	Yes pp.31-4,84	No pp. 118-120	No pp.84,89-91	No p. 90	No p. 64
	Temp. Admit. Auth. Pass	No p. 95	Yes pp. 94-95	N/A	Yes p. 95	No pp. 118-120	No pp. 93-97	No p. 96	No p. 64
B CO.	Identification Badge	Yes pp.98-99,106	Yes p. 106	N/A	Yes pp.98-9,106	No pp. 118-120	No pp. 100-3	No p. 103	Yes p. 98
	"I FORGOT" Badge	No p. 105	Yes p. 106	N/A	Yes pp. 104-6	No pp. 118-120	No pp. 104-5	N/A	Yes p. 98
	Access List	No pp. 106-107	No pp. 106-107	Yes pp. 106-107	Yes pp. 106-8	No pp. 118-120	Yes pp. 107-8	N/A	No pp. 107-8
C CO.	Visual Recognition	Regulations not applicable since there is no restriction in the regulations on using visual recognition. pp. 16-17							
	Access List	No pp. 111-112	No pp. 111-112	No pp. 111-112	Yes pp. 111-12	No pp. 118-120	Yes pp. 111-112	N/A	No pp. 111-12

*Since the Clearance and Admittance Authorization Cards do not have photographs, they are used together with the photo device to satisfactorily comply with this requirement. pp. 16 & 17.

**Pages 16 & 17.

TABLE IV

SYSTEMS' DEGREE OF COMPLIANCE WITH
ADDITIONAL IDENTIFICATION STANDARDS

	IDENTIFICATION DEVICE	ADDITIONAL IDENTIFICATION STANDARDS*																
		Tamper Resistant Design, i.e., fused Plastic, etc.	Sturdy Construction	Allows Rapid Entrance & Exit	Photo On Front Of Badge & Min. 1"	Company Name & Plant	Employee Name, Sig., D.O.B., Soc.Sec.No Color Hair Eyes, Ht, Wt.	Numbered Serially & Lost Numbers Not Re-Used	Records Cross-Filed By Name And Badge No.	Color Codes To Identify Work Shifts	Date Of Issuance And Expir.	Management Signature Or Facsimile	Make-Up And Issuance Carefully Controlled	Close Check On Term. Returns	Destroyed When Returned	Intricate Design To Make Copying Difficult	Inks Or Dyes Sensitive To Heat & Erasure	Iden. Rules Enforced
MODEL	Identification Badge	Yes pp.39-41	Yes pp.39-41	Yes pp39-41,46-7	Yes p.39	Yes pp.39-41	Yes pp.39-41	Yes p.44	Yes pp.44-45	Yes p.40	Yes pp.40-41	Yes pp.40-41	Yes pp.40-44	Yes pp.43-46	Yes p.44	Yes pp.39-41	Yes p.39	Yes pp.44,46-7
	Clear. & Admit. Auth. Card	Yes pp.50-53	Yes pp.50-53	Yes p.61	No p.52	Yes p.52	No pp.51-52	Yes p.59	Yes pp.58-61	Yes pp.52-53	Yes pp.51-52	Yes pp.51-52	Yes pp.54-58	Yes p.59	Yes p.59	Yes pp.50-52	Yes pp.50-53	Yes pp.59-61
	Temporary Badge	No pp.47-49	No pp.47-49	N/A	No pp.47-49	Yes pp.47-49	No pp.47-49	No pp.47-49	No pp.47-49	Yes pp.47-49	No pp.47-49	No pp.47-49	Yes pp.47-49	N/A pp.47-49	Yes pp.47-49	No pp.47-49	No pp.47-49	Yes pp.47-49
A CO.	Identification Card	No pp.118-20	Yes pp.64-66	Yes pp.75-6	No pp.65-66	Yes pp.65-66	No pp.65-66	No pp.64-66	No pp.73-75	No pp.64-66	Yes pp.65-66	Yes pp.65-66	Yes pp.70-72	No pp.73-75	Yes pp.73-75	Yes pp.65-66	No pp.64-66	Yes pp.75-76
	Salaried&Hourly Badges	No pp.118-20	Yes pp.67-68	Yes pp.75-6	No pp.67-68	Yes pp.67-68	No pp.67-68	No pp.67-68	No pp.73-75	Yes pp.67-68	No pp.67-68	No pp.67-68	Yes pp.70-72	No pp.73-75	Yes pp.73-75	No pp.67-68	No pp.67-68	Yes pp.75-76
	Odd-Shift & Early Admit. Cards	No pp.118-20	No p.69	Yes pp.75-6	No p.69	Yes p.69	No p.69	No p.69	No pp.73-75	No p.69	Yes p.69	Yes p.69	Yes p.72	No pp.73-75	Yes pp.73-75	No p.69	No p.69	Yes pp.75-76
	Temporary Pass	No pp.118-20	No pp.77-79	No pp.77-79	No pp.77-79	Yes pp.77-79	No pp.77-79	No pp.77-79	No pp.77-79	No pp.77-79	Yes pp.77-79	No pp.77-79	Yes pp.77-79	N/A	Yes pp.77-79	No pp.77-79	No pp.77-79	Yes pp.77-79
	Clear. & Admit. Auth. Card	No pp.118-20	Yes pp.82-85	Yes pp.92-93	No pp.82-83	Yes pp.82-83	No pp.82-83	Yes pp.87-89	Yes pp.87-89	No pp.82-84	Yes pp.82-83	Yes pp.82-83	Yes pp.85-86	Yes pp.87-89	Yes pp.87-89	No pp.82-83	No pp.82-83	Yes pp.92-93
	Access List	No pp.118-20	No pp.84-85	Yes pp.92-93	No pp.84-85	No pp.84-85	No pp.84-85	No pp.84-85	No pp.84-85	No pp.84-85	No pp.84-85	Yes pp.84-85	Yes pp.84-85	N/A	Yes pp.84-85	No pp.84-85	No pp.84-85	Yes pp.92-93
	Key-Card	No pp.118-20	Yes pp.83,31-4	Yes p.93	No pp.84,31-4	No pp.84,31-4	No pp.84,31-4	No pp.89-91	No pp.89-91	No pp.84,31-4	No pp.84,31-4	No pp.84,31-4	Yes p.86	No pp.89-91	No pp.89-91	No pp.84,31-4	No pp.84,31-4	Yes p.93
	Temp. Admit. Auth. Pass	No pp.118-20	No pp.94-95	Yes p.91	No p.95	Yes p.95	No p.95	Yes p.95	No pp.94-97	No p.95	Yes p.95	Yes pp.94-95	No pp.94-97	No pp.94-97	Yes pp.94-97	No p.95	No pp.94-95	No pp.94-97
B CO.	Identification Badge	No pp.118-20	Yes pp.98-99	Yes pp.103-4	Yes pp.98-99	Yes pp.98-99	No pp.98-99	Yes pp.101-3	No pp.101-3	No pp.98-99	Yes pp.98-99	Yes pp.98-99	Yes pp.100-1	No pp.101-3	Yes pp.101-3	Yes pp.98-99	No pp.98-99	Yes pp.103-4
	"I FORGOT" Badge	No pp.118-20	Yes pp.98,104-5	No pp.104-5	No pp.104-5	Yes pp.104-5	No pp.104-5	No pp.104-5	No pp.104-5	No pp.104-5	No pp.104-5	No pp.104-5	Yes pp.104-5	N/A	No pp.104-5	Yes pp.104-5	No pp.104-5	Yes pp.104-5
	Access List	No pp.118-20	No pp.106-7	Yes pp.108-9	No pp.106-7	No pp.106-7	No pp.106-7	No pp.106-7	No pp.106-7	No pp.106-7	No pp.106-7	Yes pp.106-7	Yes pp.106-7	N/A	Yes pp.106-7	No pp.106-7	No pp.106-7	Yes pp.108-9
C CO.	Visual Recognition	N/A	N/A	Yes p.110	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Yes pp.110-12
	Access List	No pp.118-20	No p.111	Yes p.112	No p.111	No p.111	No p.111	No p.111	No p.112	No p.111	No p.111	Yes pp.111-2	Yes pp.111-12	N/A	Yes p.112	No p.111	No p.111	Yes p.112

*Pages 23-25.

In viewing the data in Tables III and IV on pages 121 and 122, some relevant factors become apparent. Comparing the "Yes" and "No" findings of Table III for those devices falling within the scope of the Department of Defense regulations shows that the Model system has much higher percentages of "Yes" answers than any of the three companies. Higher percentages for the Model system are also found in comparing "Yes" and "No" items in Table IV and when comparing all "Yes" and "No" items in both Tables III and IV. These comparison percentages of Tables III and IV are illustrated in Table V.

TABLE V

PERCENTAGE COMPARISON OF COMPLIANCE FINDINGS OF TABLES III AND IV

	DEPARTMENT OF DEFENSE REQUIREMENTS			ADDITIONAL STANDARDS			ALL CRITERIA		
	YES	NO	%YES	YES	NO	%YES	YES	NO	%YES
MODEL	16	0	100%	37	12	76%	53	12	82%
A CO.	20	32	38%	54	80	40%	74	112	40%
B CO.	10	10	50%	21	28	43%	31	38	45%
C CO.	2	5	29%	7	11	39%	9	16	36%

Thus, tables III, IV, and V indicate that incorporating the Model system at the three companies would provide more positive and complete compliance with the Department of Defense regulations and with accepted security standards.

CHAPTER VIII

CONCLUSION

The first portion of this thesis reviewed the area of espionage with special emphasis on the present day threat to the nation's industrial complexes as posed by the Soviet espionage apparatus. A definition of the threat and its relation to employee identification systems was obtained by correlating the statements of noted authorities on the subject. This information was then developed into a realization of the need for establishing and maintaining sound security systems, with emphasis upon effective measures for positively identifying employees who work at the nation's defense industries.

Purposes were then developed on the basis of the needs and requirements for effective identification. The first purpose was to develop a model system of identification based on applicable governmental regulations and on accepted security standards. The second purpose was to determine whether the model system could be utilized at three selected defense industries of varying size and functions by analyzing the three systems in reference to the model, and, if so, whether such utilization would result in more positive security compliance.

A review of the applicable governmental regulations was then presented, followed by a presentation of additional identification standards and exemplary systems. This information was used as the basis for developing the model identification system presented in Chapter V.

In determining what type of model system to develop, several factors in addition to the regulations and standards were considered:

1. It was the writer's view that the proposed model system should have a minimum number of identification devices. Although the writer considers the one piece electronic badge system described on pages 34-37 to be superior, its use as a proposed model system was precluded by the requirement to procure the often unobtainable waivers from the contracting officer. Consideration of the Key-Card system was also overruled as a model because of this waiver requirement and the fact that Key-Cards are never authorized for controlling closed areas higher than Confidential and do not indicate the bearer*s lewellof security clearance.

2. Use of the exchange badge system was also precluded due to its inadaptability at closed areas with a high volume of personnel traffic. The procedure of having the guard locate a duplicate badge for each employee as he enters and leaves the area would

be very cumbersome in areas having hundreds of employees. To use such a method for perimeter control at large plants would also be unworkable. The cost of producing duplicate badges for each control point was also a prime factor in not proposing this as a model system of identification.

3. The Department of Defense requirement for having at least one of the devices used for closed area identification to have a photograph was also a major factor in determining the type of model system. To take a new employee photograph every time there was a change in closed areas or whenever the employee was reassigned to other work would be very costly, particularly in employee time. By identifying closed area authorization on a non-photo badge and using it along with a photo-type permanent badge, this cost factor would be greatly reduced.

4. Requiring employees to personally travel to the Identification Unit to affect changes in their closed area cards would also greatly increase system costs. By establishing request and issuance procedures that could be handled through branch office locations such as area security offices, the loss of employee time would also be reduced.

These factors, along with the Department of Defense regulations and the additional standards for

identification systems were the bases for formulating and devising the proposed model system.

The existing identification systems being used at three defense industries were then presented, using the same framework and format that was used in presenting the model system. Selection of the three industries was primarily based on their size, so that a representative view would be shown for large, medium, and small industry.

Whether the model system could be used at the three companies was then considered through a comparison of the functions and purposes of each type of identification device being used by the model and by the three companies. This comparative test indicated that all primary functions of the three companies were included in the model system.

The model and three company identification systems were then viewed in their degrees of conformity with the Department of Defense regulations and with additional standards for identification systems. This test revealed that those devices used by the model system for identifying clearance and access to closed areas were in 100 per cent compliance with the Department of Defense regulations as compared to a range of 29 to 50 per cent for the three companies. When con-

sidering all devices used for identification by the model system, a compliance factor of 76 per cent with the additional standards was realized, as compared to a range of 39 to 40 per cent for the three companies. A comparison of all identification devices with all criteria for identification indicated 82 per cent compliance by the model system and a variance of 36 to 40 per cent by the three companies. Although there is no way of determining the relative importance of the Department of Defense requirements and the 17 additional standards for identification systems, it is apparent from these results that a real need exists for improving the degree of security compliance at the three companies, and that incorporating the model system would greatly correct these deficiencies.

The writer feels there is further need for a detailed consideration of cost factors involved in the various systems and procedures described in this thesis. Selling any proposal to a company's management would appear to be greatly simplified if a cost analysis indicated that a significant savings would be realized by adopting the system being proposed. Such data, when coupled with the vital reasons for security compliance, would present a convincing argument for adopting the model system. However, the primary motivation should not involve cost, but should be found in

the realization that the goal of complete and foolproof effectiveness in the area of personnel identification is a necessary objective and of vital importance in establishing and maintaining a sound and effective security posture.

The writer's final conclusion is that this study has revealed serious deficiencies in the Department of Defense Industrial Security Regulations. As previously stated on page 119, the requirement that badges be "designed to minimize the possibility of tampering and unauthorized use" leaves much room for interpretation. The writer sees no logical reason why this vague wording should not be improved to provide stronger and more specific requirements. As indicated in the Review of Authoritative Information section of this study, the seventeen standards and criteria for identification systems are being adhered to by the Atomic Energy Commission. The writer, therefore, sees no logical reason why these standards or even more stringent requirements should not be adopted by the Department of Defense as a minimum requisite. The argument that the restriction on favoring commercial contractors and products does not allow broadening the regulation is invalid, since the Atomic Energy Commission is subject to the same restrictions as the Department of Defense, in this area.

Re-wording the section to specifically include such features as all plastic badges, bleeding inks, and/or changeable electronic codes, etc., could certainly have a profound effect in improving the degree of resistance to tampering and alteration.

The Department of Defense regulations do not even mention the problem area of duplication and copying of badges and cards. By requiring the use of electronic badges with changeable codes in highly restricted areas and possibly in all closed areas, the identification media utilized at our nation's defense industries could well approach the concept of being "fool-proof."

As stated in Chapter VI, many of the badging materials used by the companies studied are purchased from various outside suppliers, none of whom have ever been granted a Facility Security Clearance. This procedure is perfectly legitimate, since the Department of Defense regulations do not include this area of security. The writer contends that the Department of Defense regulations should insist that any identification media being utilized for controlling access to classified information should be obtained through sources cleared to the highest level of classified information being protected. Printing and production of badge core materials should be rigidly controlled. The printing plates

and over-runs should either be destroyed by the printing company or sent to the company purchasing the badges.

It is unrealistic to expect whole-hearted compliance to such vague and deficient regulations. The need for ensuring that effective security measures are maintained at our national defense industries requires that the regulations establishing the standards for the industrial security program specify sound and precise practices. Only in this way can a foundation for 100 per cent security effectiveness be established.

BIBLIOGRAPHY

A. BOOKS

Davis, John R. Industrial Plant Protection. Springfield: Charles C. Thomas Publisher, 1957.

Gocke, B. W. Practical Plant Protection and Policing. Springfield: Charles C. Thomas Publisher, 1957.

Hoover, J. Edgar. Masters of Deceit. New York: Pocket Books Inc., 1958.

Ind, Colonel Allison. A Short History of Espionage. New York: David McKay Company, Inc., 1963.

B. PUBLICATIONS OF THE GOVERNMENT, LEARNED SOCIETIES, AND OTHER ORGANIZATIONS

National Industrial Conference Board. Industrial Security; Combating Subversion and Sabotage. Studies in Business Policy No. 60. New York: National Industrial Conference Board, 1957.

National Industrial Conference Board. Industrial Security; Plant Guard Handbook. Studies in Business Policy No. 64. New York: National Industrial Conference Board, 1953.

Office of Defense Mobilization. Standards for Physical Security of Industrial and Governmental Facilities. Washington: Government Printing Office, 1958.

United States Air Force. Air Material Command Manual 205-9, Industrial Guide for Preparation of Standard Practice Procedures for the Handling and Protection of Classified Matter. Washington: Government Printing Office, August, 1957.

United States Air Force. Industrial Security Bulletin. Headquarters, Western Contracts Management Region, Mira-Loma, California, July, 1961.

United States Air Force, Industrial Security Newsletter. Headquarters, Central Contracts Management Region, Wright Patterson AFB, Ohio, December, 1961.

United States Air Force, Guide for Security Indoctrination; AFM 205-5. Washington: Government Printing Office, 1955.

United States Army. Industrial Security Management Manual. United States Army Intelligence School, Fort Holabird, Maryland, May, 1959.

United States Army. Physical Security of Military and Industrial Installations, FM 19-30. Washington: Government Printing Office, 1952.

United States Atomic Energy Commission. Physical Security Standards. Washington: Government Printing Office, 1950.

United States Atomic Energy Commission. Security. Washington: Government Printing Office, 1960.

United States Congress, House of Representatives, Committee on Un-American Activities. The Shameful Years, Thirty Years of Soviet Espionage in the United States. Washington: Government Printing Office, 1952.

United States Department of Defense. Armed Forces Industrial Security Regulation. Washington: Government Printing Office, June, 1960.

United States Department of Defense. Industrial Security Manual for Safeguarding Classified Information. Washington: Government Printing Office, November, 1961.

C. PERIODICALS

Business Week. "Tightening up Industrial Security," Business Week, (October 15, 1960), 181-185.

Committee on Identification. "Report of the Committee on Identification," Industrial Security, Vol. 1, No. 4 (December, 1956), 17-18.

Hoover, J. Edgar. "Do You Really Understand Communism?" Industrial Security, Vol. VI, No. II (April, 1962), 4-5, 23-24.

Sullivan, William C. "The Continual Threat of Espionage and Sabotage in the United States," Industrial Security, Vol. VI, No. IV (October, 1962), 44-45.

U. S. News and World Report. Testimony by J. Edgar Hoover Before the House Appropriations Committee, June 5, 1963, U. S. News and World Report, LIV (June 17, 1963), 10.

U. S. News and World Report. "The World's Big Spy Game," U. S. News and World Report, VIIIL (May 23, 1960), 46-49.

D. OTHER SOURCES

Brosnan, Edward. Chief of Physical Security for the Atomic Energy Commission, Washington, D. C. Personal Interview, March 22, 1962.

Daubert, Charles. Forms Control Department Supervisor, Lockheed Missiles and Space Company, Sunnyvale, California. Personal Interview, November, 1961.

Division Procedure Manual from B Company, Personnel Identification Section. Procedure 3.101, Section 3.

Grand, David. United States Air Force Industrial Security Inspector, Western Contracts Management Region, Mira-Loma, California. Personal Interview, November 14, 1961.

Identification Brochure from the Card Key System, Inc., Burbank, California.

Identification Brochure from Whitehead and Company, Inc., Washington, D. C., January, 1960.

Kukucka, Major Andrew J. U. S. Army Department of Counterintelligence. Speech to the American Society for Industrial Security, Washington, D. C., September 18, 1958. (Printed Copy).

Meador, Robert. Director of Security, Varian Associates, Palo Alto, California. Personal Interview, October, 1961.

Observations, Studies, and Tests conducted by the writer at the A, B, and C Companies, July 1959, to August, 1962.

Port, Tyler A. Director, Office of Security Policy, Office of the Secretary of Defense. Speech to the American Society for Industrial Security, Washington, D. C., September 18, 1958. (Printed Copy).

Shaw, Harry L. Plant Protection Manager, Lockheed Missiles and Space Company, Sunnyvale, California. Personal Interview, November, 1961.

Paper Samples from the Zellerbach Paper Company, South San Francisco, California; and from Blake, Moffitt and Towne, San Jose, California.

Trudeau, General Arthur G. United States Army Chief of Research and Development and Former Head of Army Intelligence. Speech to the American Society for Industrial Security, Washington, D. C., September 16, 1958.(Printed Copy).

Whitehead, Ned. President of Whitehead and Company, Inc., Washington, D. C., Personal Interview, August, 1960.